FACULTAD DE POSTGRADO
TRABAJO FINAL DE GRADUACIÓN

PROPUESTA DE PLAN DE CIBERSEGURIDAD PARA LA GESTIÓN DE RIESGOS EN EL ERP WEB EMPRESARIAL DE TIVITRACE BASADO EN ISO/IEC 27032 E ITIL V4

SUSTENTADO POR:

CÉSAR FRANCISCO ZEPEDA GONZÁLES
HERMES JOEL VALLECILLO MARTÍNEZ

PREVIA INVESTIDURA AL TÍTULO DE

MÁSTER EN

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

TEGUCIGALPA, FRANCISCO MORAZÁN, HONDURAS, C.A.

05 DE AGOSTO, 2025

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA

UNITEC

FACULTAD DE POSTGRADO

AUTORIDADES

UNIVERSITARIAS

RECTORA

ROSALPINA RODRÍGUEZ

VICERRECTOR ACADÉMICO NACIONAL

JAVIER ABRAHAM SALGADO LEZAMA

SECRETARIO GENERAL

ROGER MARTÍNEZ

MIRALDA

DECANA FACULTAD DE POSTGRADO

ANA DEL CARMEN RETTALLY VARGAS

PROPUESTA DE PLAN DE CIBERSEGURIDAD PARA LA GESTIÓN DE RIESGOS EN EL ERP WEB EMPRESARIAL DE TIVITRACE BASADO EN ISO/IEC 27032 E ITIL V4

TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE

MÁSTER EN GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

ASESOR METODOLÓGICO

M. Sc. JORGE RAÚL MARADIAGA CHIRINOS

MIEMBROS DE LA TERNA:

KEVIN EDUARDO FÚNEZ FÚNEZ
ALBA GABRIELA GARAY ROMERO
MANUEL SALVADOR GARCÍA LACAYO

FACULTAD DE POSTGRADO

PROPUESTA DE PLAN DE CIBERSEGURIDAD PARA LA GESTIÓN DE RIESGOS EN EL ERP WEB EMPRESARIAL DE TIVITRACE BASADO EN ISO/IEC 27032 E ITIL V4

CÉSAR FRANCISCO ZEPEDA GONZALES
HERMES JOEL VALLECILLO MARTÍNEZ

Resumen

El presente estudio surgió ante la ausencia de un plan integral de ciberseguridad que contemplara la gestión de riesgos en sistemas ERP web empresariales. Esta carencia comprometía la seguridad de la información y la continuidad operativa por la falta de lineamientos basados en ISO/IEC 27032 e ITIL V4 para enfrentar incidentes cibernéticos. El objetivo fue proponer un plan de ciberseguridad enfocado en la gestión de riesgos que reforzara la seguridad de los sistemas ERP. La investigación tuvo un enfoque mixto, con un diseño aplicado y no experimental. Se emplearon encuestas, entrevistas, listas de verificación, análisis FODA, diagrama de Ishikawa y matriz de riesgos para obtener un diagnóstico integral en la empresa TiviTrace, la cual opera con un sistema ERP web. Estas herramientas permitieron identificar vulnerabilidades y deficiencias en los procesos, así como evaluar la percepción del personal respecto a la ciberseguridad. Los hallazgos revelaron debilidades en accesos no autorizados, ataques de phishing, errores humanos y fallas en la gestión de incidentes y activos. La propuesta incluyó controles técnicos, administrativos y de sensibilización, alineados con las recomendaciones de ISO/IEC 27032 y prácticas de ITIL V4 como la gestión de incidentes, activos, continuidad del negocio y mejora continua. Esta propuesta buscó ser una guía adaptable para organizaciones que operan con ERP web, fomentando una postura proactiva frente a amenazas digitales y fortaleciendo la resiliencia organizacional.

Palabras claves: Ciberseguridad, ERP, Gestión de Riesgos, ISO/IEC 27032, ITIL V4

GRADUATE SCHOOL

PROPOSAL FOR A CYBERSECURITY PLAN FOR RISK MANAGEMENT IN TIVITRACE'S ENTERPRISE WEB-BASED ERP, BASED ON ISO/IEC 27032 AND ITIL V4

CÉSAR FRANCISCO ZEPEDA GONZALES
HERMES JOEL VALLECILLO MARTÍNEZ

Abstract

This study arose from the absence of a comprehensive cybersecurity plan that includes risk management for enterprise web-based ERP systems. This gap compromised information security and operational continuity due to the lack of guidelines based on ISO/IEC 27032 and ITIL V4 to address cyber incidents. The objective was to propose a cybersecurity plan focused on risk management to enhance the security of ERP systems. The research employed a mixed approach with an applied, non-experimental design. Surveys, interviews, checklists, SWOT analysis, Ishikawa diagram, and risk matrix were used to conduct a comprehensive diagnosis at TiviTrace, a company operating with a web-based ERP system. These tools allowed the identification of vulnerabilities and deficiencies in processes, as well as the evaluation of staff perception regarding cybersecurity. Findings revealed weaknesses in unauthorized access, phishing attacks, human errors, and failures in incident and asset management. The proposal included technical, administrative, and awareness controls aligned with the recommendations of ISO/IEC 27032 and ITIL V4 practices such as incident management, asset management, business continuity, and continuous improvement. This proposal aims to serve as an adaptable guide for organizations operating with web-based ERP systems, fostering a proactive stance against digital threats and strengthening organizational resilience.

Keywords: Cybersecurity, ERP, Risk Management, ISO/IEC 27032, ITIL V4

DEDICATORIA

A Dios, por ser mi guía constante, por darme la fortaleza en los momentos de incertidumbre y por permitirme alcanzar una meta más en mi vida. Su presencia ha sido mi mayor apoyo en este proceso.

A mis padres, por su amor incondicional, por creer siempre en mí y por enseñarme, con su ejemplo, el valor del esfuerzo, la responsabilidad y la perseverancia.

A mis hermanos, por estar siempre presentes, animándome con su compañía y confianza.

- **César Francisco Zepeda Gonzáles**.

A mis padres, por su amor incondicional y el ejemplo de entrega que siempre me inspiran. Gracias por enseñarme, con su vida, la importancia del esfuerzo, la responsabilidad y la honestidad.

A mi esposa e hija, por ser mi motor cotidiano. A ti, amor mío, por acompañarme con paciencia y fe en cada paso de este camino; y a nuestra pequeña, por recordarme a diario la alegría de soñar y la valentía de perseverar.

A mis hermanos, por su cercanía inquebrantable. Su apoyo, confianza y palabras de aliento han sido un refugio y una fuerza silenciosa que me impulsa a seguir adelante.

- **Hermes Joel Vallecillo Martínez**

AGRADECIMIENTO

Deseamos expresar nuestro más profundo agradecimiento a todas aquellas personas e instituciones que hicieron posible la realización de este trabajo. En especial, agradecemos sinceramente al M.Sc. Jorge Raúl Maradiaga Chirinos por su guía constante, asesoramiento metodológico y valiosos aportes que enriquecieron significativamente esta investigación. Asimismo, agradecemos a la Universidad Tecnológica Centroamericana (UNITEC), especialmente a la Facultad de Postgrado, por brindarnos los recursos y facilidades necesarias para el desarrollo exitoso de nuestra tesis.

Extendemos nuestra gratitud a nuestras familias por su apoyo incondicional, paciencia y comprensión durante todo el desarrollo de este estudio. Su respaldo emocional fue un factor determinante para alcanzar esta meta académica. Asimismo, agradecemos a nuestros compañeros de clase y docentes, quienes aportaron con ideas, experiencias y recomendaciones que fortalecieron el alcance y profundidad de esta propuesta. Finalmente, reconocemos y valoramos el apoyo brindado por las empresas que nos facilitaron el acceso a información relevante y casos de estudio fundamentales para validar y fortalecer nuestra investigación.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1. INTRODUCCIÓN

La presente investigación se centra en el análisis de la falta de un plan integral de ciberseguridad que permita a las organizaciones mitigar, gestionar o transferir los riesgos asociados al uso de sistemas ERP empresariales, teniendo como objetivo desarrollar una propuesta de plan de ciberseguridad para la gestión de riesgos en ERP web empresariales, basado en los lineamientos de la norma ISO/IEC 27032 y el marco de referencia ITIL V4. La ISO/IEC 27032 proporciona directrices específicas para la ciberseguridad, enfocándose en la protección de la información en entornos digitales, mientras que ITIL V4 ofrece un enfoque estructurado para la gestión de servicios de TI, permitiendo una mejor alineación entre la seguridad y los objetivos estratégicos de las organizaciones.

En la actualidad, la transformación digital y la adopción de sistemas de planificación de recursos empresariales (ERP) han permitido a las organizaciones optimizar sus procesos, mejorar la toma de decisiones y fortalecer su competitividad. Sin embargo, el crecimiento exponencial de las amenazas cibernéticas ha convertido a estos sistemas en objetivos prioritarios de ataques que pueden comprometer la confidencialidad, integridad y disponibilidad de la información crítica. Ante esta problemática, surge la necesidad de implementar estrategias efectivas para la gestión de riesgos en ciberseguridad, alineadas con estándares internacionales y mejores prácticas.

El interés en desarrollar este trabajo radica en la creciente exposición de los ERP a vulnerabilidades como accesos no autorizados, ataques de ransomware, fugas de datos y deficiencias en la configuración de seguridad. Estas amenazas no solo afectan la operatividad

de las empresas, sino que también pueden generar pérdidas económicas y daños reputacionales significativos. Al contar con un plan de ciberseguridad estructurado, se busca mitigar, gestionar y transferir los riesgos cibernéticos, garantizando así un entorno más seguro y resiliente.

Metodológicamente, la investigación se basa en un enfoque mixto, combinando análisis documental con estudios de caso en empresas que han implementado estrategias de ciberseguridad en sus sistemas ERP. Se llevo a cabo un diagnóstico de las vulnerabilidades más comunes, seguido de la formulación de un plan de acción basado en controles de seguridad, estrategias de monitoreo continuo y la implementación de estándares globales en ciberseguridad.

La investigación está organizada en diferentes secciones o apartados. En primer lugar, se realiza un análisis del contexto actual de la ciberseguridad en ERP y la importancia de la gestión de riesgos. Posteriormente, se describen los fundamentos de la ISO/IEC 27032 e ITIL V4, resaltando su aplicabilidad en la protección de sistemas empresariales. En capítulos posteriores, se presentan los hallazgos del estudio y se propone un plan de ciberseguridad adaptable a diferentes entornos empresariales.

Con este estudio, se espera aportar una guía práctica que permita a las organizaciones fortalecer su postura de seguridad, optimizar la respuesta ante incidentes y garantizar la continuidad del negocio en un contexto digital que presenta desafíos crecientes.

1.2. ANTECEDENTES DEL PROBLEMA

1. Monitor ERP System AB: Fortaleciendo la Seguridad en el Soporte Remoto

Monitor ERP System AB, una empresa sueca especializada en el desarrollo de software ERP para fabricantes, enfrentaba crecientes preocupaciones de sus clientes respecto a las violaciones de ciberseguridad. Con una base de más de 5,000 clientes y 300,000 usuarios diarios en más de 30 países, la compañía reconoció la necesidad de mejorar la seguridad en su soporte remoto. El equipo de TI de Monitor ERP utilizaba previamente una solución de acceso remoto que carecía de capacidades avanzadas de autenticación y registro, lo que limitaba el control sobre las conexiones a los servidores de los clientes. Esta situación generaba riesgos potenciales de seguridad y una falta de confianza por parte de los clientes.

Para abordar estos desafíos, Monitor ERP implementó Splashtop On-Prem, una solución de soporte remoto que ofrece opciones de despliegue en las instalaciones del cliente, permitiendo un control total sobre el entorno de soporte. Esta herramienta proporcionó autenticación de dos factores y métodos avanzados de encriptación, fortaleciendo significativamente la seguridad de las conexiones remotas.

Además, la solución permitió al equipo de TI personalizar las configuraciones de seguridad según las necesidades específicas de cada cliente, mejorando la eficiencia y reduciendo los costos de soporte en un 50%. La capacidad de registrar y monitorear detalladamente las actividades de los usuarios también minimizó la exposición a responsabilidades legales, al proporcionar evidencia clara de las acciones realizadas durante las sesiones de soporte (Splashtop, s. f.).

2. Hormel Foods: Unificando Operaciones con Oracle Cloud ERP

Hormel Foods, una compañía global con más de 50 marcas reconocidas como SPAM y Skippy Peanut Butter, enfrentaba el desafío de gestionar sistemas de TI dispares debido a múltiples adquisiciones. Esta fragmentación dificultaba la integración de datos y procesos, afectando la eficiencia operativa y la capacidad de respuesta al mercado.

Para abordar esta problemática, Hormel Foods colaboró con KPMG para implementar Oracle Cloud ERP, una solución integral que abarca la gestión financiera, de la cadena de suministro y de recursos humanos. Este proyecto de transformación digital buscaba estandarizar los procesos empresariales, mejorar la calidad de los datos y proporcionar una visión unificada del desempeño de la compañía.

La implementación de Oracle Cloud ERP permitió a Hormel Foods consolidar sus sistemas en una plataforma única, eliminando redundancias y facilitando la toma de decisiones basada en datos precisos y en tiempo real. La estandarización de procesos y la automatización de tareas rutinarias resultaron en una mayor eficiencia operativa y una reducción significativa de costos.

Además, la integración de módulos de gestión del rendimiento empresarial y de la cadena de suministro mejoró la planificación y ejecución de operaciones, permitiendo a la empresa adaptarse rápidamente a las demandas del mercado y optimizar su cadena de valor (Perspectives, s. f.), (Brown, 2022).

3. DataSentinel S.L.: Integración de Sistemas para Mejorar la Seguridad de la de la Información.

DataSentinel S.L., una empresa española en crecimiento dedicada a servicios de ciberseguridad, identificó ineficiencias en la gestión de datos y comunicación interna debido al uso de sistemas dispares. Esta fragmentación no solo afectaba la eficiencia operativa, sino que también representaba riesgos para la seguridad de la información, un aspecto crítico en su sector.

Para abordar estos desafíos, DataSentinel decidió implementar un sistema ERP que integrara todos los departamentos de la empresa, desde ventas y recursos humanos hasta operaciones y finanzas. La solución seleccionada fue Monitor ERP, conocida por su enfoque en empresas manufactureras pero adaptable a diversas industrias.

La implementación de Monitor ERP permitió a DataSentinel centralizar la gestión de la información, reduciendo la duplicidad de datos y mejorando la precisión de la información disponible para la toma de decisiones. Esta centralización facilitó la implementación de políticas de seguridad coherentes en toda la organización, asegurando que los protocolos de ciberseguridad se aplicaran de manera uniforme.

Además, la integración de módulos específicos de seguridad y control de acceso dentro del ERP permitió a DataSentinel monitorear en tiempo real las actividades internas, detectando y respondiendo rápidamente a posibles amenazas o brechas de seguridad. Esta capacidad proactiva fortaleció la confianza de sus clientes en la protección de sus datos y mejoró la reputación de la empresa en el mercado (Guitart, 2024).

4. PYMEs en Cayambe, Ecuador: Implementación de Estándares Internacionales de Seguridad

Un estudio realizado en el cantón Cayambe, Ecuador, analizó el estado de la ciberseguridad en las pequeñas y medianas empresas (PYMEs) locales. Los resultados revelaron que la mayoría de estas empresas carecían de medidas adecuadas de protección cibernética, lo que las hacía vulnerables a diversas amenazas, desde ataques de malware hasta brechas de datos sensibles.

La investigación destacó la necesidad urgente de que estas PYMEs adoptaran estándares internacionales de seguridad de la información, como ISO/IEC 27032, para mitigar los riesgos asociados a la creciente digitalización de sus operaciones. La implementación de este estándar proporciona un marco integral para gestionar la ciberseguridad, abordando aspectos como la protección de datos, la gestión de incidentes y la concienciación del personal.

Además, se recomendó la adopción de las mejores prácticas de ITIL V4 para la gestión de servicios de TI, lo que permitiría a las empresas optimizar sus procesos internos y garantizar una respuesta eficiente ante incidentes de ciberseguridad (Bautista Chimarro, 2023).

5. Empresas en Honduras: Impacto de los Ciberataques en los Sistemas

Un estudio sobre ciberseguridad en Honduras reveló que múltiples empresas han sido afectadas por ataques cibernéticos durante 2023. Estas compañías sufrieron pérdidas millonarias debido a la infiltración de software malicioso que secuestró sus sistemas y

archivos, exigiendo pagos de rescate para su liberación. El informe destacó la vulnerabilidad de las organizaciones hondureñas frente a amenazas como el ransomware, que tuvo un crecimiento significativo en el país. Aunque el estudio no menciona específicamente los sistemas ERP, los ataques cibernéticos pueden comprometer plataformas de este tipo, que gestionan información clave para la operación de las empresas. Se hace hincapié en la necesidad de adoptar marcos de seguridad más robustos para proteger sistemas sensibles, como los ERP, y prevenir incidentes similares en el futuro (La Prensa, 2023).

6. Crecimiento del Ransomware en Honduras y su Impacto en Empresas

En la primera mitad de 2023, el número de ataques de ransomware en Honduras creció 12 veces en comparación con el año anterior, afectando gravemente a empresas que dependen de tecnologías operacionales. A pesar de que el estudio no menciona explícitamente los sistemas ERP, estos son susceptibles a ataques de ransomware, lo que podría causar graves interrupciones en las operaciones empresariales.

El informe resaltó que la mayoría de las empresas afectadas no contaban con una estrategia integral de ciberseguridad. Para mitigar estos riesgos, se recomendó que las empresas refuercen sus controles de seguridad, priorizando la capacitación de sus equipos y el monitoreo continuo de sus sistemas ERP (La Prensa, 2023).

7. Empresas Centroamericanas: Crecimiento de Ciberataques y Riesgos

Un informe sobre ciberseguridad en Centroamérica evidenció que el 74% de las empresas en la región fueron víctimas de ciberataques en 2021, lo que refleja un aumento del 25% en comparación con 2020. Aunque no se menciona específicamente el uso de ERP en

este informe, es importante destacar que plataformas como estas, utilizadas por muchas empresas, son un blanco atractivo para los ciberdelincuentes. El estudio sugirió que las empresas centroamericanas, incluidas las de Honduras, deben mejorar sus estrategias de ciberseguridad y reforzar sus controles de seguridad, incluyendo la capacitación de sus equipos y la adopción de medidas preventivas para proteger sus plataformas tecnológicas, como los ERP (Advice Group Latam, 2021).

1.3. DEFINICIÓN DEL PROBLEMA

En el contexto de las empresas que utilizan sistemas ERP para gestionar sus operaciones, la ciberseguridad representa un desafío crítico. A medida que las organizaciones dependen cada vez más de soluciones digitales y sistemas integrados para gestionar datos y procesos empresariales, se han incrementado las amenazas cibernéticas que pueden comprometer la seguridad de estos sistemas. La falta de una estrategia robusta de ciberseguridad, específicamente diseñada para la gestión de riesgos en ERP, deja a las empresas vulnerables a ataques que pueden resultar en pérdidas económicas significativas, daños a la reputación y, en casos extremos, la paralización total de las operaciones.

El problema que se aborda en esta investigación radica en la insuficiencia de planes de ciberseguridad adaptados a los ERP empresariales, que a menudo no consideran las amenazas específicas relacionadas con estos sistemas integrados. Aunque muchas organizaciones implementan medidas de seguridad generales, estas no siempre son suficientes para proteger la complejidad y el volumen de datos que circulan en un ERP, ni para cumplir con las normativas internacionales y las mejores prácticas en ciberseguridad. Además, la falta de una cultura organizacional que priorice la seguridad informática contribuye a la vulnerabilidad de los sistemas.

En este contexto, es crucial desarrollar un plan de ciberseguridad que no solo contemple las amenazas generales del entorno digital, sino que también se enfoque en los riesgos específicos que enfrentan los sistemas ERP empresariales. Este plan debe estar alineado con estándares internacionales como ISO/IEC 27032, que se centra en la ciberseguridad, y con marcos de gestión de servicios como ITIL V4, que proporciona un enfoque estructurado para la gestión de los riesgos tecnológicos. La implementación de un plan de ciberseguridad efectivo puede ayudar a las empresas a mitigar los riesgos asociados con sus ERP, garantizar la protección de los datos críticos, y mejorar su capacidad para enfrentar incidentes de seguridad de manera proactiva.

1.4. PREGUNTAS DE INVESTIGACIÓN

1.4.1. PREGUNTA GENERAL

¿Cómo puede un plan de ciberseguridad basado en ISO/IEC 27032 e ITIL v4 mitigar, gestionar o transferir los riesgos de ciberseguridad en los ERP empresariales?

1.4.2. PREGUNTAS ESPECÍFICAS

1. ¿Cuáles son los principales riesgos de ciberseguridad en los ERP empresariales?
2. ¿Cómo pueden aplicarse las mejores prácticas de la norma ISO/IEC 27032 en la gestión de riesgos de ciberseguridad en ERP empresariales?
3. ¿Qué estrategias pueden implementarse para la detección y mitigación de Amenazas Persistentes Avanzadas (APT) en ERP empresariales?
4. ¿Cómo puede contribuir un plan de respuesta y recuperación alineado con ITIL V4 a la continuidad del negocio en ERP empresariales?
5. ¿Cómo se puede medir la efectividad del plan de ciberseguridad en la reducción de riesgos de ciberseguridad en ERP empresariales?

1.5. OBJETIVOS DE INVESTIGACIÓN

1.5.1. OBJETIVO GENERAL

Diseñar una propuesta de plan de ciberseguridad para la gestión de riesgos en ERP web empresariales, basado en ISO/IEC 27032 e ITIL V4, con el fin de mitigar, gestionar o transferir los riesgos de ciberseguridad en plataformas web críticas.

1.5.2. OBJETIVOS ESPECÍFICOS

1. Identificar y clasificar los riesgos de ciberseguridad en ERP empresariales mediante un análisis de vulnerabilidades y auditorías de seguridad, con el fin de determinar las amenazas más críticas.
2. Analizar las mejores prácticas de seguridad de la información de la norma ISO/IEC 27032 y su aplicabilidad en la gestión de riesgos de ciberseguridad en ERP empresariales.
3. Definir estrategias de detección y mitigación de Amenazas Persistentes Avanzadas (APT) en ERP empresariales, utilizando controles de seguridad basados en ISO/IEC 27032.
4. Identificar cada uno de los activos según su categoría de riesgo para determinar cuáles serían las mejores alternativas para dar respuesta y recuperación ante incidentes alineados con ITIL V4 para mejorar la continuidad del negocio en ERP empresariales.
5. Evaluar el impacto del plan de ciberseguridad mediante indicadores clave de desempeño (KPI) para medir su efectividad en la reducción de riesgos en ERP empresariales.

1.6. JUSTIFICACIÓN

Las empresas, especialmente aquellas que manejan plataformas web, juegan un papel crucial en el crecimiento económico y la competitividad de los mercados. En un entorno digital cada vez más globalizado, la adopción de nuevas tecnologías ha traído consigo una mayor exposición a riesgos cibernéticos que amenazan no solo los activos digitales de las empresas, sino también su reputación y sostenibilidad a largo plazo. Estos riesgos, derivados de la falta de protocolos de seguridad robustos, pueden llevar a consecuencias graves, incluyendo la pérdida de datos confidenciales, interrupción de servicios, o incluso un ataque que degrade la confianza de los clientes en la empresa. Por ello, la implementación de planes de ciberseguridad es esencial, ya que permite a las organizaciones mitigar estos riesgos, garantizando la protección de la información y la continuidad de sus operaciones.

En el contexto de Latinoamérica, donde las plataformas web empresariales están en constante crecimiento, la falta de un enfoque estructurado y formal en ciberseguridad representa una amenaza significativa. Países como Honduras, donde las pequeñas y medianas empresas (PYMEs) representan un alto porcentaje del mercado y generan una parte considerable del empleo, se encuentran en una situación vulnerable frente a amenazas cibernéticas. Según estudios recientes, muchas de estas empresas aún no cuentan con protocolos de seguridad adecuados, lo que las hace susceptibles a ataques que podrían afectar no solo su actividad, sino también la economía local. La implementación de un plan de ciberseguridad basado en estándares internacionales como ISO 27032 e ITIL v4, permitirá no solo proteger estos activos digitales, sino también fomentar un entorno de confianza y estabilidad en el sector, lo cual es clave para su crecimiento y competitividad.

La propuesta de un plan de ciberseguridad para la gestión de riesgos en plataformas web empresariales tiene un gran impacto social, pues asegura que las empresas puedan operar de manera segura, sin poner en riesgo los datos personales de sus clientes y usuarios. Este tipo de plan también ayudará a la inclusión digital de empresas pequeñas y medianas, facilitando su acceso a soluciones tecnológicas sin temor a ser vulneradas por ciberdelincuentes. Además, a nivel regional, implementar medidas de seguridad digital contribuye a una mayor resiliencia en toda la infraestructura empresarial, lo que permite que más empresas participen de forma segura en el comercio digital, impulsando la economía de la región. A nivel empresarial, un plan de ciberseguridad adecuado es fundamental no solo para proteger los activos de la empresa, sino también para asegurar su crecimiento y sostenibilidad. La capacidad de adaptarse a las normas internacionales de seguridad y gestión de servicios como ISO 27032 e ITIL V4 se convierte en un diferenciador competitivo importante, pues las empresas que invierten en seguridad digital tienen más probabilidades de establecer relaciones duraderas con sus clientes y ofrecer servicios más confiables. Implementar un sistema de gestión de riesgos cibernéticos de manera integral, permitirá a las empresas minimizar el impacto de incidentes y mejorar sus prácticas de recuperación ante desastres, asegurando su operación en el largo plazo.

CAPÍTULO II. MARCO TEÓRICO

En el presente proyecto, el marco teórico se centra en el análisis de la ciberseguridad en entornos empresariales, con especial énfasis en la gestión de riesgos en sistemas ERP (Enterprise Resource Planning). La transformación digital y la adopción de estos sistemas han permitido a las organizaciones optimizar sus procesos y mejorar la toma de decisiones. Sin embargo, la creciente sofisticación de las amenazas cibernéticas ha convertido a los ERP en objetivos de ataques que pueden comprometer la confidencialidad, integridad y disponibilidad de la información crítica.

Este apartado contextualiza la relevancia de la investigación dentro del ámbito de la seguridad de la información y establece la conexión entre las mejores prácticas internacionales y la necesidad de contar con un plan integral de ciberseguridad. Para ello, se abordan los fundamentos de la ISO/IEC 27032, que proporciona directrices para la protección en entornos digitales, y el marco ITIL V4, que ofrece un enfoque estructurado para la gestión de servicios de TI, permitiendo una mejor alineación entre la seguridad y los objetivos estratégicos de las organizaciones.

Asimismo, se analizan los principales riesgos asociados a la implementación y operación de sistemas ERP web, tales como accesos no autorizados, ataques de ransomware, fugas de datos y configuraciones deficientes de seguridad. En este contexto, se destaca la importancia de adoptar estrategias efectivas para la mitigación, gestión y transferencia de estos riesgos, garantizando un entorno empresarial seguro y resiliente.

A través de un enfoque mixto, combinando análisis documental con estudios de caso en empresas que han implementado estrategias de ciberseguridad en sus ERP, esta

investigación busca proporcionar un marco de referencia que facilite la protección de estos sistemas críticos.

2.1 MACROENTORNO.

2.2.1. INTRODUCCIÓN A LA GESTIÓN DE RIESGOS DE CIBERSEGURIDAD EN ERP EMPRESARIALES

La ciberseguridad en los sistemas ERP (Enterprise Resource Planning) empresariales es un aspecto fundamental en la protección de la información y la continuidad operativa de las organizaciones. Estos sistemas, que integran múltiples procesos de negocio, almacenan datos críticos que pueden ser blanco de ataques cibernéticos. La creciente sofisticación de las amenazas ha impulsado la adopción de marcos de seguridad como ISO/IEC 27032 e ITIL V4, que proporcionan directrices para la protección de la infraestructura digital.

La gestión de riesgos de ciberseguridad en ERP requiere un enfoque estructurado basado en el análisis de vulnerabilidades y auditorías de seguridad. Identificar y clasificar los riesgos permite a las organizaciones priorizar acciones para mitigar amenazas críticas, reducir la superficie de ataque y mejorar la resiliencia ante incidentes de seguridad. De acuerdo con el Instituto Nacional de Estándares y Tecnología (NIST), la evaluación de riesgos debe considerar amenazas internas y externas, vulnerabilidades en la infraestructura de TI y el impacto potencial sobre los activos organizacionales ((NIST), 2022).

El objetivo de esta sección es analizar cómo la identificación y clasificación de riesgos de ciberseguridad en ERP puede fortalecer la postura de seguridad empresarial. Para ello, se revisarán marcos de referencia y estándares internacionales

que han demostrado efectividad en la mitigación de riesgos, proporcionando lineamientos aplicables a diversos sectores e industrias.

2.2.2. EVALUACIÓN DE RIESGOS Y AUDITORÍAS DE SEGURIDAD

Las auditorías de seguridad son una herramienta clave en la gestión de riesgos cibernéticos. Estas evaluaciones permiten detectar vulnerabilidades en la configuración de los sistemas ERP, verificar el cumplimiento de normativas de seguridad y evaluar la efectividad de los controles implementados. De acuerdo con ISO/IEC 27032, la auditoría de ciberseguridad debe incluir pruebas de penetración, análisis de configuración y revisión de accesos para garantizar la protección de la información sensible.

Por otro lado, la metodología de ITIL V4 enfatiza la importancia de la gestión de incidentes y la recuperación ante desastres en entornos empresariales. La integración de estrategias de seguridad en la gestión de servicios de TI ayuda a reducir el impacto de posibles brechas y a mejorar la respuesta ante eventos de seguridad.

La norma ISO/IEC 27032 es un estándar internacional enfocado en la ciberseguridad y la protección de la información en entornos digitales. Fue elaborada por la Organización Internacional de Normalización (ISO) junto con la Comisión Electrotécnica Internacional (IEC), con el propósito de ofrecer un marco integral para gestionar los riesgos relacionados con la seguridad cibernética y fortalecer la capacidad de las organizaciones para enfrentar amenazas digitales. Impulsa el uso de enfoques adecuados para proteger la información y proporciona mecanismos que ayudan a controlarla de forma efectiva en la empresa. También permite implementar medidas que resguarden los procesos operativos, las acciones realizadas en entornos

digitales, las aplicaciones empleadas, el tratamiento de datos y los servicios utilizados, incluyendo la preparación del personal que operará con estas soluciones. Esta norma fue creada con dos fines que serían cubrir los aspectos relacionados con ciberseguridad que no se habían tocado en versiones anteriores y a la vez promover la cooperación entre agentes como el CSF, CyberSecurity Framework y el Marco de Ciberseguridad del NITS.

Por otro lado, la ISO/IEC /27032 está enfocado en cuatro ejes fundamentales que son: Seguridad de la información, Seguridad de las redes, Seguridad en Internet y la Protección de infraestructuras críticas para la información, los cuales ofrecen seguridad a todo el ciberespacio de las empresas como dotar de un plan de acción en caso de presentarse una crisis y planificando la resolución de incidentes todo con el objetivo de contar con una estrategia para combatir los riesgos que se pueden presentar o que se lleguen a materializar.

Cabe mencionar algunas diferencias entre la ISO 27032 e ISO 27001 ya que, aunque ambas normas están relacionadas con la seguridad de la información presentan diferencias ya que la ISO 27001 está centrada en la gestión de la seguridad de la información general la ISO 27032 se enfoca exclusivamente en ciberseguridad y protección contra amenazas digitales, y para poder adoptar la norma en las organizaciones, se recomienda seguir estos pasos:

1. Evaluar la situación actual: Identificar vulnerabilidades y riesgos cibernéticos existentes.
2. Desarrollar políticas de seguridad: Establecer normas internas alineadas con ISO 27032.

3. Capacitar al personal: Formar a los empleados en buenas prácticas de ciberseguridad.
4. Implementar controles técnicos: Uso de firewalls, antivirus, cifrado de datos y otras medidas de seguridad.
5. Monitorear y mejorar continuamente: Realizar auditorías y pruebas para garantizar la efectividad de las estrategias

2.2.3 ANÁLISIS DE LAS MEJORES PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN SEGÚN LA NORMA ISO/IEC 27032 Y SU APLICABILIDAD EN LA GESTIÓN DE RIESGOS DE CIBERSEGURIDAD EN ERP EMPRESARIALES

La norma ISO/IEC 27032 establece un marco integral para la ciberseguridad, proporcionando directrices específicas para proteger los activos digitales de las organizaciones y garantizar la integridad de los sistemas de información (International Organization for Standardization [ISO], 2023). Esta norma se centra en la colaboración entre diferentes partes interesadas para mitigar riesgos cibernéticos y reforzar la seguridad en entornos digitales, especialmente en sistemas críticos como los ERP empresariales.

En el contexto de los sistemas de Planificación de Recursos Empresariales (ERP), la implementación de la ISO/IEC 27032 resulta fundamental debido a la sensibilidad y criticidad de los datos manejados en estos sistemas. Los ERP integran múltiples procesos empresariales, desde la gestión financiera hasta la logística y los recursos humanos, convirtiéndose en objetivos estratégicos para atacantes

cibernéticos (Almeida, 2022). Por lo tanto, aplicar las mejores prácticas de ciberseguridad no solo minimiza las vulnerabilidades, sino que también fortalece la resiliencia organizacional ante amenazas emergentes.

2.2.4 IDENTIFICACIÓN Y CLASIFICACIÓN DE RIESGOS EN ERP

Uno de los principales enfoques de la norma ISO/IEC 27032 es la identificación y clasificación sistemática de riesgos cibernéticos. Este proceso implica la realización de auditorías de seguridad y análisis de vulnerabilidades para detectar y evaluar posibles amenazas (National Institute of Standards and Technology [NIST], 2022). En el caso de los ERP, las amenazas más comunes incluyen el acceso no autorizado, la fuga de información sensible, el sabotaje interno y los ataques de ransomware (Chen et al., 2021).

La norma recomienda adoptar un enfoque proactivo basado en la gestión de riesgos que incluya la identificación de activos críticos, la evaluación del impacto potencial de las amenazas y la priorización de los riesgos según su probabilidad y gravedad (ISO, 2023). Además, se enfatiza la necesidad de implementar controles de seguridad ajustados a la infraestructura tecnológica del ERP para garantizar la protección de los datos y la continuidad del negocio (Sommers & Bensoussan, 2023).

2.2.5 APLICABILIDAD DE LAS MEJORES PRÁCTICAS DE ISO/IEC 27032 EN ERP

La ISO/IEC 27032 establece un conjunto de prácticas recomendadas que, aplicadas a los ERP empresariales, permiten una gestión eficiente de los riesgos de ciberseguridad. Estas prácticas incluyen:

1. **Evaluación de Vulnerabilidades:** Implementar auditorías periódicas para identificar debilidades en la infraestructura del ERP. Este enfoque sistemático facilita la detección temprana de riesgos y la aplicación de medidas correctivas (Almeida, 2022).
2. **Gestión de Incidentes de Seguridad:** Desarrollar procedimientos estandarizados para la respuesta y recuperación ante incidentes, minimizando el impacto de las brechas de seguridad en los procesos empresariales (Chen et al., 2021).
3. **Protección de la Información Crítica:** Aplicar cifrado de datos, autenticación multifactorial y segmentación de redes para resguardar la confidencialidad, integridad y disponibilidad de la información (ISO, 2023).
4. **Concienciación y Capacitación en Ciberseguridad:** Fomentar una cultura de seguridad a través de programas de formación continua dirigidos a empleados y proveedores, reduciendo el riesgo asociado al factor humano (Sommers & Bensoussan, 2023).
5. **Colaboración Interinstitucional:** Establecer mecanismos de cooperación con organismos gubernamentales y asociaciones sectoriales para compartir información sobre amenazas emergentes y buenas prácticas de ciberseguridad (NIST, 2022).

2.2.6 BENEFICIOS DE IMPLEMENTAR LA ISO/IEC 27032 EN LA GESTIÓN DE RIESGOS DE ERP

La adopción de las directrices de la ISO/IEC 27032 en la gestión de riesgos de ciberseguridad en ERP empresariales proporciona beneficios tangibles, entre ellos:

1. **Reducción de Riesgos:** La identificación proactiva y mitigación de vulnerabilidades disminuye la exposición a ciberataques.
2. **Cumplimiento Normativo:** Asegura el cumplimiento con estándares internacionales y marcos regulatorios locales, fortaleciendo la gobernanza corporativa.
3. **Resiliencia Operativa:** Mejora la capacidad de respuesta y recuperación ante incidentes, garantizando la continuidad del negocio.
4. **Confianza del Cliente:** Refuerza la confianza de los clientes y partes interesadas al demostrar un compromiso con la seguridad de la información.

2.2.7. ESTRATEGIAS DE DETECCIÓN Y MITIGACIÓN DE AMENAZAS PERSISTENTES AVANZADAS (APT) EN ERP EMPRESARIALES BASADAS EN ISO/IEC 27032

Las Amenazas Persistentes Avanzadas (APT) representan un riesgo significativo para los sistemas ERP empresariales debido a su sofisticación, persistencia y capacidad de evadir las defensas tradicionales (National Institute of Standards and Technology [NIST], 2022). Estas amenazas están diseñadas para infiltrarse silenciosamente, permanecer indetectables por largos períodos y extraer información confidencial o interrumpir los procesos empresariales (Chen et al., 2021).

2.2.8. ESTRATEGIAS DE DETECCIÓN DE APT

La norma ISO/IEC 27032 sugiere implementar un enfoque integral para la detección temprana de APT en ERP empresariales, el cual incluye:

1. **Monitoreo Continuo:** Implementar sistemas de monitoreo continuo para identificar patrones anómalos de comportamiento en el tráfico de red y en las interacciones con el ERP. Esto incluye el uso de Sistemas de Detección de Intrusiones (IDS) y Sistemas de Prevención de Intrusiones (IPS) para alertar sobre actividades inusuales (ISO, 2023).
2. **Análisis de Indicadores de Compromiso (IoC):** Utilizar herramientas avanzadas para identificar Indicadores de Compromiso, como direcciones IP sospechosas, cambios en la configuración del sistema y accesos no autorizados (Sommers & Bensoussan, 2023).
3. **Inteligencia de Amenazas:** Integrar fuentes de inteligencia de amenazas cibernéticas para anticipar posibles vectores de ataque. Esto permite adaptar las estrategias de detección a las tácticas emergentes utilizadas por los atacantes (NIST, 2022).

2.2.9. ESTRATEGIAS DE MITIGACIÓN DE APT

Para mitigar el impacto de las APT en los ERP empresariales, ISO/IEC 27032 recomienda las siguientes acciones:

1. **Segmentación de Redes:** Implementar una segmentación de redes efectiva para limitar el movimiento lateral de los atacantes dentro de la infraestructura de ERP (Almeida, 2022).

2. **Control de Acceso Rigoroso:** Establecer políticas de control de acceso basadas en el principio de privilegio mínimo. Esto implica restringir los permisos de los usuarios y aplicar autenticación multifactorial para acceder a los sistemas críticos (ISO, 2023).

3. **Respuesta a Incidentes:** Diseñar y probar regularmente un plan de respuesta a incidentes específico para APT, que permita contener, erradicar y recuperar los sistemas ERP afectados (Chen et al., 2021).

4. **Actualización de Sistemas:** Mantener los sistemas ERP actualizados con parches de seguridad para reducir las vulnerabilidades explotables por los atacantes (Sommers & Bensoussan, 2023).

2.2.10 IDENTIFICACIÓN DE ACTIVOS SEGÚN SU CATEGORÍA DE RIESGO Y ESTRATEGIAS DE RESPUESTA Y RECUPERACIÓN ANTE INCIDENTES ALINEADOS CON ITIL V4 PARA MEJORAR LA CONTINUIDAD DEL NEGOCIO EN ERP EMPRESARIALES

La correcta identificación y clasificación de activos en un sistema ERP es fundamental para implementar estrategias efectivas de respuesta y recuperación ante incidentes, alineadas con las mejores prácticas de ITIL V4 (Axelos, 2022). Según ITIL V4, los activos pueden clasificarse en activos de hardware, software, información y personal, cada uno con distintos niveles de riesgo y criticidad.

2.2.11 CLASIFICACIÓN DE ACTIVOS EN ERP

1. **Activos Críticos:** Incluyen bases de datos financieras, registros de clientes y procesos logísticos esenciales. Estos activos requieren medidas de protección

avanzadas como copias de seguridad redundantes y cifrado de extremo a extremo (Axelos, 2022).

2. **Activos Sensibles:** Comprenden la información confidencial de empleados y documentos estratégicos. Para estos activos, ITIL V4 recomienda la implementación de controles de acceso basados en privilegios y auditorías regulares (Sommers & Bensoussan, 2023).
3. **Activos de Soporte:** Incluyen infraestructuras físicas y plataformas de software. Su protección implica la aplicación de políticas de gestión de parches y mantenimiento preventivo (ISO, 2023).

2.2.12 ESTRATEGIAS DE RESPUESTA Y RECUPERACIÓN ALINEADAS CON ITIL V4

1. **Gestión de Incidentes:** Establecer un flujo de trabajo estructurado para la detección, análisis y resolución rápida de incidentes, minimizando el tiempo de inactividad del ERP (Axelos, 2022).
2. **Gestión de Problemas:** Identificar la causa raíz de los incidentes recurrentes y aplicar soluciones permanentes para evitar su reaparición (ISO, 2023).
3. **Gestión de Continuidad del Negocio**: Implementar planes de recuperación ante desastres (DRP) que incluyan procedimientos de respaldo automatizados y pruebas periódicas de recuperación (Sommers & Bensoussan, 2023).

Estas estrategias garantizan la resiliencia operativa de los sistemas ERP, permitiendo una respuesta eficaz ante amenazas cibernéticas y asegurando la continuidad del negocio.

2.2.13 EVALUACIÓN DEL IMPACTO DE UN PLAN DE CIBERSEGURIDAD EN SISTEMAS ERP EMPRESARIALES

1. DEFINICIÓN DE INDICADORES CLAVE DE DESEMPEÑO (KPI)

Los Indicadores Clave de Desempeño (KPI) son herramientas fundamentales para medir la efectividad de un plan de ciberseguridad en sistemas ERP, especialmente en un entorno empresarial donde la protección de los activos digitales y la continuidad operativa son cruciales. Estos indicadores deben de tener ciertas características las cuales se detallan en la Figura 1 de la infografía siguiente:

Figura 1. Criterios SMART Para elaboración de KPIs

Criterios SMART para elaboración de KPIs

Nota: elaboracion propia de infografia, basada en Doran (1981)

2.2.14 KPI RECOMENDADOS PARA EVALUAR LA EFECTIVIDAD DEL PLAN DE CIBERSEGURIDAD

Para medir la efectividad de un plan de ciberseguridad, es necesario establecer los siguientes KPIs:

a) Número Total de Incidentes de Seguridad: Este KPI mide la cantidad de incidentes reportados en un período determinado. Una reducción en este número indicaría que las defensas del sistema ERP están siendo más efectivas.

b) Tiempo Medio para Detectar (MTTD): Este indicador mide el tiempo promedio desde la ocurrencia de un incidente hasta su detección. Una disminución en el MTTD sugiere que la organización cuenta con sistemas de monitoreo de seguridad eficientes.

c) Tiempo Medio para Responder (MTTR): Este KPI evalúa el tiempo promedio desde que un incidente es detectado hasta que es resuelto. Un MTTR más corto indica una mayor eficiencia en la respuesta ante incidentes de seguridad.

d) Porcentaje de Sistemas con Parches Actualizados: Este indicador refleja el porcentaje de sistemas ERP que cuentan con las últimas actualizaciones y parches de seguridad. Mantener este porcentaje alto es fundamental para evitar vulnerabilidades que puedan ser explotadas por ciber atacantes.

e) Número de Intentos de Acceso No Autorizado Bloqueados: Mide la cantidad de intentos de intrusión detectados y bloqueados. Un número elevado de

bloqueos demuestra la efectividad de las medidas preventivas de seguridad implementadas en el sistema ERP.

2.2.15 IMPLEMENTACIÓN Y SEGUIMIENTO DE LOS KPI

Para garantizar una evaluación precisa y efectiva del impacto del plan de ciberseguridad, es importante seguir estos pasos:

a) Establecer Líneas Base: Antes de la implementación del plan de ciberseguridad, es fundamental definir los valores iniciales de cada KPI para facilitar la comparación y medición del progreso.

b) Monitoreo Continuo: Implementar herramientas de monitoreo en tiempo real que permitan la recolección de datos precisos y actualizados sobre los KPIs definidos, asegurando que el sistema ERP esté constantemente vigilado.

c) Informes Periódicos: Generar reportes regulares sobre los KPIs que reflejen las tendencias y permitan detectar áreas de mejora o vulnerabilidades emergentes.

d) Revisión y Ajuste de Estrategias: Basándose en los resultados obtenidos, es necesario revisar y ajustar las políticas y procedimientos de seguridad para enfrentar de manera efectiva los riesgos y amenazas cibernéticas.

La evaluación del impacto de un plan de ciberseguridad mediante KPIs bien definidos es esencial para medir la efectividad en la reducción de riesgos y asegurar la protección de los sistemas ERP empresariales, estos indicadores no solo ofrecen una visión clara del estado actual de la seguridad, sino que también ayudan a la toma

de decisiones informadas para mejorar continuamente las defensas cibernéticas de la organización, asegurando su continuidad operativa a largo plazo.

2.3 MICROENTORNO

2.3.1 INTRODUCCIÓN A LA GESTIÓN DE RIESGOS DE CIBERSEGURIDAD EN ERP EMPRESARIALES

La gestión de riesgos de ciberseguridad es fundamental para proteger las infraestructuras tecnológicas de cualquier organización, y en el caso de los sistemas ERP, se convierte en un componente esencial para salvaguardar los datos y procesos críticos del negocio. En el caso de los **ciberataques a las instituciones del Estado en Honduras (2023),** se evidenció que la falta de una gestión efectiva de riesgos dejó a muchas organizaciones vulnerables a amenazas cibernéticas, con consecuencias que afectaron tanto la seguridad de la información como la eficiencia operativa.

La adopción de un sistema ERP robusto que implemente medidas de protección, como las descritas en la **norma ISO/IEC 27032**, permite que las organizaciones identifiquen, evalúen y clasifiquen sus riesgos de manera proactiva. Esto no solo garantiza la protección de los datos sensibles, sino que también permite mitigar los riesgos derivados de posibles ciberataques. La gestión adecuada de riesgos es esencial para la protección de los sistemas ERP que centralizan las operaciones empresariales (Heraldo, 2023).

2.3.2 EVALUACIÓN DE RIESGOS Y AUDITORÍAS DE SEGURIDAD

En cuanto a la evaluación de riesgos y auditorías de seguridad, el caso de los ciberataques en el sector financiero de Honduras pone en evidencia la importancia de realizar

auditorías periódicas de seguridad en los sistemas ERP. En un entorno empresarial, los sistemas ERP gestionan grandes volúmenes de datos sensibles, como información financiera, inventarios y recursos humanos. La falta de auditorías de seguridad periódicas expone a las organizaciones a posibles brechas de seguridad que pueden ser aprovechadas por actores maliciosos.

La implementación de auditorías regulares, basadas en estándares internacionales como **ISO/IEC 27032**, es crucial para detectar vulnerabilidades dentro de los sistemas ERP. La norma establece controles específicos para evaluar la seguridad de los sistemas de información y proteger los activos digitales, lo cual es esencial para garantizar que los sistemas ERP sean resilientes ante posibles ciber amenazas.

De igual manera, las auditorías proporcionan una visión integral de las vulnerabilidades que pueden afectar no solo la infraestructura tecnológica, sino también los procesos de negocio que dependen del sistema ERP. Adoptar este enfoque de evaluación de riesgos permite que las organizaciones no solo se protejan contra amenazas conocidas, sino también se preparen para nuevas formas de ciberataques (Prensa, 2022).

2.3.3 ANÁLISIS DE LAS MEJORES PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN SEGÚN LA NORMA ISO/IEC 27032 Y SU APLICABILIDAD EN LA GESTIÓN DE RIESGOS DE CIBERSEGURIDAD EN ERP EMPRESARIALES

En el análisis de las mejores prácticas de seguridad de la información según la norma ISO/IEC 27032, el Banco Nacional de Honduras (BNH) representa un ejemplo claro de cómo la adopción de estándares internacionales de seguridad puede fortalecer la protección de los sistemas empresariales, incluidos los ERP. ISO/IEC 27032 proporciona un marco para

abordar la seguridad cibernética de forma integral, considerando tanto las amenazas externas como las internas.

La implementación de esta norma en un sistema ERP ayuda a las organizaciones a gestionar los riesgos de manera efectiva, ya que esta norma incluye controles de seguridad que son directamente aplicables a los sistemas de gestión empresarial. La adopción de ISO/IEC 27032 en los ERP permite proteger tanto los datos como los procesos críticos, asegurando que los sistemas sean más seguros y resilientes ante ciberataques. Además, al adoptar este tipo de estándares, las empresas pueden asegurarse de cumplir con las regulaciones de protección de datos y mantener la confianza de sus clientes (Seguros, 2025).

2.3.4 ESTRATEGIAS DE DETECCIÓN Y MITIGACIÓN DE AMENAZAS PERSISTENTES AVANZADAS (APT) EN ERP EMPRESARIALES BASADAS EN ISO/IEC 27032

La detección y mitigación de Amenazas Persistentes Avanzadas (APT) son fundamentales para proteger los sistemas ERP ante ataques sofisticados que pueden permanecer ocultos en el sistema durante largos períodos. El caso de las empresas energéticas en Honduras que fueron víctimas de un ataque APT demuestra lo importante que es contar con estrategias eficaces para detectar y mitigar estas amenazas.

La norma ISO/IEC 27032 ofrece directrices específicas para la protección de sistemas frente a APT, recomendando una combinación de monitoreo constante, auditorías regulares y la implementación de herramientas de seguridad avanzadas como firewalls, sistemas de detección de intrusos (IDS), y técnicas de análisis de comportamiento. Adoptar estas estrategias dentro de un sistema ERP no solo permite la detección temprana de APT, sino que también fortalece la capacidad de respuesta de la organización ante amenazas

persistentes, garantizando que el sistema ERP se mantenga funcional y seguro a pesar de los intentos de ataque (El Diario de Honduras, 2022).

2.3.5 IDENTIFICACIÓN DE ACTIVOS SEGÚN SU CATEGORÍA DE RIESGO Y ESTRATEGIAS DE RESPUESTA Y RECUPERACIÓN ANTE INCIDENTES ALINEADOS CON ITIL V4 PARA MEJORAR LA CONTINUIDAD DEL NEGOCIO EN ERP EMPRESARIALES

La identificación de activos y la clasificación de riesgos son componentes clave para la planificación de la continuidad del negocio, especialmente en el contexto de ITIL V4. El caso de la empresa de logística en Honduras resalta cómo la adopción de ITIL V4 para la gestión de incidentes permitió a la organización clasificar sus activos críticos y establecer estrategias de respuesta ante incidentes de ciberseguridad.

Al alinear los procesos de gestión de incidentes con ITIL V4, las empresas pueden garantizar una respuesta efectiva ante cualquier incidente de ciberseguridad, minimizando el impacto en las operaciones del negocio. Para un sistema ERP, esto significa establecer procedimientos para la rápida recuperación de datos y operaciones, de manera que la interrupción del servicio sea mínima y la seguridad de los datos se mantenga intacta.

ITIL V4 también pone un fuerte énfasis en la mejora continua, lo que permite que las empresas ajusten y optimicen sus estrategias de respuesta y recuperación a medida que evolucionan las amenazas. La adopción de este enfoque mejora la resiliencia operativa y asegura que el sistema ERP siga siendo un activo valioso para la organización (Diario La Prensa, 2023).

2.3.6 EVALUACIÓN DEL IMPACTO DE UN PLAN DE CIBERSEGURIDAD EN SISTEMAS ERP EMPRESARIALES

La evaluación del impacto de un plan de ciberseguridad es esencial para medir la efectividad de las estrategias de protección implementadas, y este es especialmente importante en sistemas ERP, donde se gestionan activos clave de la organización. El Gobierno de Honduras adoptó un plan de ciberseguridad a nivel nacional para proteger sus plataformas electrónicas, incluidas las plataformas ERP utilizadas en sus operaciones administrativas y financieras.

Los KPI establecidos en este plan permitieron medir el éxito de las estrategias de protección, lo que condujo a una reducción significativa de los incidentes de ciberseguridad. La adopción de indicadores de rendimiento alineados con ITIL V4 para evaluar la efectividad de los controles de seguridad en los ERP permitió mejorar las políticas y procedimientos de respuesta ante incidentes, asegurando la continuidad operativa y la protección de la información crítica (Comisión Nacional de Telecomunicaciones (CONATEL) , 2024).

2.4 TEORÍAS DE SUSTENTO

2.4.1 ISO/IEC 27032 - CIBERSEGURIDAD: DIRECTRICES PARA LA GESTIÓN DE RIESGOS CIBERNÉTICOS

La norma **ISO/IEC 27032** proporciona un conjunto de directrices para abordar la ciberseguridad en un contexto global e interconectado, siendo fundamental en la protección de sistemas tecnológicos y la gestión de riesgos cibernéticos en organizaciones que implementan soluciones como los sistemas ERP web. Esta norma, surgida como una necesidad de respuesta a los desafíos de seguridad en el ámbito digital, juega un papel

esencial en la protección de datos, infraestructura crítica y servicios digitales, especialmente en el marco de la Cuarta Revolución Industrial.

ISO/IEC 27032 se centra en cuatro áreas principales de gestión: la seguridad en la infraestructura tecnológica, la protección de datos personales, la gestión de incidentes y la gestión de la continuidad del negocio. Al aplicar estos principios en la gestión de ciberseguridad de los ERP web empresariales, las organizaciones pueden construir una estructura sólida para prevenir y mitigar los riesgos cibernéticos, asegurando la integridad, confidencialidad y disponibilidad de los datos e información procesada por estos sistemas. Además, la norma fomenta un enfoque colaborativo, que incluye a todas las partes interesadas, como proveedores, socios comerciales y clientes, en la implementación de medidas de seguridad.

Relación con la Cuarta Revolución Industrial:

En el contexto de la Cuarta Revolución Industrial, la ISO/IEC 27032 resulta crucial, ya que el aumento de la conectividad y la integración de tecnologías avanzadas como la inteligencia artificial (IA), la nube y el Internet de las Cosas (IoT) expanden significativamente la superficie de ataque en las organizaciones. Los sistemas ERP web, como soluciones clave para la gestión empresarial, están expuestos a amenazas que podrían comprometer operaciones críticas. La norma establece un enfoque integral para mitigar estos riesgos, ayudando a las organizaciones a adaptarse de manera eficiente a un entorno altamente digitalizado.

El desarrollo e implementación de esta norma en los sistemas ERP permite a las organizaciones no solo proteger sus activos y datos, sino también cumplir con regulaciones

internacionales en materia de ciberseguridad, lo cual es esencial para asegurar la confianza de los usuarios y partes interesadas en un entorno tan dinámico y susceptible a amenazas.

2.4.2 ITIL V4 - GESTIÓN DE SERVICIOS DE TI Y SU RELACIÓN CON LA CIBERSEGURIDAD

La metodología ITIL v4, reconocida a nivel mundial por su enfoque en la gestión de servicios de tecnología de la información (TI), ofrece un marco para garantizar que los servicios de TI, incluidos los que apoyan sistemas ERP web empresariales, sean entregados de manera eficiente y segura. ITIL v4 destaca la necesidad de una alineación continua entre los objetivos estratégicos del negocio y los servicios tecnológicos, con un enfoque integral que incluye la gestión de riesgos, incidentes y la protección de los servicios digitales, que son esenciales para mantener la integridad de los sistemas ERP.

El marco de ITIL v4 se basa en un ciclo de vida de servicios que abarca desde el diseño hasta la mejora continua. Entre sus prácticas clave se encuentran la gestión de incidentes, la gestión de problemas y la gestión de la seguridad, las cuales son fundamentales en la implementación de un plan de ciberseguridad. Al adoptar ITIL v4, las organizaciones pueden identificar, responder y mitigar amenazas cibernéticas de manera proactiva, minimizando el impacto en los procesos empresariales.

Relación con la Cuarta Revolución Industrial:

La Cuarta Revolución Industrial ha traído consigo un entorno empresarial mucho más ágil y digitalizado, donde los servicios tecnológicos están profundamente integrados en las operaciones diarias de las organizaciones. La gestión de estos servicios se vuelve aún más crítica en un contexto donde los sistemas ERP web juegan un papel fundamental en la gestión de datos y recursos empresariales. La metodología ITIL v4 se adapta perfectamente a estos

cambios, ya que proporciona un marco flexible y adaptativo para gestionar los servicios de TI de manera efectiva en un entorno digital en constante evolución.

A medida que las organizaciones adoptan tecnologías emergentes como la automatización y la inteligencia artificial, la metodología ITIL v4 se convierte en un aliado crucial para garantizar que los servicios de TI, incluidos los que respaldan los sistemas ERP web, sean seguros, eficientes y alineados con las necesidades estratégicas del negocio.

2.5 METODOLOGÍAS

En este apartado se detallan las metodologías utilizadas en la investigación, estableciendo su aplicabilidad en la gestión de riesgos de ciberseguridad en plataformas ERP empresariales. La selección de estas metodologías responde a la necesidad de contar con un enfoque estructurado y normativo para abordar la seguridad de la información y la gestión de servicios de TI.

2.5.1 ANÁLISIS DE LAS METODOLOGÍAS

1. ISO/IEC 27032

DESCRIPCIÓN Y ALCANCE

ISO/IEC 27032 es un estándar internacional que proporciona directrices para mejorar la ciberseguridad mediante la identificación, prevención, detección y respuesta ante amenazas en el ciberespacio. Fue desarrollado por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) con el objetivo de establecer un marco de referencia para la colaboración entre distintas partes interesadas en la protección del entorno digital, incluyendo empresas, gobiernos y usuarios finales.

El estándar se enfoca en abordar los riesgos emergentes en el ciberespacio, especialmente aquellos asociados con el uso de plataformas interconectadas, como los sistemas de planificación de recursos empresariales (ERP). A diferencia de ISO/IEC 27001, que proporciona un sistema de gestión de la seguridad de la información (SGSI) basado en controles específicos, ISO/IEC 27032 adopta un enfoque más amplio, centrándose en la protección contra amenazas cibernéticas y la resiliencia organizacional en entornos digitales complejos (ISO, 2020).

Principales Componentes de ISO/IEC 27032

El estándar abarca múltiples aspectos de la ciberseguridad, incluyendo:

1. **Gestión de riesgos cibernéticos**: Define un proceso estructurado para evaluar amenazas y vulnerabilidades en sistemas interconectados, incluyendo ERP empresariales.
2. **Protección de activos de información**: Establece controles de seguridad para prevenir accesos no autorizados y garantizar la integridad y disponibilidad de los datos.
3. **Detección de incidentes cibernéticos**: Proporciona lineamientos para la identificación temprana de amenazas y actividades maliciosas.
4. **Respuesta y recuperación ante incidentes**: Describe estrategias para minimizar el impacto de ataques cibernéticos y restaurar la operatividad de los sistemas afectados.

5. **Colaboración entre actores del ciberespacio**: Fomenta la cooperación entre empresas, gobiernos y proveedores de servicios tecnológicos para fortalecer la ciberseguridad global.

Implementación de ISO/IEC 27032 en la tesis

En esta investigación, ISO/IEC 27032 se aplicará como marco de referencia principal para la gestión de riesgos de ciberseguridad en ERP empresariales. La elección de este estándar responde a la necesidad de contar con un enfoque estructurado para abordar los desafíos específicos de seguridad en plataformas empresariales interconectadas.

La aplicación del estándar en la tesis se centrará en los siguientes aspectos:

- **Evaluación de vulnerabilidades en ERP**: Se analizarán los riesgos más comunes que afectan a estos sistemas, accesos no autorizados y exfiltración de datos.
- **Implementación de controles de seguridad**: Se definirán estrategias de mitigación basadas en las directrices de ISO/IEC 27032, incluyendo autenticación multifactor (MFA), cifrado de datos y monitoreo de actividades sospechosas.
- **Gestión de incidentes y respuesta a amenazas**: Se establecerán procedimientos para la detección y respuesta ante ataques, alineados con las mejores prácticas del estándar.
- **Desarrollo de políticas de seguridad cibernética**: Se propondrán lineamientos internos para mejorar la resiliencia organizacional ante amenazas digitales.

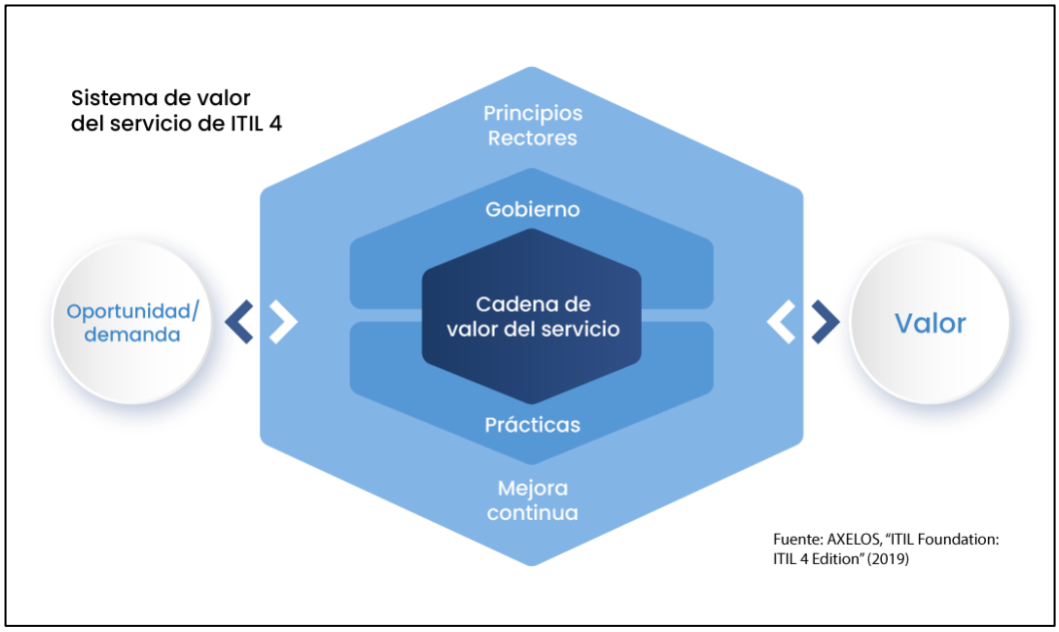
2. ITIL V4

DESCRIPCIÓN Y ALCANCE

ITIL V4 es un marco de referencia internacionalmente reconocido para la gestión de servicios de TI. Su propósito es proporcionar un conjunto de mejores prácticas para la planificación, entrega, operación y mejora de los servicios tecnológicos dentro de una organización.

A diferencia de versiones anteriores, ITIL V4 introduce un enfoque más flexible y alineado con metodologías ágiles, DevOps y Lean, lo que permite una adaptación más eficiente a los cambios tecnológicos y a las necesidades del negocio. La estructura del marco se basa en el "Sistema de Valor del Servicio" (SVS), el cual facilita la entrega continua de valor a los usuarios finales y promueve una cultura de mejora continua dentro de la organización (Axelos, 2019).

Figura 2: Sistema de valor del servicio de ITIL 4.



3. PRINCIPALES COMPONENTES DE ITIL V4

Gobernanza y gestión de servicios TI: Establece roles y responsabilidades claras en la administración de servicios tecnológicos, asegurando que las estrategias de ciberseguridad se alineen con los objetivos del negocio.

Mejora continua: Promueve la optimización constante de los procesos de gestión de TI, permitiendo una adaptación dinámica a nuevas amenazas y vulnerabilidades.

Gestión de incidentes y problemas: Define procedimientos estructurados para la identificación, análisis y resolución de fallos en los sistemas empresariales, minimizando el impacto de incidentes de ciberseguridad.

Gestión de riesgos y cumplimiento: Proporciona un marco para evaluar amenazas y asegurar el cumplimiento de normativas de seguridad dentro de la organización.

Implementación de ITIL V4 en la tesis

El uso de ITIL V4 en esta investigación permitirá estructurar un modelo eficiente de gestión de incidentes y riesgos de ciberseguridad en ERP empresariales. Su implementación abarcará los siguientes aspectos:

Estandarización del proceso de respuesta ante incidentes: Se definirá un marco de acción basado en las mejores prácticas de ITIL V4, asegurando que la respuesta ante incidentes de seguridad sea rápida, efectiva y documentada.

Monitoreo y mejora continua de la seguridad: Se aplicará el modelo de mejora continua de ITIL para evaluar y optimizar de forma constante las estrategias de ciberseguridad en ERP.

Gestión proactiva de amenazas: Se implementarán controles basados en ITIL para anticipar y mitigar riesgos antes de que afecten la operatividad del negocio.

Alineación con la estrategia empresarial: Se asegurarán que las políticas de seguridad se integren con los objetivos organizacionales, promoviendo un enfoque holístico en la gestión de riesgos.

2.5.2 ANTECEDENTES DE LAS METODOLOGÍAS

1. HISTORIA DE LA ISO/IEC 27032

La norma ISO/IEC 27032 surge como respuesta a la creciente problemática de ataques cibernéticos y delitos informáticos. Con el incremento de amenazas digitales, las organizaciones han requerido marcos normativos específicos para fortalecer su ciberseguridad. Su primera publicación en 2012 marcó un hito en la gestión de riesgos en el ciberespacio, proporcionando directrices que complementan la gestión de la seguridad de la información establecida en la norma ISO/IEC 27001.

A lo largo de los años, ISO/IEC 27032 ha evolucionado para adaptarse a los desafíos emergentes en la seguridad digital, abordando aspectos clave como la protección contra amenazas avanzadas persistentes (APT), la gestión de vulnerabilidades y la colaboración entre distintos sectores para garantizar la seguridad en línea.

2. EVOLUCIÓN DE ITIL HASTA LA VERSIÓN V4

ITIL fue desarrollado inicialmente en la década de 1980 por el gobierno del Reino Unido como un conjunto de buenas prácticas para la gestión de servicios de TI. Su propósito era mejorar la calidad de los servicios tecnológicos en las organizaciones mediante la adopción de procesos estructurados y eficientes.

Desde su primera versión, ITIL ha pasado por varias actualizaciones para adaptarse a las nuevas tendencias en gestión de TI. La versión ITIL V4, publicada en 2019, introduce conceptos modernos como la integración con metodologías ágiles, la automatización de procesos y la entrega continua de valor a los usuarios. Esta evolución ha permitido que ITIL se mantenga relevante en entornos empresariales dinámicos y altamente digitalizados.

2.5.3 ANÁLISIS CRÍTICO DE LAS METODOLOGÍAS APLICACIÓN DE ISO/IEC 27032 EN LA INVESTIGACIÓN

La presente investigación adopta ISO/IEC 27032 como un marco fundamental para la gestión de riesgos de ciberseguridad en ERP empresariales. Esta norma permitirá establecer un enfoque estructurado para la identificación de amenazas, la implementación de controles preventivos y la respuesta a incidentes en los sistemas de información de la organización.

En particular, su aplicación facilitará:

- La identificación de vulnerabilidades en plataformas ERP utilizadas en entornos empresariales.
- El diseño de estrategias de mitigación de riesgos basadas en estándares internacionales.
- La implementación de un modelo de cooperación entre usuarios, administradores de sistemas y proveedores de software para mejorar la seguridad.
- La definición de directrices de respuesta ante incidentes, garantizando la continuidad del negocio y la minimización de impactos.

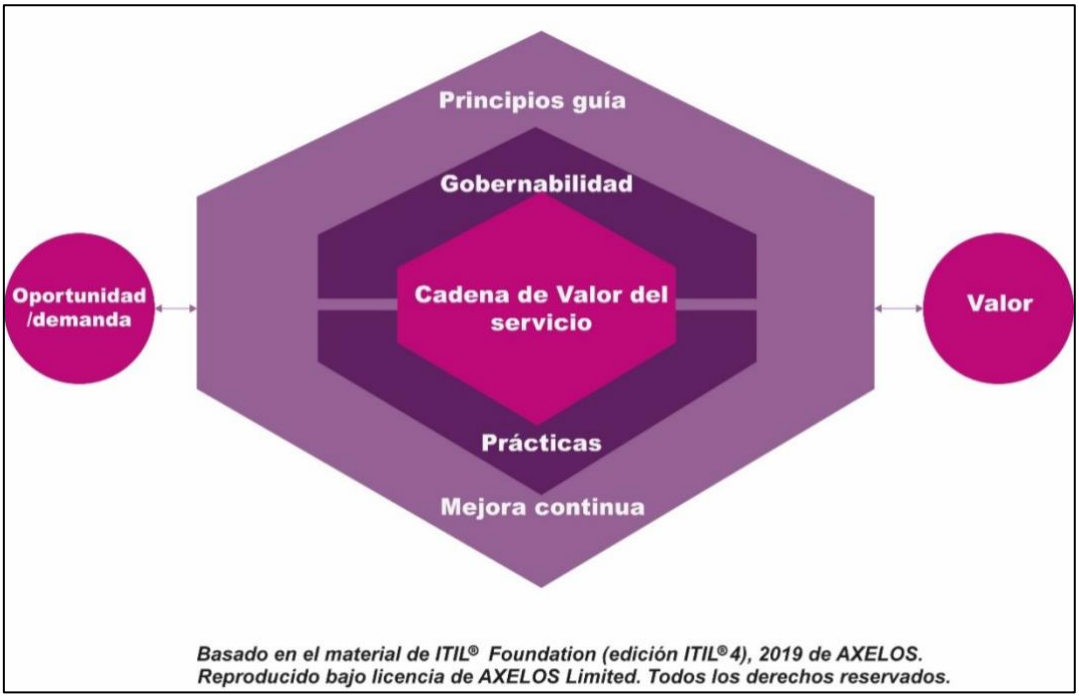
2.5.4 USO DE ITIL V4 EN LA INVESTIGACIÓN

ITIL V4 será utilizado en la presente investigación como un marco de referencia para la gestión de incidentes de seguridad en ERP empresariales. Su aplicación permitirá:

- Mejorar la gestión de incidentes de ciberseguridad mediante procesos estructurados y estandarizados.
- Facilitar la integración de mejores prácticas en la operación de plataformas ERP, asegurando la alineación con los objetivos organizacionales.
- Optimizar la respuesta ante eventos de seguridad, minimizando tiempos de recuperación y reduciendo el impacto en las operaciones empresariales.

ITIL V4 contempla un enfoque integral para la gestión de riesgos asociados a la ciberseguridad, facilitando la identificación, evaluación y mitigación de amenazas que puedan comprometer la continuidad, disponibilidad e integridad del sistema ERP. La incorporación de prácticas sistemáticas de gestión de riesgos permite anticipar vulnerabilidades y establecer controles eficaces que refuercen la resiliencia organizacional ante posibles incidentes, complementando así la gestión de incidentes y el ciclo de mejora continua implementados en esta investigación.

Figura 3: Principios Guía ITIL 4.



1. APLICACIÓN AL PROYECTO

En este proyecto ITIL V4 será aplicado como marco fundamental para establecer una gestión robusta y estratégica de la seguridad y riesgos del ERP web empresarial. Se aprovecharán prácticas claves de ITIL V4 como la gestión del cambio, gestión de incidentes, gestión del riesgo y mejora continua. Estas prácticas permitirán asegurar que las medidas específicas de ciberseguridad derivadas de ISO/IEC 27032 se implementen sistemáticamente y permanezcan actualizadas frente a amenazas emergentes. Además, ITIL V4 facilitará la integración estratégica entre las iniciativas digitales y las operaciones cotidianas del ERP, fortaleciendo integralmente la resiliencia cibernética de la organización (AXELOS, 2020).

2. HERRAMIENTAS ESPECÍFICAS

Matriz RACI: Clarifica roles y responsabilidades, facilitando la comunicación efectiva, resolución de conflictos y optimización en la toma de decisiones durante la gestión operativa del ERP web empresarial (AXELOS, 2020).

Acuerdos de Nivel de Servicio (SLA): Documentos formales que definen claramente las expectativas y estándares requeridos en términos de disponibilidad, integridad y continuidad operativa del ERP, garantizando el cumplimiento efectivo y confiable de los servicios

Sistema de Registro y Seguimiento de Incidentes: Facilita una gestión integral y efectiva de incidentes al proporcionar capacidades para registrar, analizar y resolver rápidamente cualquier problema relacionado con la seguridad y operatividad del ERP

Ciclo PDCA (Plan-Do-Check-Act): Marco metodológico para implementar mejoras continuas en la gestión de seguridad, garantizando una adaptación constante y efectiva a nuevas amenazas y vulnerabilidades (AXELOS, 2020).

3. ISO/IEC 27032 DEFINICIÓN

La norma ISO/IEC 27032 proporciona directrices específicas y prácticas recomendadas para la gestión de la ciberseguridad, enfocándose especialmente en la protección efectiva del ciberespacio, incluyendo la identificación proactiva, prevención y respuesta eficaz ante amenazas cibernéticas que afectan sistemas críticos expuestos en internet, como los ERP web empresariales (ISO/IEC, 2023).

4. ANTECEDENTES

ISO/IEC 27032 fue publicada originalmente en 2012 por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), con el propósito de abordar el rápido incremento y sofisticación de ciberamenazas. La actualización más reciente en 2023 incorpora directrices para la gestión avanzada de seguridad en plataformas de computación en la nube y fortalece las recomendaciones para la protección integral de infraestructuras tecnológicas críticas (ISO/IEC, 2023).

5. APLICACIÓN AL PROYECTO

La metodología ISO/IEC 27032 será empleada en esta investigación de maestría para gestionar específicamente los riesgos cibernéticos asociados con el ERP web empresarial. Sus recomendaciones permitirán identificar, evaluar y mitigar amenazas mediante controles técnicos y administrativos rigurosos. Esto asegurará la protección integral del ERP, fortaleciendo la resiliencia organizacional frente a incidentes cibernéticos y manteniendo la continuidad operativa.

2.6 HERRAMIENTAS ESPECÍFICAS

2.6.1 ANÁLISIS DE VULNERABILIDADES WEB

Utilización de herramientas técnicas como OWASP ZAP y Nessus, fundamentales para la detección proactiva de vulnerabilidades en el ERP, asegurando una intervención oportuna y efectiva ante brechas potenciales de seguridad (OWASP Foundation, 2023; Tenable, 2023).

2.6.2 ANÁLISIS DE IMPACTO AL NEGOCIO (BIA)

Herramienta clave para evaluar con precisión el impacto potencial de amenazas cibernéticas sobre activos críticos del ERP, facilitando una planificación estratégica y efectiva en la gestión de riesgos (ISO/IEC, 2023).

2.6.3 PLANES DE RESPUESTA ANTE INCIDENTES CIBERNÉTICOS

Proporcionan protocolos estructurados y detallados para la gestión efectiva y coordinada de incidentes, asegurando tiempos de respuesta ágiles y una mitigación rápida del impacto operacional (ISO/IEC, 2023).

2.6.4 MONITOREO PROACTIVO Y GESTIÓN DE EVENTOS DE SEGURIDAD

Implementación de soluciones tecnológicas avanzadas como Splunk e IBM QRadar, capaces de monitorear en tiempo real, detectar amenazas de manera temprana y proporcionar alertas oportunas que permiten una respuesta inmediata y efectiva frente a eventos de seguridad cibernética (Splunk, 2023; IBM, 2023).

2.7 CONCEPTUALIZACIÓN

El presente estudio aborda la implementación de un Plan de Ciberseguridad para la Gestión de Riesgos en ERP Empresariales, basado en las normas ISO/IEC 27032 e ITIL v4. Para ello, se establecen conceptos clave que permiten comprender los fundamentos teóricos y metodológicos aplicados en la investigación.

- **CIBERSEGURIDAD**

La ciberseguridad se define como el conjunto de estrategias, tecnologías, procesos y controles diseñados para proteger sistemas informáticos, redes, programas y datos contra

ataques, daños o accesos no autorizados (ISO/IEC 27032, 2012). Su enfoque principal es la protección de la información en entornos digitales, minimizando riesgos de vulnerabilidad.

- **GESTIÓN DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN**

Es el proceso de identificación, análisis y mitigación de riesgos que afectan la seguridad de los datos empresariales. En esta tesis, se implementa mediante el estándar ISO/IEC 27032, que proporciona directrices sobre cómo abordar las amenazas cibernéticas en infraestructuras empresariales.

- **ERP (ENTERPRISE RESOURCE PLANNING) WEB EMPRESARIALES**

Los ERP web son plataformas integradas que permiten gestionar procesos empresariales en la nube o en entornos web. Si bien ofrecen accesibilidad y escalabilidad, también presentan desafíos en materia de ciberseguridad, por lo que requieren estrategias robustas para proteger la información.

- **ISO/IEC 27032 - DIRECTRICES PARA LA CIBERSEGURIDAD**

La norma ISO/IEC 27032 establece un marco de referencia para la protección del ciberespacio, abordando amenazas y proporcionando estrategias de defensa. En esta investigación, se utiliza para definir medidas de seguridad aplicadas a ERP empresariales, asegurando la integridad y disponibilidad de los datos.

- **ITIL V4 - GESTIÓN DE SERVICIOS DE TI**

El marco ITIL v4 proporciona mejores prácticas para la gestión eficiente de servicios tecnológicos. Su implementación en esta tesis se enfoca en la gestión de incidentes y la seguridad operativa dentro del ERP empresarial, asegurando un enfoque estructurado en la protección de la infraestructura TI.

- **SEGURIDAD EN LA NUBE**

Dado que los ERP web operan en entornos cloud, la seguridad en la nube es un aspecto clave en esta investigación. Se consideran mecanismos de protección como cifrado de datos, autenticación multifactor y auditorías de seguridad.

- **PROTECCIÓN DE DATOS PERSONALES**

En el contexto hondureño, la protección de datos está regulada por la Ley de Protección de Datos Personales y la Ley de Comercio Electrónico. Este estudio analiza cómo estas normativas influyen en la seguridad de los ERP empresariales.

- **RESPUESTA ANTE INCIDENTES DE SEGURIDAD**

La capacidad de una empresa para gestionar incidentes de seguridad es fundamental para garantizar la continuidad del negocio. La norma ISO/IEC 27032 establece procedimientos específicos para mitigar los efectos de ciberataques en infraestructuras empresariales.

2.8 MARCO LEGAL

El marco legal establece las regulaciones internacionales y nacionales aplicables a la ciberseguridad en ERP empresariales. A continuación, se presenta un análisis de los principales estándares y normativas que rigen esta investigación.

2.8.1 MARCO LEGAL INTERNACIONAL

El marco internacional de referencia para esta investigación está basado en las siguientes normativas:

- ISO/IEC 27032:2012 – Directrices para la Ciberseguridad, establece las mejores prácticas para la seguridad en entornos digitales.

- ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información (SGSI), que define la estructura para la protección de los activos de información.
- ITIL v4 (2019) – Gestión de servicios de TI, con énfasis en la seguridad de la información y gestión de incidentes.

Estas normativas proporcionan el marco metodológico en el cual se basa esta tesis para definir estrategias de mitigación de riesgos en ERP web empresariales.

2.8.2 MARCO LEGAL NACIONAL (HONDURAS)

En el contexto hondureño, las regulaciones que rigen la ciberseguridad y la protección de datos son las siguientes:

- Código Penal de Honduras (Decreto 130-2017): Tipifica los delitos informáticos y establece sanciones para actividades como el acceso ilícito a sistemas y el robo de información, como se describe en el párrafo XXII de Seguridad de las redes y de los sistemas informáticos, desde el Articulo 398 al Artículo 405.
- Ley de Comercio Electrónico (Decreto 149-2022): Regula el comercio digital y la seguridad en transacciones electrónicas.
- Ley de Protección de Datos Personales (Decreto 54-2019): Establece los principios y obligaciones para la protección de datos en plataformas digitales.
- Reglamento de Seguridad de la Información en Instituciones Financieras (CNBS, Resolución 1062/23-2020): Define lineamientos de ciberseguridad para el sector financiero, aplicables a ERP de bancos y empresas del sector.

En la investigación, se considera el impacto de estas regulaciones en la seguridad de los sistemas ERP en Honduras, asegurando el cumplimiento de estándares nacionales e internacionales.

2.8.3 RELACIÓN CON EL ANÁLISIS DEL MACROENTORNO Y MICROENTORNO

En el capítulo 2, se ha abordado el marco legal internacional en el análisis del macroentorno, destacando el papel de la ISO/IEC 27032 e ITIL v4 como estándares globales de referencia. Por lo tanto, en esta sección se enfatiza la normativa nacional de Honduras, asegurando la integración de ambos marcos regulatorios en la investigación.

CAPÍTULO III. METODOLOGÍA DE LA INVESTIGACIÓN

3.1. ENFOQUE DE LA INVESTIGACIÓN

El enfoque metodológico utilizado en esta investigación es mixto, ya que combina métodos cualitativos y cuantitativos para analizar la situación actual de ciberseguridad en los ERP empresariales y proponer un plan de gestión de riesgos basado en estándares internacionales como ISO/IEC 27032 e ITIL V4. La combinación de ambos enfoques permite obtener un entendimiento más completo y profundo del fenómeno estudiado, aprovechando la rigurosidad de los datos numéricos y la riqueza del análisis contextual.

3.1.1. ENFOQUE CUANTITATIVO

En esta investigación, el componente cuantitativo permitirá:

- Evaluar el nivel de cumplimiento de los ERP con los estándares de ciberseguridad.
- Cuantificar el número y tipo de vulnerabilidades detectadas en los sistemas ERP.
- Analizar la percepción de los usuarios sobre la seguridad de los sistemas mediante encuestas estructuradas.
- Aplicar pruebas de auditoría a los sistemas ERP para obtener métricas específicas sobre riesgos y cumplimiento normativo.

3.1.2. ENFOQUE CUALITATIVO

En esta investigación, el componente cualitativo contribuirá a:

- Identificar las principales preocupaciones y desafíos de los profesionales de TI en la gestión de ciberseguridad en ERP.
- Analizar casos de estudio de empresas que han implementado medidas de seguridad en sus sistemas ERP.

- Evaluar la percepción de los responsables de TI sobre las estrategias actuales de protección y respuesta ante incidentes.
- Interpretar las respuestas de entrevistas a expertos en ciberseguridad para conocer las mejores prácticas y tendencias en la protección de ERP.

3.1.3. JUSTIFICACIÓN DEL ENFOQUE MIXTO

El uso de un enfoque mixto en esta investigación es fundamental para abordar la problemática de manera integral. Hernández et al. (2022) señalan que este enfoque es ideal cuando se requiere:

- Combinar la objetividad del análisis numérico con la subjetividad del análisis interpretativo.
- Obtener una visión holística del fenómeno estudiado.
- Validar los hallazgos de un método con los del otro, incrementando la confiabilidad y validez de la investigación.

En el contexto de este estudio, el enfoque mixto permite analizar tanto el comportamiento cuantificable de los riesgos de ciberseguridad en los ERP como las percepciones y estrategias organizacionales que afectan la gestión de estos riesgos. Además, el enfoque mixto facilita una triangulación de datos, es decir, la combinación de múltiples fuentes de información (encuestas, auditorías, entrevistas y revisión documental) para generar conclusiones más robustas y fundamentadas.

3.1.4. APLICACIÓN DEL ENFOQUE MIXTO EN LA INVESTIGACIÓN

Etapa de la Investigación	Método Cuantitativo	Método Cualitativo
Análisis de la situación actual de ciberseguridad en ERP	Encuestas a la empresa TiviTrace sobre el cumplimiento de estándares	Entrevistas con personal de ciberseguridad en TiviTrace
Identificación de vulnerabilidades y riesgos	Auditorías de seguridad y análisis estadístico de incidentes	Revisión de documentación de seguridad en la empresa TiviTrace.
Propuesta de plan de ciberseguridad	Modelado de impacto de riesgos en base a datos recopilados	Análisis de mejores prácticas y estrategias de mitigación

3.2. ALCANCE DE LA INVESTIGACIÓN

3.2.1. ALCANCE EXPLORATORIO

En su fase inicial, el estudio es exploratorio, ya que busca identificar los principales riesgos de ciberseguridad en ERP empresariales dentro de Honduras. De acuerdo con Sampieri, Collado y Lucio (2020), la investigación exploratoria es apropiada cuando existe poca información previa y se requiere construir un marco teórico preliminar. En este sentido, se recopilarán datos sobre las vulnerabilidades más comunes y las prácticas de seguridad adoptadas por las organizaciones.

3.2.2. ALCANCE DESCRIPTIVO

A medida que la investigación avanza, adquiere un carácter descriptivo, ya que detalla las vulnerabilidades encontradas en los ERP empresariales y las clasifica de acuerdo con los estándares ISO/IEC 27032 e ITIL V4. Además, tiene un enfoque explicativo, al analizar las posibles causas subyacentes de estas vulnerabilidades y sus impactos en la seguridad de la información.

Según Hernández et al. (2022), la investigación descriptiva permite caracterizar fenómenos mediante la recopilación de información estructurada, mientras que la investigación explicativa busca comprender las razones que los originan. Este enfoque combinado permite identificar los riesgos, explicar cómo se relacionan con deficiencias en la gestión de ciberseguridad y proponer medidas para mitigarlos.

3.3. DISEÑO

3.3.1. POBLACIÓN Y GRUPO DE ESTUDIO

La población objeto de estudio en esta investigación está conformada por 7 personas pertenecientes a la empresa TiviTrace, en la cual se centra exclusivamente este análisis. Esta población se divide en dos grupos principales: 5 integrantes del área de Tecnologías de la Información y Seguridad Informática (4 ingenieros y 1 gerente de TI), y 2 usuarios operativos del sistema ERP, que representan la totalidad de los colaboradores que utilizan dicha plataforma dentro de la organización.

La inclusión de ambos grupos responde a la necesidad de obtener una visión integral sobre la gestión de ciberseguridad en el contexto del sistema ERP, considerando tanto la perspectiva técnica (relacionada con la implementación, mantenimiento y protección del sistema), como la perspectiva operativa (relacionada con el uso diario y la interacción directa con el ERP).

Dado que TiviTrace únicamente cuenta con 2 usuarios activos del ERP, se consideró pertinente que el estudio se centrara en ellos como fuente directa para obtener datos relevantes sobre el uso, vulnerabilidades percibidas y prácticas cotidianas asociadas al sistema. A su vez, el personal del área de TI permite comprender la postura organizacional, las medidas implementadas y los riesgos técnicos existentes.

Según Sampieri et al. (2014), definir claramente la población del estudio es fundamental para identificar de forma precisa el universo de análisis y garantizar la validez de los hallazgos.

3.4. OPERACIONALIZACIÓN DE LAS VARIABLES

La operacionalización de las variables permite convertir conceptos abstractos en indicadores medibles, facilitando su evaluación empírica. En esta investigación, se identifican dos variables principales:

- Variable Independiente (VI): Nivel de ciberseguridad en sistemas ERP.
- Variable Dependiente (VD): Efectividad del plan integral de ciberseguridad.

Cada variable se descompone en dimensiones e indicadores precisos, con definiciones conceptuales y operacionales.

3.5. MATRIZ DE OPERACIONALIZACIÓN DE LAS VARIABLES

Variable	Definición Conceptual	Dimensiones	Indicadores	Definición Operacional / Escala	Instrumento
Nivel de ciberseguridad en ERP (VI)	Grado de cumplimiento del ERP con estándares de ciberseguridad, reflejando capacidad de resistir amenazas.	Cumplimiento de estándares	Porcentaje de Controles ISO/IEC 27032 implementados	Porcentaje de controles aplicados (0-100%)	Lista de verificación (Anexo A)
		Gestión de incidentes	Protocolo ITIL V4 implementado; Tiempo promedio de resolución	Presencia (Sí/No); Tiempo en días	Entrevista estructurada (Anexo B); Registro de incidencias
		Vulnerabilidades técnicas	Número de vulnerabilidades críticas detectadas	Conteo absoluto en auditoría documental políticas de seguridad	Informe técnico (Datos internos)
		Concientización del personal	Porcentaje de personal capacitado en ciberseguridad	Porcentaje de empleados	Registro de capacitación (Datos internos)

				capacitados el último año	
Efectividad del plan de ciberseguridad (VD)	Grado en que el plan basado en ISO 27032 e ITIL V4 reduce ciberataques y mejora la gestión de riesgos.	Reducción de incidentes	Porcentaje de incidentes de seguridad (pre vs post plan)	Diferencia porcentual en incidentes trimestrales	Registro de incidentes (Antes/Después)
		Mejora en controles	Nivel de madurez de controles implementados	Escala de 1 a 5 (evaluación de expertos)	Cuestionario a expertos (Anexo D)
		Continuidad del negocio	Tiempo de recuperación ante incidentes críticos	Horas promedio para restaurar operaciones	Registro de incidentes / Plan de contingencia
		Percepción de seguridad	Puntaje de confianza en seguridad del ERP	Promedio encuestas Likert 1-5	Encuesta Likert a TI (Anexo E)

3.6. TÉCNICAS, INSTRUMENTOS, PROCEDIMIENTO Y PLAN DE ANÁLISIS

3.6.1 TÉCNICAS

Se adoptó un enfoque metodológico mixto, combinando técnicas cuantitativas y cualitativas para abordar el fenómeno de estudio desde una perspectiva integral. Se utilizaron encuestas estructuradas para recopilar datos medibles sobre la percepción y las prácticas de seguridad; entrevistas semiestructuradas para profundizar en la experiencia de los expertos; observación directa del entorno tecnológico para corroborar prácticas operativas; y auditorías documentales de políticas y procedimientos de seguridad existentes. Asimismo, se aplicaron herramientas de análisis estratégico como el FODA, el diagrama de Ishikawa y una matriz de riesgos basada en la norma ISO/IEC 27032, con el fin de identificar causas raíz, vulnerabilidades y prioridades de mitigación. La triangulación de estas técnicas fortaleció la validez y la confiabilidad de los hallazgos, siguiendo el modelo de diseño mixto explicativo secuencial (Creswell & Plano Clark, 2018).

3.6.2 INSTRUMENTOS

Instrumentos Para implementar las técnicas descritas se diseñaron y validaron los siguientes instrumentos:

- **Cuestionario estructurado (Anexo E):** Incluye preguntas cerradas y escalas Likert dirigidas al personal de TI para evaluar la percepción y cumplimiento de medidas de seguridad.
- **Guía de entrevista semiestructurada (Anexo B):** Conformada por preguntas abiertas alineadas a los objetivos del estudio, permite profundizar en experiencias y desafíos de seguridad.
- **Lista de verificación ISO 27032 (Anexo A):** Herramienta de cotejo para revisar la implementación de controles de seguridad según la norma ISO/IEC 27032.
- **Registros institucionales internos:** Documentos como reportes de incidentes, registros de capacitación, SLA, entre otros, que proporcionan datos adicionales para corroborar los resultados.
- **Diagrama de Ishikawa:** Herramienta visual que identifica y organiza las posibles causas de problemas o vulnerabilidades en la ciberseguridad del ERP, facilitando el análisis estructurado de factores técnicos, humanos y organizacionales.

- **FODA:** Análisis estratégico que evalúa fortalezas, oportunidades, debilidades y amenazas relacionadas con la gestión de seguridad en el ERP, apoyando la identificación de áreas de mejora y planificación de acciones.
- **Matriz de riesgo:** Instrumento que clasifica y prioriza riesgos identificados según su probabilidad e impacto, ayudando a focalizar esfuerzos en las amenazas más críticas para la seguridad del ERP.

3.7. PROCEDIMIENTOS

Los procedimientos seguidos en la investigación abarcaron desde la planificación hasta la elaboración de informes finales. Dado que se emplearon diferentes instrumentos de recolección de datos (cuestionarios, entrevistas, observación y auditorías documentales), se estableció un proceso de aplicación y análisis específico para cada uno, de la siguiente forma:

1. Autorización ética

   Solicitud formal a la organización y firma de consentimientos informados, tanto para la aplicación de cuestionarios y entrevistas como para la realización de observaciones y auditorías en los sistemas de la organización.

2. Procedimientos para cada instrumento

   2.1. Cuestionarios

   - Aplicación: Se distribuyeron los cuestionarios a los participantes mediante un formulario en línea Google Forms explicando su propósito y asegurando la confidencialidad de las respuestas.

- Análisis: Se codificaron y tabularon las respuestas en Microsoft Excel. En el caso de las preguntas abiertas, se realizó un análisis de contenido para agrupar y categorizar la información de acuerdo con las dimensiones de la investigación.

2.2. Entrevistas

- Aplicación: Se efectuaron entrevistas semiestructuradas con personal de TI, responsables de seguridad y usuarios clave. Para ello, se empleó una guía con preguntas enfocadas en la gestión de ciberseguridad y la experiencia con los sistemas ERP.
- Análisis: Las entrevistas se transcribieron textualmente y se codificaron por categorías empleando un software de análisis cualitativo a continuación, se agruparon los hallazgos en torno a temas clave identificados en la literatura y en los objetivos de la investigación.

2.3. Observación del entorno

- Aplicación: Se llevó a cabo una observación directa de los procesos y del uso de los sistemas, registrando prácticas cotidianas, interacciones y posibles brechas de seguridad en un diario de campo.
- Análisis: Se revisaron las notas y se clasificaron los hallazgos en categorías preliminares, contrastando dicha información con los datos obtenidos en los cuestionarios y las entrevistas.

2.4. Auditorías en entornos controlados

- Aplicación: Se realizaron auditorías técnicas en la infraestructura de TI y las redes de la organización, revisando configuraciones y procedimientos de seguridad.

Para ello, se siguieron guías de verificación basadas en las mejores prácticas de ISO/IEC 27032 e ITIL V4.

- Análisis: Se compararon los resultados de las auditorías con los estándares establecidos, identificando brechas y fortalezas. Posteriormente, se consolidaron en un informe de hallazgos técnicos, que sirvió de base para las recomendaciones finales.

3. Organización y verificación de datos
    - Al finalizar la recolección, se procedió a codificar la información, transcribir las entrevistas, sistematizar los datos provenientes de la observación y consolidar los resultados de las auditorías. Este paso fue esencial para asegurar la calidad y coherencia de la base de datos final.

4. Triangulación metodológica
    - Con el fin de asegurar la consistencia de la información, se integraron de manera cruzada los datos de cuestionarios, entrevistas, observación y auditorías. Mediante este ejercicio de triangulación, se pudieron confirmar hallazgos, identificar posibles discrepancias y fundamentar las conclusiones finales.

5. Elaboración de reportes
    - Finalmente, se presentaron los hallazgos clave a la organización como parte del compromiso ético y se elaboraron los capítulos de resultados de la tesis. En dichos reportes se incluyeron recomendaciones específicas basadas en los resultados consolidados de cada uno de los instrumentos.

3.8. PLAN DE ANÁLISIS

- Cuantitativo: Estadística descriptiva (frecuencias, promedios) y comparaciones pre-post para evaluar la mejora tras la implementación del plan. En función del tamaño de muestra (N=5), no se aplicaron pruebas inferenciales, pero se exploraron correlaciones indicativas.
- Cualitativo: Análisis de contenido temático (Braun & Clarke, 2006) aplicado a transcripciones y observaciones para identificar patrones narrativos.
- Integración mixta: Mediante triangulación convergente se relacionaron resultados cuantitativos y cualitativos, permitiendo una interpretación más rica y contextualizada de los hallazgos.

3.9. FUENTES DE INFORMACIÓN

3.9.1 FUENTES PRIMARIAS

Incluyen todos los datos originales generados por el investigador en el marco de este estudio: encuestas, entrevistas, observaciones, auditorías y registros técnicos recolectados directamente en la empresa objeto de estudio.

3.9.2 FUENTES SECUNDARIAS

Comprenden la literatura científica consultada, incluyendo libros, artículos académicos, normas internacionales (ISO/IEC 27032, ITIL V4), informes técnicos y documentación institucional preexistente. Todas las fuentes fueron citadas conforme a las normas APA séptima edición.

3.10. MATRIZ DE CONGRUENCIA METODOLÓGICA

La matriz de congruencia metodológica asegura que los elementos del estudio estén alineados entre sí. En ella se relacionan los objetivos específicos, las preguntas de investigación, las variables, los instrumentos de recolección de datos y el tipo de análisis a realizar. Esto permite mantener coherencia en el desarrollo del trabajo y facilita la conexión entre las distintas partes de la tesis.

Pregunta de Investigación	Objetivo Especifico	Enfoque Metodológico	Variables	Dimensiones	Indicadores	Instrumentos
¿Qué riesgos de ciberseguridad afectan al sistema ERP y cómo se clasifican?	Identificar y clasificar los riesgos de ciberseguridad en ERP	Cualitativa	Nivel de ciberseguridad	Tipos de amenazas, Áreas del sistema afectadas	Tipos de vulnerabilidad, Impacto potencial, Probabilidad de explotación	Herramientas técnicas, Guía de entrevista, Lista de verificación
¿Qué controles de ISO/IEC 27032 están implementados en la empresa?	Analizar la aplicabilidad de ISO/IEC 27032	Mixta	Nivel de ciberseguridad	Ámbitos de control, Grado de cumplimiento	Porcentaje de implementación de controles ISO	Cuestionario estructurado, Lista de verificación
¿Qué controles podrían aplicarse para mitigar APT?	Definir estrategias de detección y mitigación de APT	Cualitativa	Nivel de ciberseguridad	Prevención, Detección, Respuesta	Identificación de controles ISO, Potencial de mitigación para APT	Normas ISO, Guía de entrevista
¿Qué medidas existen para garantizar continuidad?	Categorizar activos según riesgo y definir respuestas	Mixta	Nivel de ciberseguridad, Continuidad de negocio	Clasificación de activos, Estrategias de continuidad, Tiempo de recuperación	Tipo de estrategia, Tiempo de recuperación, Eficiencia en respuesta	Cuestionario, Registros, Guía de entrevista

¿Ha mejorado la seguridad tras aplicar el plan?	Evaluar el impacto del plan de ciberseguridad	Cuantitativa	Efectividad del plan	Reducción de incidentes, Percepción de seguridad	Número de incidentes antes/después, Percepción de seguridad tras implementación del plan	Cuestionario, Registro de incidentes, Guía de entrevista

Esta matriz evidencia cómo cada objetivo se operacionaliza y se responde mediante datos válidos y métodos apropiados, garantizando la coherencia metodológica del estudio.

CAPÍTULO IV. RESULTADOS Y ANÁLISIS

En este capítulo se presentan y analizan los resultados obtenidos a partir de los tres instrumentos de recolección de datos aplicados durante la investigación. La Encuesta sobre Ciberseguridad en el uso del ERP Empresarial fue respondida por 2 usuarios del sistema; la Lista de Verificación ISO/IEC 27032 para Sistemas ERP, por 5 colaboradores con conocimiento técnico-administrativo del entorno ERP; y la Guía de Entrevista Semiestructurada sobre Ciberseguridad en ERP Empresariales, también fue aplicada a 5 participantes clave.

La integración de estos instrumentos permitió obtener una visión amplia y detallada del estado actual de la ciberseguridad en los sistemas ERP de la organización, considerando tanto las prácticas implementadas como las percepciones del personal. Los hallazgos se organizan en función de los objetivos específicos planteados, permitiendo evaluar el nivel de cumplimiento de buenas prácticas, identificar debilidades en los controles existentes y detectar oportunidades de mejora. Este análisis se alinea con los marcos ISO/IEC 27032 e ITIL V4, aportando evidencia concreta sobre su aplicabilidad en entornos empresariales reales y proporcionando la base para la formulación de un plan de ciberseguridad integral.

4.1 RECOLECCIÓN Y ANÁLISIS DE DATOS

Los instrumentos de recolección de datos fueron validados mediante el juicio de expertos, contando con la asesoría del maestro guía M. Sc. Jorge Maradiaga. El objetivo de este proceso fue asegurar que los instrumentos fueran detallados, claros y comprensibles para los entrevistados, lo que permitiría obtener información relevante y valiosa para la investigación.

4.1.1 IDENTIFICACIÓN Y CLASIFICACIÓN DE RIESGOS DE CIBERSEGURIDAD EN ERP EMPRESARIALES

Con el propósito de identificar y clasificar los riesgos de ciberseguridad en ERP empresariales mediante un análisis de vulnerabilidades y auditorías de seguridad se aplicó un enfoque mixto que combina tres fuentes de evidencia complementarias. La Figura 4 de la distribución muestra la arquitectura general del método y cómo cada componente se vincula con los resultados (Figs. 4-17, Tabla 1, Tabla 5 y Figs. 18-19-20).

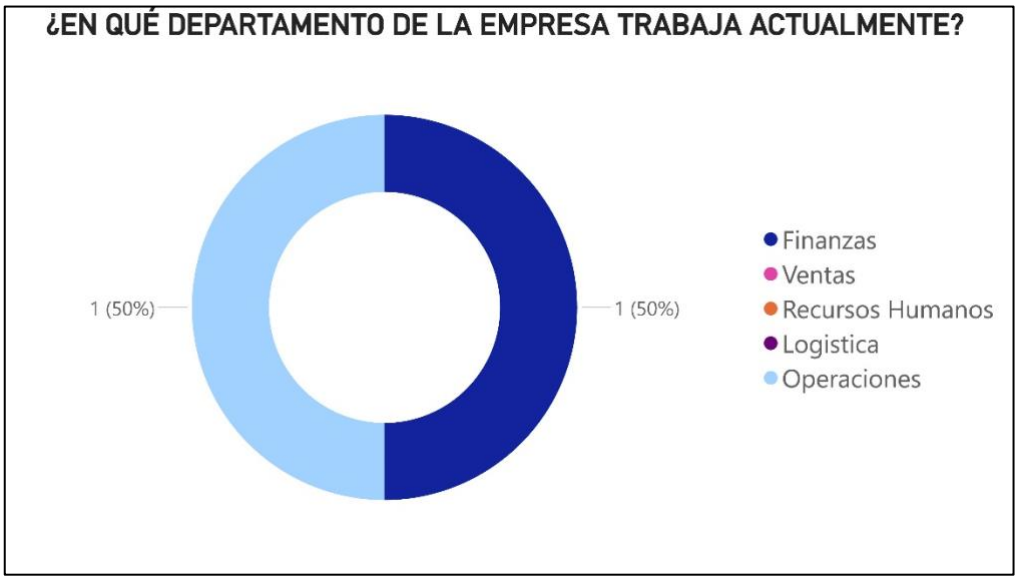
Componente	Descripción	Producto Asociado
a) Instrumentos socio-organizativos	Encuestas, entrevistas y listas de verificación aplicadas a usuarios clave y responsables de TI.	Figs. 4–17 y sus respectivos análisis.
b) Análisis de causas raíz (Diagrama de Ishikawa)	Desglose de las causas del riesgo crítico de phishing clasificadas en Personas, Procesos, Tecnología, Entorno, Recursos y Políticas a partir de los hallazgos.	Análisis de Ishikawa (Fig. 18)
c) Auditoría documental de políticas de seguridad	Revisión formal de políticas, registros y evidencias, conforme a ISO/IEC 27032.	6 no-conformidades y 4 observaciones (Tabla 1).
d) Análisis FODA (visión estratégica)	Síntesis macro de factores internos (Fortalezas-Debilidades) y externos (Oportunidades-Amenazas) derivados de (a) y (b).	Fig. 19: Matriz FODA
e) Matriz de Riesgos Empresarial (P × I)	Evaluación de riesgos identificados según su probabilidad e impacto, sin considerar medidas mitigantes.	Tabla 5 y mapa de calor (Fig. 20).

Se ejecutó una auditoría documental rigurosa, triangulada con las declaraciones obtenidas mediante los instrumentos socio-organizativos, lo que permitió construir una caracterización válida del riesgo a nivel organizacional, humano y tecnológico.

4.1.2 RESULTADOS DE LOS INSTRUMENTOS SOCIO-ORGANIZATIVOS

Se presentan los resultados derivados de los cuestionarios y entrevistas. Cada indicador se analiza en su respectivo epígrafe para contextualizar la exposición al riesgo desde el punto de vista humano, organizativo y procedimental.

Figura 4: Distribución de departamentos de los usuarios del ERP.



Nota: Elaboración Propia.

Análisis:

Se analizó la procedencia departamental de los dos usuarios que interactúan con el sistema ERP en TiviTrace. Este indicador permite identificar qué áreas de la empresa tienen una participación más activa y frecuente, lo cual es fundamental para enfocar adecuadamente las estrategias de ciberseguridad y establecer controles adaptados al contexto operativo real.

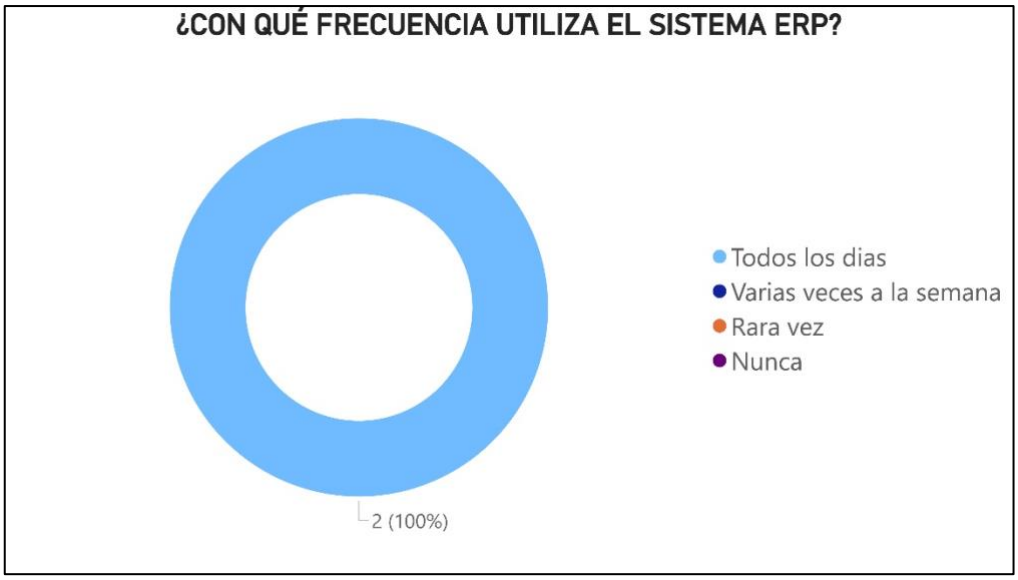
En este estudio se incluyeron dos colaboradores clave fuera del área de Tecnología de la Información (TI), quienes utilizan el sistema ERP como parte de sus funciones diarias.

Estos usuarios pertenecen a los departamentos de Operaciones y Finanzas, respectivamente, lo cual evidencia que el uso del ERP trasciende al personal técnico y se extiende a unidades operativas esenciales dentro de la organización.

Tal como se muestra en la figura 4, los departamentos mencionados concentran a la totalidad de los usuarios operativos encuestados. Este hallazgo es especialmente relevante, ya que dichas áreas gestionan procesos críticos como facturación, logística, compras y contabilidad, convirtiéndolas en objetivos potenciales para amenazas cibernéticas como fraudes, accesos indebidos o pérdida de datos sensibles.

La evidencia sugiere que los colaboradores de los departamentos administrativos y financieros están en contacto constante con el ERP, lo que incrementa la necesidad de establecer medidas de protección adecuadas. Además, esta distribución revela un punto clave, al estar las operaciones críticas fuera del control directo del área de TI, se vuelve indispensable descentralizar la responsabilidad en seguridad, promoviendo una cultura de corresponsabilidad en el uso seguro del sistema. Una falla humana en estos departamentos podría comprometer la integridad operativa completa. Por tanto, el diseño del plan de ciberseguridad debe considerar controles específicos para estos perfiles no técnicos, incluyendo segmentación de accesos, alertas contextuales y capacitación diferenciada.

Figura 5: Frecuencia de uso de ERP.



Nota: Elaboración Propia.

Análisis:

Se evaluó la frecuencia de uso del sistema ERP, aspecto clave para estimar su nivel de exposición a riesgos de ciberseguridad. Tal como se muestra en la Figura 5, los dos encuestados que representan la totalidad de la población que utiliza el ERP en TiviTrace indicaron que utilizan el sistema a diario, lo cual confirma que esta plataforma es esencial para el desempeño de sus funciones.

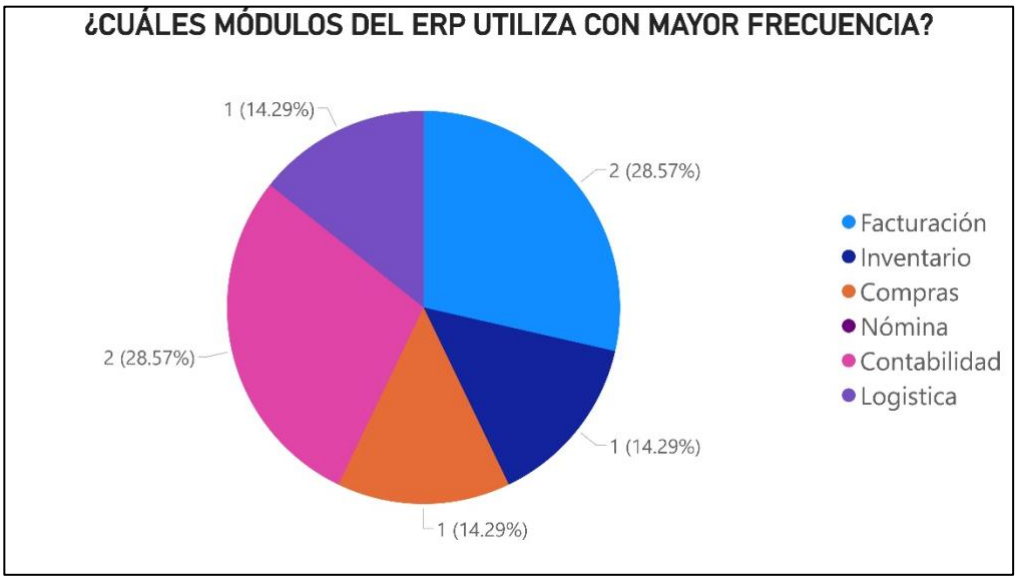
Ambos pertenecen a los departamentos de Operaciones y Finanzas, y no forman parte del área de Tecnología de la Información (TI). Esto evidencia que el uso del ERP en TiviTrace está centrado en áreas operativas clave, responsables de gestionar procesos sensibles como facturación, logística y contabilidad.

El hallazgo principal indica que, al tratarse de una herramienta de uso diario, el ERP representa un punto de entrada constante para posibles amenazas, tanto internas como externas. Por ello, los riesgos asociados no deben considerarse eventos aislados, sino como

escenarios recurrentes que requieren vigilancia continua. Esta situación revela un alto grado de dependencia funcional del sistema, subrayando la urgencia de implementar medidas de seguridad sólidas, permanentes y en constante actualización, adaptadas al contexto operativo de los usuarios reales del sistema.

El uso continuo también incrementa la posibilidad de que se normalicen malas prácticas, como compartir credenciales o ignorar advertencias de seguridad, lo cual puede debilitar las defensas del sistema. Además, una interrupción en el servicio tendría un impacto inmediato en la continuidad de operaciones, especialmente en áreas críticas como Finanzas y Operaciones, lo que hace indispensable contar con planes de respuesta ante incidentes bien definidos.

Figura 6: Módulos del ERP más utilizados por los usuarios.



Nota: Elaboración Propia.

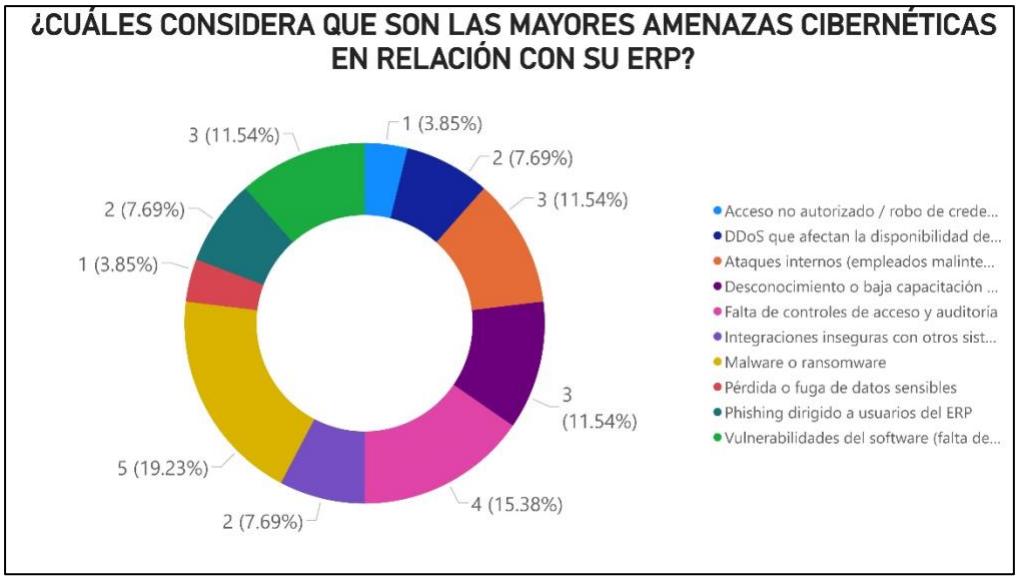
Análisis:

se investigó qué módulos del sistema ERP son utilizados con mayor frecuencia. Este dato permite identificar cuáles áreas del sistema deben tener mayores controles de seguridad.

En la figura 6 se muestra que los módulos más utilizados son Facturación**,** Contabilidad**,** Compras, Inventario y Logística**.** Estos módulos gestionan información altamente sensible y transacciones financieras clave. El hallazgo revela que los módulos críticos están directamente expuestos a los usuarios a diario, y, por ende, son propensos a errores humanos o accesos indebidos si no se resguardan adecuadamente. La tendencia indica que hay una centralización de operaciones en ciertos módulos, por lo cual es prioritario asegurar estos componentes mediante cifrado, autenticación avanzada y auditorías frecuentes.

El uso intensivo de estos módulos por parte de personal no especializado en ciberseguridad también puede derivar en una mayor probabilidad de omisiones en los controles, como el uso de contraseñas débiles o la validación insuficiente de datos. Adicionalmente, cualquier vulnerabilidad explotada en estos módulos podría comprometer múltiples procesos simultáneamente, generando un impacto transversal en la operación del negocio. Por lo tanto, la priorización de estos módulos en el plan de ciberseguridad es estratégica y crítica.

Figura 7: Amenazas cibernéticas percibidas en relación con el ERP.



Nota: **Elaboración** **Propia.**

Análisis:

Se solicitó a los encuestados que identificaran las principales amenazas que enfrentan sus sistemas ERP. La figura 7 revela una amplia variedad de amenazas percibidas, entre ellas accesos no autorizados, robo de credenciales, infecciones por malware o ransomware, vulnerabilidades debido a la falta de actualizaciones, ataques de denegación de servicio (DdoS) y amenazas internas. Esta diversidad de riesgos indica que el entorno ERP está expuesto tanto a actores externos como a riesgos generados desde dentro de la organización, ya sea por descuidos, falta de formación o intenciones maliciosas.

Uno de los hallazgos más destacados es la mención reiterada a la falta de capacitación del personal, lo cual incrementa el riesgo de ataques de ingeniería social, como el phishing. Asimismo, la ausencia de mecanismos de gestión de vulnerabilidades y la debilidad en las integraciones con otros sistemas elevan el riesgo general del entorno. Este análisis evidencia la necesidad de adoptar un enfoque integral de ciberseguridad, que combine medidas técnicas

como el control de acceso, la segmentación de redes y la actualización constante de software con acciones organizativas, tales como la formación continua, auditorías regulares y una cultura de seguridad bien establecida**.** Esto demuestra que no basta con proteger la infraestructura tecnológica, sino que es imprescindible abordar también el comportamiento humano como vector de riesgo. La coexistencia de múltiples tipos de amenazas sugiere un ecosistema ERP sin capas defensivas suficientes, con brechas tanto técnicas como organizacionales.

Figura 8: Principales Medidas de Seguridad Implementadas en ERP Empresariales.

Nota: Elaboración Propia.

Análisis:

En la figura 8 se observa que las medidas más comunes son el Control de Acceso Basado en Roles (RBAC), la autenticación multifactor (MFA) y el cifrado de 256 bits para proteger información confidencial, como en gestores de contraseñas.

El Control de Acceso Basado en Roles es una práctica fundamental para limitar el acceso a datos y funcionalidades, restringiéndolos según la función del usuario, lo que reduce la posibilidad de accesos indebidos internos y externos. La adopción de MFA es un paso significativo hacia la reducción de riesgos asociados con el compromiso de credenciales, añadiendo capas adicionales de seguridad que deben ser validadas antes de permitir el acceso. Por otro lado, el uso de cifrado robusto protege la confidencialidad de los datos tanto en reposo como en tránsito, impidiendo que agentes maliciosos puedan obtener información crítica aún en caso de vulnerar otros controles.

Un hallazgo importante es que, aunque muchas empresas adoptan estas medidas, la efectividad real depende de la correcta configuración y la integración de estos controles en el ecosistema ERP. En ocasiones, la falta de actualización o la implementación parcial puede generar vulnerabilidades. Además, la integración de software antivirus complementa la protección, ayudando a defender los sistemas contra malware y otras amenazas activas.

La tendencia observada confirma una alineación progresiva con las mejores prácticas recomendadas por la norma ISO/IEC 27032, enfatizando la importancia de controles robustos para gestionar y mitigar riesgos de ciberseguridad en ERP empresariales. Por lo tanto, el diseño del plan de ciberseguridad debe contemplar la implementación efectiva y combinada de MFA, cifrado avanzado, RBAC y soluciones antivirus para garantizar la confidencialidad, integridad y disponibilidad de la información crítica, mejorando así la postura de seguridad y la continuidad del negocio.

Figura 9: Políticas y Procedimientos de Seguridad Implementados en ERP Empresariales.

Nota: Elaboración Propia.

Pregunta: ¿Qué políticas y procedimientos de seguridad existen?

Análisis:

En la figura 9 se evidencian respuestas que indican la implementación de diversos mecanismos formales como políticas de seguridad de la información, control de accesos, auditorías, manejo de logs y validación de usuarios.

Entre las respuestas destaca la existencia de una "Política de seguridad de la información y política de control de acceso", que establece claramente los lineamientos sobre el uso responsable, la protección de los datos y el acceso restringido según los niveles de autorización. Estas políticas son la base de una cultura organizacional orientada a la prevención de incidentes y al cumplimiento normativo. Asimismo, la mención de auditorías

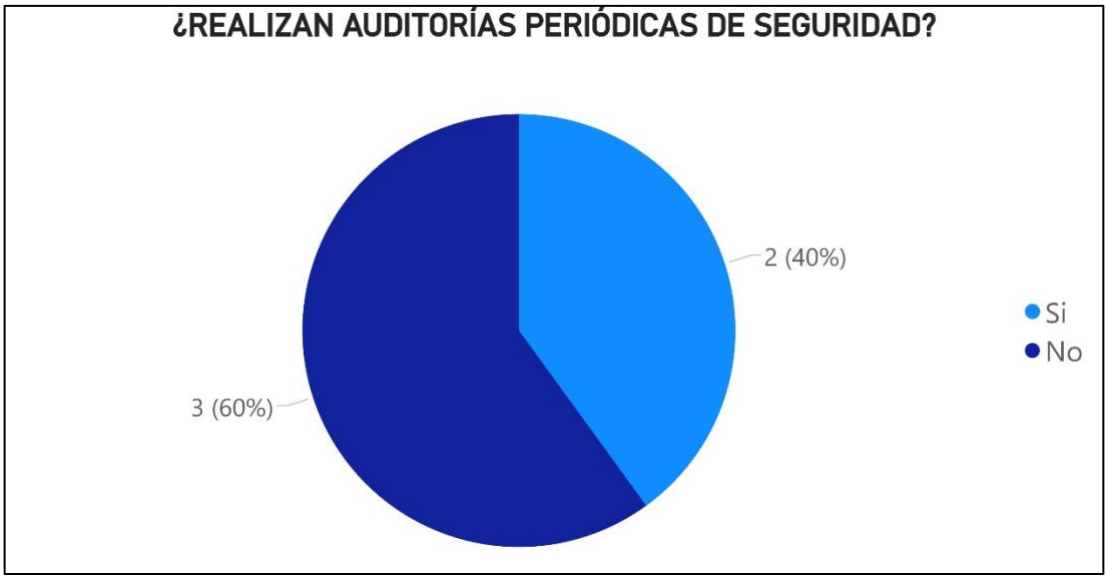
refuerza el compromiso con la verificación periódica del cumplimiento de dichas políticas, lo cual permite detectar brechas, malas prácticas y áreas de mejora.

Otras respuestas resaltan el uso de contraseñas temporales generadas por el sistema, así como la restricción de privilegios para el cambio de contraseñas, reservado únicamente a los usuarios administradores. Este enfoque, combinado con la autenticación personalizada por parte del usuario y el uso de tokens JWT (JSON Web Token) para el manejo de sesiones, demuestra un esfuerzo por mantener una autenticación robusta y trazabilidad de accesos mediante logs de movimientos.

Un hallazgo relevante es la variedad de mecanismos que complementan las políticas: niveles de autenticación diferenciados, validación de usuarios y gestión de privilegios, lo cual permite no solo controlar el acceso, sino también identificar y responder rápidamente ante accesos anómalos o no autorizados.

La tendencia observada sugiere que las organizaciones están comenzando a adoptar políticas formales como parte de un enfoque estratégico de seguridad, sin embargo, aún hay oportunidad de fortalecer la estandarización y documentación de procedimientos, especialmente aquellos alineados con ISO/IEC 27032 e ITIL V4. La formalización de estas políticas en todos los niveles y su revisión periódica garantizarán una mayor madurez en la gestión de riesgos cibernéticos. Por ende, el diseño del plan de ciberseguridad debe contemplar el desarrollo, evaluación y difusión de políticas claras, actualizadas y orientadas a mitigar amenazas y garantizar la resiliencia del ERP empresarial.

Figura 10: Frecuencia de Auditorías de Seguridad Realizadas en los ERP Empresariales.



Nota: Elaboración Propia.

Análisis:

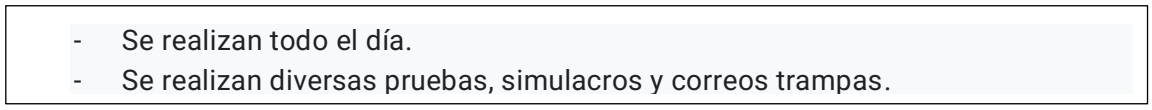
En la figura 10 se presentan los resultados obtenidos ante esta consulta, en la cual se evidencia que la práctica no está estandarizada en todas las organizaciones. De las cinco respuestas analizadas, tres indicaron que no realizan auditorías periódicas, mientras que únicamente dos afirmaron que sí las efectúan.

Este hallazgo refleja una preocupación significativa en materia de ciberseguridad, ya que las auditorías periódicas son uno de los mecanismos más efectivos para identificar vulnerabilidades, evaluar el cumplimiento de políticas de seguridad, y corregir deficiencias antes de que puedan ser explotadas por agentes maliciosos. La ausencia de auditorías recurrentes sugiere un bajo nivel de madurez en la gestión de riesgos y podría estar relacionada con limitaciones de recursos, desconocimiento de buenas prácticas, o una baja priorización del tema en la agenda institucional.

La tendencia identificada señala que la mayoría de las organizaciones encuestadas aún no han incorporado las auditorías como parte regular de su estrategia de ciberseguridad. Esto puede derivar en una exposición prolongada a amenazas sin detección oportuna, comprometiendo la integridad, confidencialidad y disponibilidad de los datos procesados en sus ERP empresariales. En contraste, las organizaciones que sí realizan auditorías demuestran una proactividad y mayor conciencia sobre los riesgos, alineándose con las recomendaciones establecidas por marcos normativos como ISO/IEC 27032, que promueve la evaluación continua de la postura de seguridad.

Este indicador pone en evidencia la necesidad urgente de implementar auditorías periódicas como parte integral del plan de ciberseguridad. Estas no solo deben contemplar aspectos técnicos del ERP, sino también el cumplimiento de políticas, la eficacia de los controles implementados y la capacidad de respuesta ante incidentes. El diseño del plan deberá incluir la calendarización de auditorías internas y externas, con el acompañamiento de personal especializado, así como el uso de herramientas automatizadas que permitan mejorar la eficiencia en la detección de brechas y la mejora continua del sistema.

Figura 11: Métodos de Gestión de Auditorías de Seguridad en ERP Empresariales.



Nota: Elaboración Propia.

Análisis:

En este indicador, se recopilaron dos respuestas específicas de los encuestados que afirmaron realizar auditorías de seguridad. La primera respuesta menciona que las auditorías se realizan “todo 1 día”, lo que indica que la organización ejecuta una jornada completa dedicada a la

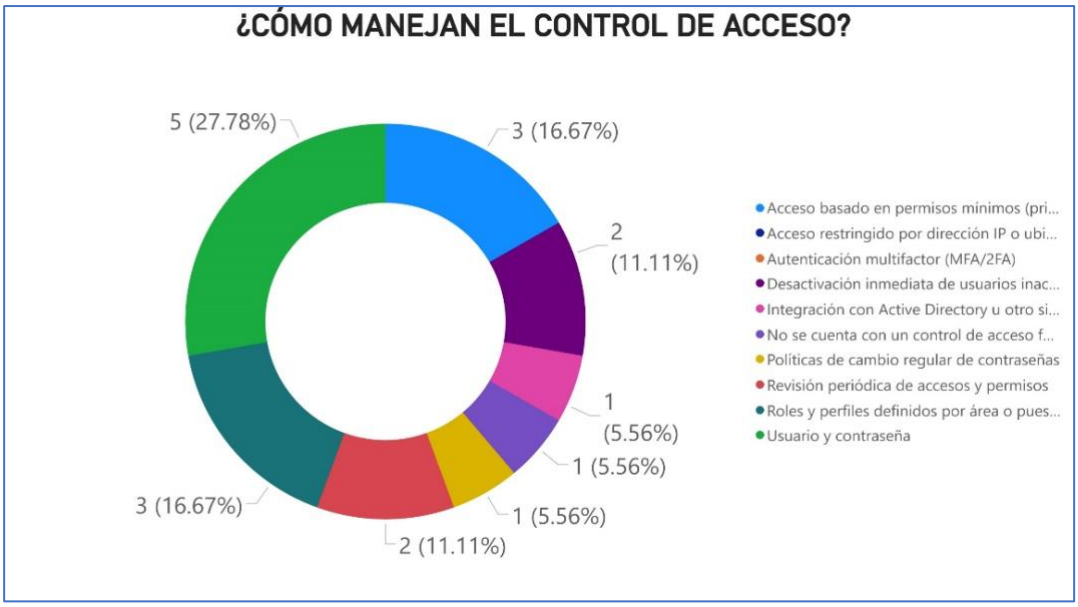
revisión de sus sistemas. Esta práctica, aunque muestra intención de control, puede carecer de profundidad si no se acompaña de una planificación rigurosa, herramientas adecuadas y seguimiento de hallazgos.

Por otro lado, la segunda respuesta describe un enfoque más detallado, que incluye la realización de diversas pruebas, simulacros y el uso de correos trampa. Este tipo de medidas son propias de un enfoque proactivo y preventivo frente a amenazas, lo cual demuestra una mayor madurez en la gestión de ciberseguridad. Los simulacros permiten evaluar la capacidad de respuesta del personal ante incidentes, mientras que los correos trampa (phishing simulations) son útiles para identificar debilidades en la concienciación del personal y promover acciones correctivas.

En la figura 11 se observan estos métodos diferenciados, lo que refleja un grado de disparidad entre las prácticas implementadas por las empresas que sí ejecutan auditorías. Esta variabilidad pone de manifiesto la necesidad de establecer procedimientos estandarizados basados en marcos como ISO/IEC 27032, que brinden directrices claras sobre la frecuencia, alcance y seguimiento de auditorías.

Como hallazgo relevante, se identifica que no todas las empresas que realizan auditorías lo hacen con la misma rigurosidad ni con los mismos recursos, lo que puede generar brechas de seguridad. La tendencia sugiere que algunas organizaciones están avanzando hacia prácticas más integrales, mientras que otras aún se encuentran en etapas iniciales. Se concluye que promover lineamientos unificados y buenas prácticas podría elevar la calidad y efectividad de las auditorías de seguridad en ERP empresariales.

Figura 12: Métodos de Control de Acceso Implementados en ERP Empresariales.



Nota: Elaboración Propia.

Análisis:

El control de acceso constituye una de las primeras líneas de defensa frente a amenazas internas y externas, al garantizar que solo los usuarios autorizados puedan ingresar y operar dentro del sistema, de acuerdo con sus funciones y niveles jerárquicos. En la figura 12 se visualizan los mecanismos de control de acceso que utilizan los encuestados en sus plataformas ERP.

Los resultados revelan que todos los participantes aplican el método más básico de control de acceso: el uso de nombre de usuario y contraseña. Este mecanismo es el punto de partida mínimo para la autenticación, aunque por sí solo es insuficiente frente a amenazas avanzadas. Sin embargo, cuatro de los cinco encuestados complementan este método con prácticas más avanzadas, como la definición de roles y perfiles según el área o puesto de trabajo, la aplicación del principio de menor privilegio (limitando los accesos estrictamente necesarios para cumplir funciones), y la desactivación inmediata de cuentas de usuarios

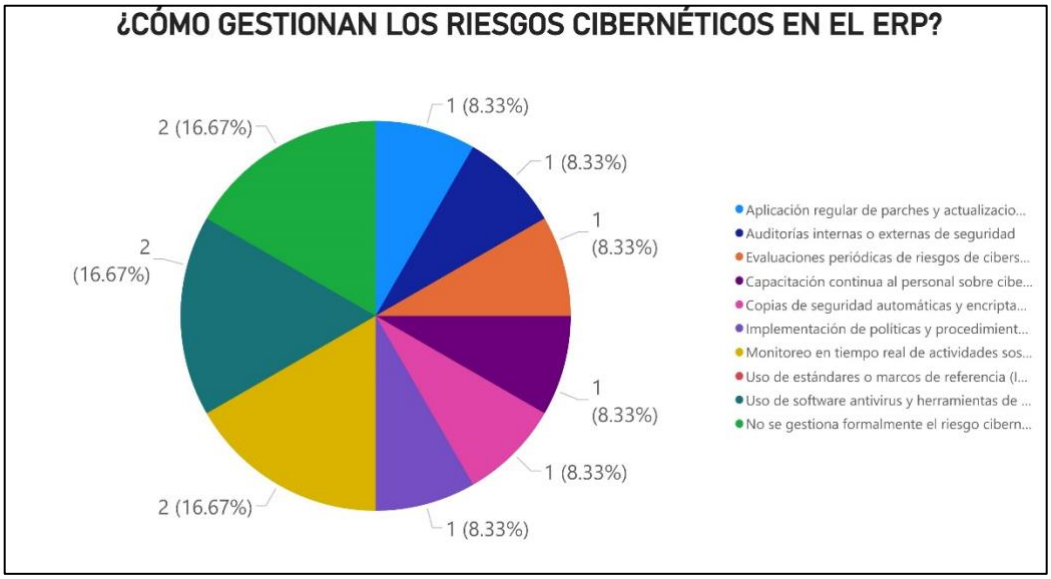
inactivos o exempleados. Estas medidas reflejan una orientación hacia una administración de accesos más consciente y alineada con buenas prácticas de ciberseguridad.

Uno de los encuestados incluso menciona la revisión periódica de permisos y accesos, las políticas de cambio regular de contraseñas y la integración con un sistema de autenticación centralizado como Active Directory. Esta implementación indica un mayor nivel de madurez en la gestión de identidades, ya que permite centralizar el control, auditar accesos y reducir errores humanos en la asignación de privilegios.

No obstante, también se evidencia una debilidad significativa: una de las respuestas admite no contar con un control de acceso formal. Esto representa un riesgo crítico, ya que deja abierta la posibilidad de accesos no autorizados, ya sea por negligencia o por fallos en la configuración del sistema. Esta falta de estructura pone en riesgo la integridad y confidencialidad de la información contenida en el ERP.

Como hallazgo relevante, se observa que, si bien existe una tendencia positiva hacia el uso de controles más robustos, la implementación no es homogénea en todas las organizaciones. La conclusión apunta a la necesidad de adoptar estándares como los propuestos en ISO/IEC 27032, que fomentan políticas estructuradas de acceso, monitoreo constante y formación del personal. Reforzar el control de acceso con autenticación multifactor (MFA) y herramientas de gestión de identidades contribuiría sustancialmente a minimizar los riesgos asociados a accesos indebidos, fortaleciendo la postura de seguridad en los sistemas ERP.

Figura 13: Estrategias empleadas para la gestión de riesgos cibernéticos en el ERP.



Nota: Elaboración Propia.

Análisis:

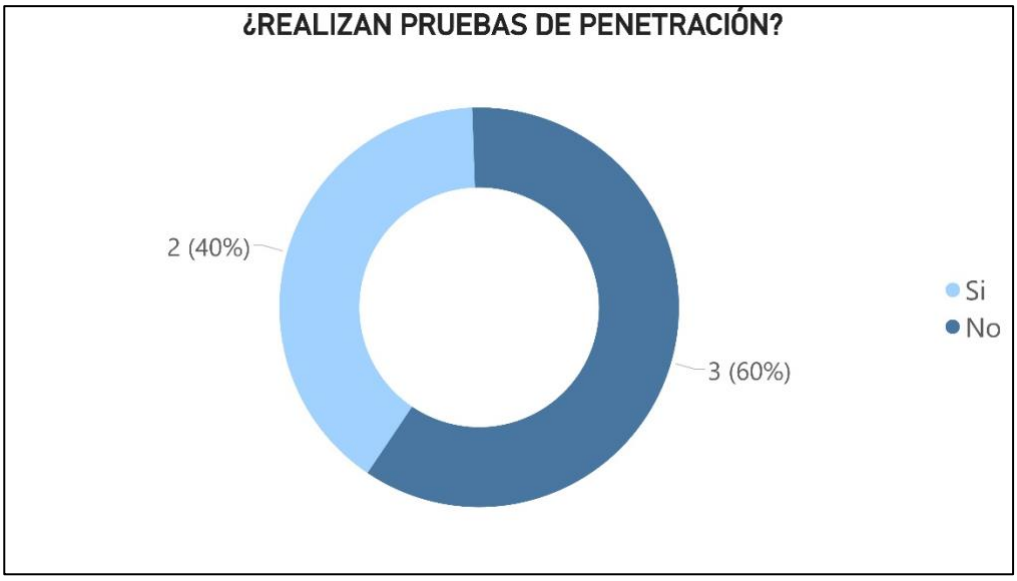
Para el cumplimiento del objetivo 1, orientado a identificar y clasificar los riesgos de ciberseguridad en sistemas ERP mediante análisis de vulnerabilidades y auditorías, esta pregunta proporciona información clave sobre el nivel de madurez en la gestión de riesgos dentro de TiviTrace. En la figura 13 se observa una variabilidad en las prácticas de gestión del riesgo cibernético: el 40% de las respuestas indican la ausencia de una gestión formal, lo cual representa una vulnerabilidad crítica que podría comprometer la seguridad del ERP.

Por otro lado, algunas respuestas reflejan prácticas más maduras, como el monitoreo en tiempo real, uso de antivirus, evaluaciones periódicas de riesgo, parches de seguridad, auditorías, copias de respaldo y capacitación continua. Estas acciones son coherentes con las recomendaciones de normas como la ISO/IEC 27032, que subraya la importancia del factor humano y de un enfoque preventivo en la gestión del riesgo. La existencia simultánea de

prácticas sólidas y carencias críticas evidencia un enfoque fragmentado de la seguridad, donde la protección depende del área o individuo involucrado.

Este hallazgo revela una brecha significativa dentro de TiviTrace en cuanto al enfoque de ciberseguridad, mientras algunas áreas aplican medidas, otras carecen de estrategias formales. Esta fragmentación incrementa la exposición a incidentes, ya que las fallas en un solo punto pueden comprometer todo el sistema ERP. Esta disparidad justifica la necesidad de un plan integral que estandarice y fortalezca la gestión de riesgos, alineándose con buenas prácticas y marcos internacionales.

Figura 14: Pruebas de penetración realizadas en ERP empresarial.



Nota: Elaboración Propia.

Análisis:

En la Figura 14 se observa que solo algunos realizan estas pruebas, mientras que la mayoría no lo hace. Esta falta de pruebas periódicas representa un riesgo, ya que dificulta la detección temprana de vulnerabilidades críticas. Sin estas pruebas, la organización está más

expuesta a ataques y posibles brechas de seguridad. Este hallazgo refleja una carencia en los procesos proactivos de seguridad, lo que evidencia una gestión de riesgos reactiva en lugar de preventiva. Las pruebas de penetración, al no formar parte de una rutina institucionalizada, dejan vacíos en la detección de amenazas latentes que podrían ser aprovechadas por actores maliciosos internos o externos. La tendencia muestra una necesidad clara de mejorar las prácticas de seguridad mediante la implementación regular de pruebas de penetración para fortalecer la gestión de riesgos y proteger mejor los sistemas ERP. Además, la ausencia de estas pruebas compromete el cumplimiento de estándares internacionales como ISO/IEC 27032, que recomiendan realizar simulaciones controladas de ataque para evaluar la resistencia del entorno digital. Institucionalizar estas prácticas permitiría anticiparse a incidentes, generar evidencia para auditorías y fortalecer la cultura organizacional hacia una ciberseguridad continua y adaptativa.

Figura 15: Gestión de resultados de pruebas de penetración en ERP empresarial.

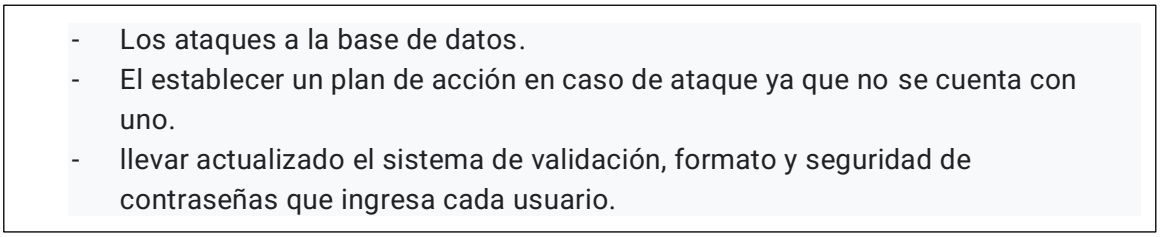
Nota: Elaboración Propia.

Análisis:

Es fundamental no solo realizar pruebas de penetración, sino también gestionar adecuadamente los resultados para mitigar los riesgos identificados. En la Figura 15 se refleja que la gestión de resultados se realiza durante todo el día o a nivel de Gerencia de IT, lo que indica un enfoque activo en el seguimiento y corrección de vulnerabilidades. Este enfoque demuestra una comprensión básica de la importancia del ciclo completo de las pruebas de

seguridad: identificar, analizar, priorizar y remediar. Este manejo continuo y de alto nivel permite una respuesta rápida ante hallazgos críticos, mejorando la seguridad del ERP. No obstante, la limitada participación y formalización de este proceso entre los encuestados evidencia una debilidad organizacional, donde la responsabilidad puede estar centralizada pero no institucionalizada. Esta situación limita la trazabilidad de las acciones correctivas y reduce la posibilidad de establecer métricas de mejora continua. Sin embargo, la limitación de respuestas indica que no todas las organizaciones tienen procesos formales definidos para esta gestión, lo cual puede comprometer la eficacia del plan de ciberseguridad. La tendencia apunta a la necesidad de formalizar y ampliar estos procesos para asegurar una gestión integral de riesgos basada en los resultados de las pruebas. La implementación de procedimientos documentados, responsables designados, cronogramas de remediación y revisiones periódicas permitiría alinear esta gestión con marcos internacionales como ISO/IEC 27032 e ITIL V4, asegurando una respuesta estructurada ante vulnerabilidades.

Figura 16: Principales desafíos en la ciberseguridad del ERP.



Nota: Elaboración Propia.

Análisis:

Busca identificar y clasificar los riesgos de ciberseguridad, los resultados reflejan desafíos críticos en la gestión de la seguridad del ERP. En la Figura 16 se destaca que el principal reto es la ausencia de un plan formal de acción ante ataques, lo cual deja la plataforma vulnerable ante incidentes. Además, se identifican dificultades en mantener actualizadas las políticas de seguridad, especialmente en cuanto a contraseñas robustas para usuarios. También se señala la amenaza directa a la base de datos, un activo crítico que, si se ve comprometido, puede causar daños significativos a la continuidad y confidencialidad de la información. Otro desafío importante es la gestión de vulnerabilidades desconocidas y la falta de personal especializado en ciberseguridad, lo cual limita la capacidad de detección y respuesta efectiva frente a amenazas avanzadas.

Por último, la integración con sistemas legados y la complejidad de los entornos híbridos constituyen obstáculos técnicos que dificultan la implementación y mantenimiento de controles modernos y efectivos. Esta diversidad tecnológica demanda un enfoque actualizado y profesional para mantener la infraestructura segura y en constante evolución. Estos hallazgos evidencian la necesidad de diseñar un plan integral basado en normas como ISO/IEC 27032 e ITIL V4, que aborde estos desafíos mediante estrategias claras de mitigación, capacitación continua y gestión efectiva de vulnerabilidades, alineándose con la gestión integral de riesgos en el ERP.

Figura 17: Principales oportunidades para mejorar la ciberseguridad en el ERP.

- Desarrollo y ejecución de planes de respuesta a incidentes, incluyendo simulacros periódicos.
- Mejora en las políticas y prácticas de seguridad para la gestión de contraseñas.
- Implementación de monitoreo constante y análisis de alertas de seguridad en tiempo real
- Capacitación continua dirigida a reducir riesgos de ingeniería social, con énfasis en phishing.

Nota: Elaboración Propia.

Análisis:

En la Figura 17 se observa que una de las principales oportunidades es la elaboración y puesta en práctica de un plan formal de ciberseguridad, acompañado de simulacros que permitan evaluar la respuesta ante incidentes reales. Esto es fundamental para preparar a la organización y minimizar impactos en caso de ataques. Otra oportunidad clave identificada es el fortalecimiento de la seguridad en la gestión de contraseñas, uno de los puntos más vulnerables en muchos sistemas. Mejorar políticas, promover contraseñas robustas y adoptar tecnologías como MFA puede reducir significativamente el riesgo de accesos no autorizados.

Además, se reconoce la importancia de la capacitación continua del personal, sobre todo para mitigar riesgos asociados a la ingeniería social como el phishing, que es una de las principales vías de entrada para los atacantes. La formación adecuada en este aspecto permite crear una cultura de seguridad que complementa las medidas técnicas. Finalmente, se destaca la necesidad de implementar un monitoreo constante de la actividad en el ERP, lo que facilitaría la detección temprana de comportamientos anómalos y posibles amenazas, contribuyendo a una gestión proactiva de la ciberseguridad. Estas oportunidades apuntan a la necesidad de un enfoque integral que incluya políticas, tecnología, procesos y cultura organizacional para

mitigar los riesgos en el ERP, alineándose con la propuesta de plan basada en ISO/IEC 27032 e ITIL V4.

4.1.3 DIAGRAMA DE ISHIKAWA

El Diagrama de Ishikawa, también conocido como “Diagrama de Causa-Efecto”, es una herramienta de análisis ampliamente utilizada en la gestión de calidad, mejora de procesos y gestión de riesgos, incluyendo su aplicación en el ámbito de la seguridad de la información. Su principal función es identificar, organizar y visualizar de manera estructurada las causas raíz de un problema específico, permitiendo a las organizaciones abordar los factores subyacentes que generan una situación adversa. En el contexto del presente estudio, esta herramienta se emplea para examinar de forma sistemática los factores que contribuyen a uno de los riesgos más significativos identificados en la empresa TiviTrace: los accesos no autorizados y los ataques de ingeniería social, en particular el phishing, que afectan directamente al sistema ERP empresarial.

Este tipo de amenazas constituye una vulnerabilidad crítica, ya que compromete la confidencialidad, integridad y disponibilidad de la información gestionada por el ERP, impactando tanto la operación cotidiana como la toma de decisiones estratégicas de la organización. La explotación de debilidades técnicas, la falta de preparación del personal y la ausencia de controles efectivos aumentan la exposición a estos incidentes, evidenciando la necesidad de una evaluación detallada de las causas que los propician. A través del Diagrama de Ishikawa, se facilita la comprensión de esta problemática mediante la categorización de las causas potenciales en seis dimensiones clave: recursos humanos, tecnología, procesos, políticas organizacionales, cultura organizacional y proveedores externos. Estas categorías permiten abordar el problema desde una perspectiva integral, que reconoce la

interdependencia entre factores técnicos, humanos y estructurales en la gestión de ciberseguridad dentro de sistemas ERP.

- Recursos Humanos: Deficiencias en la capacitación del personal, desconocimiento de buenas prácticas en ciberseguridad, y una escasa sensibilización frente a amenazas como el phishing.
- Tecnología: Falta de mecanismos avanzados de autenticación (como MFA), carencia de sistemas de monitoreo en tiempo real, y vulnerabilidades derivadas de software desactualizado o mal configurado.
- Procesos: Ausencia de procedimientos estandarizados para la gestión de accesos, protocolos de seguridad poco efectivos o inexistentes, y falta de auditorías periódicas.
- Políticas Organizacionales: Normativas internas poco claras o desactualizadas respecto al uso del ERP, debilidades en la gestión de contraseñas, y ausencia de lineamientos específicos para incidentes de seguridad.
- Cultura Organizacional: Baja concienciación sobre la importancia de la ciberseguridad, escaso compromiso institucional para fortalecer el entorno digital, y resistencia al cambio tecnológico.
- Proveedores Externos: Integraciones con terceros sin validación de cumplimiento de estándares de seguridad, accesos compartidos sin control adecuado, y falta de acuerdos de nivel de servicio (SLAs) con cláusulas específicas de protección de datos.

La representación gráfica de las causas facilita la comprensión del problema y la priorización de acciones correctivas, fortaleciendo el diseño preventivo del plan de ciberseguridad según ISO/IEC 27032 e ITIL v4.

Figura 18: Diagrama de Ishikawa del Proyecto

Nota: Elaboración propia.

4.1.4 AUDITORÍA DOCUMENTAL DE POLÍTICAS DE SEGURIDAD INTERNA

La auditoría documental de políticas de seguridad interna se diseñó siguiendo las directrices de los controles de ISO/IEC 27032:2023 (ciberseguridad). Su objetivo fue verificar, mediante evidencia escrita y registros, el grado de conformidad del ERP con las políticas y procedimientos de seguridad declarados por la organización. El equipo auditor revisó políticas, bitácoras de acceso, actas de capacitación, respaldos y configuraciones del

sistema, entrevistando a responsables de TI para aclarar dudas y solicitar documentos adicionales.

La **ISO/IEC 27032:2023** dedica su cláusula 9.2 a un conjunto de controles de alto nivel para la "seguridad en Internet". Cada No-Conformidad (NC) y Observación (OB) detectada durante la auditoría documental se alinea con uno o, en algunos casos, varios de esos controles. A continuación, se explica dicho mapeo y la razón por la que cada hallazgo constituye un riesgo:

Hallazgos de cumplimiento: No-conformidades (Viola el requisito ISO/EIC 27032) y observaciones (Punto débil o practica que se debe mejorar), estos hallazgos documentales se incorporan como causas raíz en el Diagrama de Ishikawa (Fig. 18) y refuerzan los hallazgos de los instrumentos socio-organizativos.

Tabla 1: No conformidades(NC) y Observaciones(OB)

Código	Control ISO/IEC 27032 : 2023	Brecha detectada	Por qué es relevante
NC-01	9.2.2 Políticas de seguridad en Internet	Política de contraseñas desactualizada	Las políticas son la piedra angular; un requisito obsoleto (longitud, caducidad, complejidad) expone al ERP a credenciales triviales o reutilizadas.
NC-02	9.2.5 Gestión de incidentes de seguridad	Sin registro formal de incidentes de phishing	ISO exige un proceso documentado para reportar, resolver y aprender de cada incidente. Sin evidencia, la organización no puede demostrar mejora continua ni cumplimiento.
NC-03	9.2.8 Continuidad de negocio (copias de seguridad)	Backups sin pruebas de restauración	La norma aclara que la simple existencia de backups no basta; deben verificarse de forma rutinaria para garantizar la recuperación ante ataques de ransomware.
NC-04	9.2.3 Control de acceso	Accesos remotos sin verificación de identidad fuerte	Falta de MFA o de mecanismos equivalentes contradice la exigencia de autenticación robusta para toda conexión expuesta a Internet.

NC-05	9.2.4 Educación, concienciación y formación	Sin evidencia de capacitaciones anuales	El estándar subraya que las amenazas evolucionan; la formación periódica es obligatoria para mitigar vectores sociales como phishing o vishing.
NC-06	9.2.10 Gestión de vulnerabilidades	Parches críticos aplicados > 30 días	ISO/IEC 27032 enfatiza la rápida aplicación de parches para vulnerabilidades explotables en Internet. Demoras prolongadas elevan la superficie de ataque.
OB-01	9.2.6 Gestión de activos	Inventario de activos incompleto	Sin un inventario exacto, no se pueden asignar controles ni calificar riesgos de forma fiable.
OB-02	9.2.18 Monitoreo	Logs conservados < 90 días	La retención corta dificulta investigaciones forenses y contraviene las buenas prácticas de trazabilidad.
OB-03	9.2.6 Gestión de activos / 9.2.2 Políticas	Falta de clasificación de datos	La norma requiere etiquetar la información para aplicar niveles de protección coherentes.
OB-04	9.2.13 Gestión de cambios	Escasa trazabilidad de cambios	Sin registro detallado de cambios, la organización no puede auditar configuraciones ni revertir ajustes inseguros.

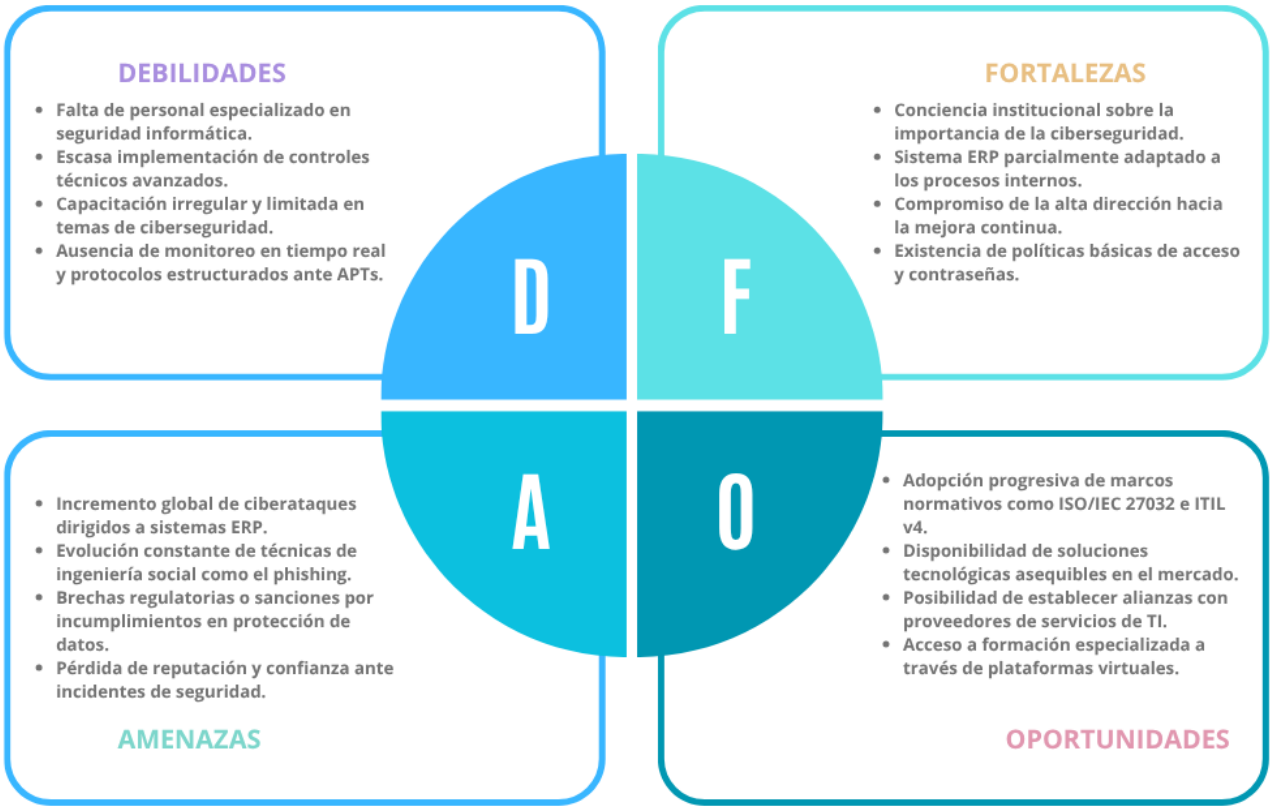
4.1.5 MATRIZ DE ANÁLISIS FODA

El análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) es una herramienta estratégica que permite identificar factores internos y externos que influyen en el desempeño de una organización, facilitando la formulación de planes de acción adecuados. En el marco del presente estudio sobre ciberseguridad en sistemas ERP empresariales, esta matriz se ha aplicado a la empresa TiviTrace con el objetivo de comprender su posicionamiento actual frente a los riesgos cibernéticos y su capacidad para gestionarlos de manera proactiva.

La evaluación considera elementos internos (fortalezas y debilidades) que derivan de la estructura, procesos, recursos humanos y tecnológicos de la organización, así como factores externos (oportunidades y amenazas) que provienen del entorno digital, normativo y competitivo en el cual opera. Este análisis proporciona una visión clara de las condiciones

que pueden potenciar o limitar la implementación de medidas efectivas de ciberseguridad, permitiendo priorizar acciones que refuercen la protección de los activos digitales

Figura 19: Matriz de análisis FODA.



Nota: Elaboración propia.

Este análisis FODA permite delinear un mapa estratégico de intervención en ciberseguridad, maximizando las fortalezas institucionales, corrigiendo debilidades críticas, aprovechando oportunidades del entorno tecnológico y regulatorio, y anticipándose a las amenazas emergentes que podrían comprometer la continuidad operativa de TiviTrace. En este sentido, el uso del análisis FODA no solo complementa el diagnóstico de riesgos, sino que también orienta la planificación táctica hacia una gestión más resiliente y sostenible de la seguridad informática en entornos empresariales complejos.

4.1.6 RIESGOS IDENTIFICADOS

La identificación de riesgos constituye una etapa crítica dentro de la gestión de la seguridad de la información, ya que permite anticipar y gestionar las amenazas que pueden comprometer la confidencialidad, integridad y disponibilidad de los activos del sistema ERP de TiviTrace. Esta sección resume los principales riesgos detectados a partir de los instrumentos aplicados (entrevistas, encuestas y listas de verificación), categorizándolos según su naturaleza y proporcionando una codificación para facilitar su análisis y seguimiento posterior. Las categorías consideradas son:

- Humano: Relacionado con errores, negligencias o malas prácticas por parte del personal interno o usuarios del sistema.
- Tecnológico: Referente a vulnerabilidades en la infraestructura tecnológica, deficiencias técnicas o carencias en herramientas de protección.
- Organizacional: Asociado a procesos deficientes, políticas internas inadecuadas o ausencia de protocolos.
- Externo: Derivado de amenazas externas como ciberataques, phishing o intrusiones no autorizadas.

El propósito de esta tabla es sentar las bases para la matriz de evaluación y el diseño de estrategias de mitigación que refuercen la postura de ciberseguridad de la empresa.

Tabla 2: Clasificación de riesgos identificados en el sistema ERP según su tipo.

Código	Tipo de Riesgo	Riesgo Identificado
R1	Humano	Uso de contraseñas débiles o compartidas por parte del personal
R2	Humano	Desconocimiento o escasa formación en prácticas seguras de ciberseguridad
R3	Tecnológico	Ausencia de autenticación multifactor en el acceso al sistema ERP
R4	Tecnológico	Fallas en la actualización y mantenimiento de los sistemas
R5	Organizacional	Falta de políticas claras de seguridad de la información
R6	Organizacional	Procesos internos no estandarizados o sin validación cruzada
R7	Externo	Ataques de phishing dirigidos a empleados de áreas críticas
R8	Externo	Intentos de acceso no autorizado mediante técnicas de fuerza bruta
R9	Organizacional	Ausencia de un plan de continuidad del negocio ante incidentes graves
R10	Tecnológico	Exposición del ERP a internet sin controles perimetrales adecuados

4.1.7 MATRIZ DE RIESGOS EMPRESARIAL (PROBABILIDAD × IMPACTO)

Para valorar el riesgo inherente asociado a cada hallazgo identificado, se utilizó una matriz de evaluación basada en dos dimensiones: *probabilidad (P)* e *impacto (I)*. Ambos factores se calificaron en una escala de 1 a 3:

Tabla 3: Escalas de valoración de probabilidad de impacto para la matriz de riesgos.

Escala	Descripción	Valores
Probabilidad (P)	Frecuencia o verosimilitud estimada de ocurrencia	1 Baja 2 Media 3 Alta
Impacto (I)	Magnitud del daño sobre confidencialidad, integridad y disponibilidad	1 Menor 2 Significativo 3 Crítico

El Nivel de Riesgo (NR) se calcula como NR = P × I y se clasifica así:

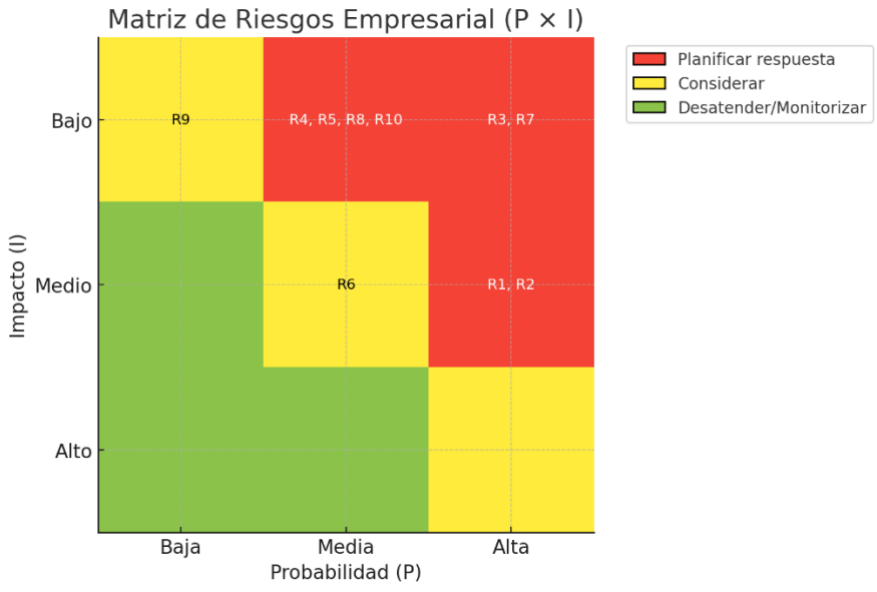
Tabla 4: Clasificación del nivel riesgo y acciones recomendadas.

NR	Categoría	Acción recomendada
1–2	Bajo	Monitorear
3–4	Medio	Mejorar cuando sea viable
6	Alto	Mitigar de forma prioritaria
9	Crítico	Mitigación inmediata

Tabla 5: Evaluación de Riesgos Inherentes (sin mitigación)

Código	Tipo	Riesgo identificado	P	I	NR	Clasificación
R1	Humano	Contraseñas débiles/compartidas	3	2	**6**	Alto
R2	Humano	Falta de formación en ciberseguridad	3	2	**6**	Alto
R3	Tecnológico	Ausencia de MFA en el ERP	3	3	**9**	**Crítico**
R4	Tecnológico	Parches y mantenimiento tardíos	2	3	**6**	Alto
R5	Organizacional	Políticas de seguridad insuficientes	2	3	**6**	Alto
R6	Organizacional	Procesos no estandarizados	2	2	4	Medio
R7	Externo	Phishing dirigido a empleados clave	3	3	**9**	**Crítico**
R8	Externo	Fuerza bruta contra credenciales	2	3	**6**	Alto
R9	Organizacional	Sin plan de continuidad de negocio	1	3	3	Medio
R10	Tecnológico	ERP expuesto sin control perimetral	2	3	**6**	Alto

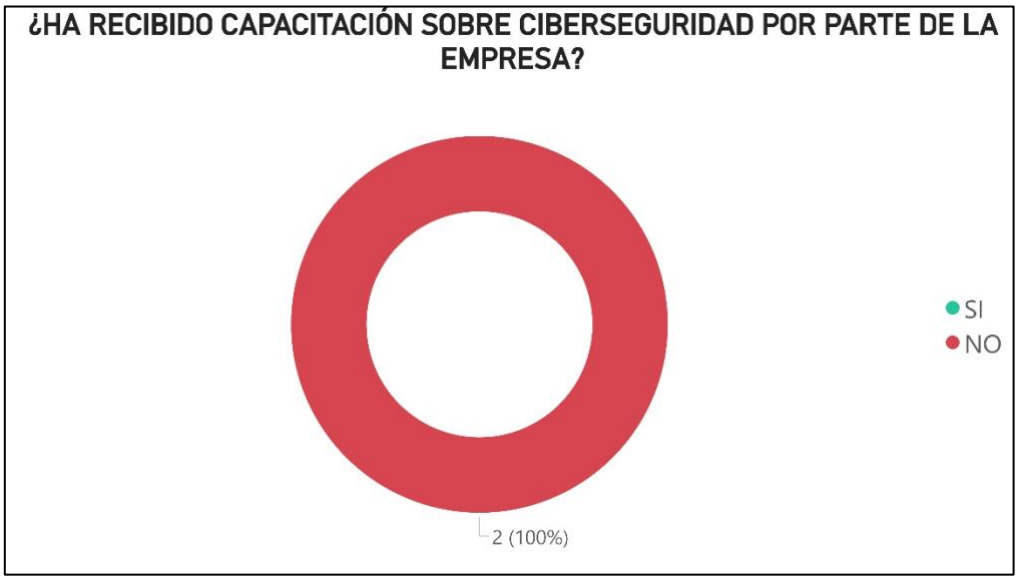
Figura 20: Mapa de Calor.



4.1.8 ANÁLISIS DE LAS MEJORES PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA NORMA ISO/IEC 27032 Y SU APLICABILIDAD EN LA GESTIÓN DE RIESGOS DE CIBERSEGURIDAD EN ERP EMPRESARIALES.

En este objetivo se recopilaron datos mediante encuestas, entrevistas y revisión documental, a fin de identificar el grado de alineación entre las prácticas actuales de ciberseguridad en los ERP empresariales y las recomendaciones de la norma ISO/IEC 27032. Los resultados revelaron deficiencias críticas en formación del personal, como el desconocimiento generalizado sobre phishing, la ausencia de capacitación y la baja capacidad para identificar accesos sospechosos. Además, se detectó una escasa adopción de normas como ISO 27032 o NIST, con poca aplicación práctica, especialmente en empresas con ERP propios. A pesar de ello, se observaron avances en controles de acceso, uso parcial de autenticación multifactor y cifrado de datos. Estos hallazgos reflejan una implementación parcial de buenas prácticas, destacando la necesidad urgente de fortalecer la educación, estandarización y aplicación formal de medidas de seguridad bajo marcos internacionales. A su vez, se presenta un análisis preliminar de los resultados obtenidos,

Figura 21: Porcentaje de usuarios capacitados en ciberseguridad.



Nota: Elaboración Propia

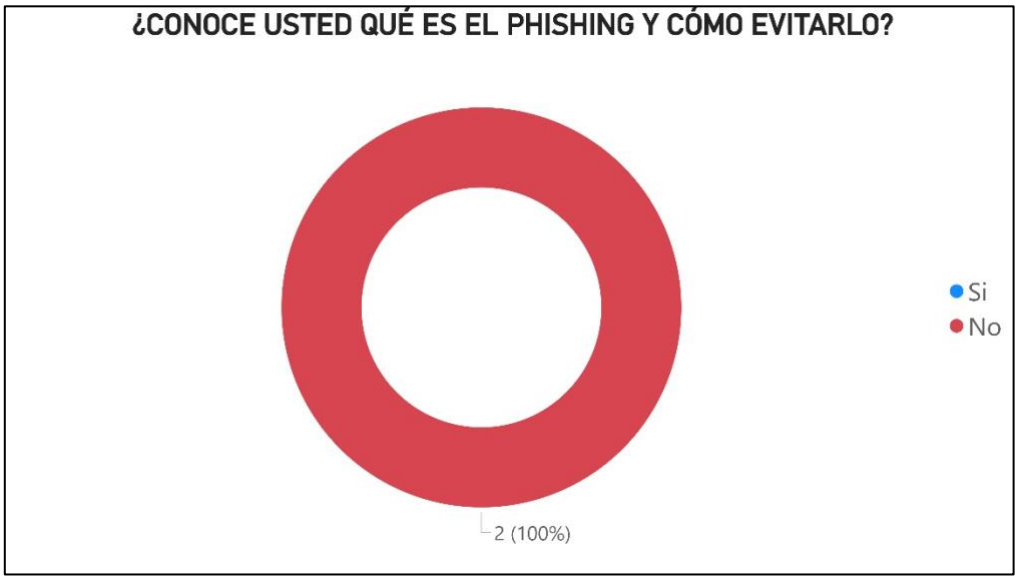
Análisis:

En este indicador se evaluó si los colaboradores han recibido formación sobre prácticas seguras en el uso del ERP. En la Figura 21 se observa que ninguno de los encuestados ha recibido capacitación en ciberseguridad por parte de la empresa, lo cual representa un hallazgo preocupante. Este dato evidencia una brecha crítica en la estrategia organizacional de seguridad, pues la formación es un componente esencial para fortalecer la primera línea de defensa contra amenazas cibernéticas. Es relevante mencionar que entre los encuestados se incluye personal de TiviTrace que no pertenece al área de Tecnología de la Información (TI), lo que resalta aún más la necesidad de extender los programas de formación a todas las áreas de la organización. La falta de formación implica una mayor vulnerabilidad ante ataques de ingeniería social, errores de configuración y negligencia en la protección de accesos.

La ausencia de un programa formal de concientización incrementa significativamente la

probabilidad de incidentes derivados de factores humanos, especialmente ataques de phishing y manipulación de credenciales. Esto pone en riesgo tanto la confidencialidad como la integridad de la información gestionada por el ERP. La tendencia revela una ausencia sistemática de programas de concientización, lo cual expone a la organización a riesgos que podrían ser mitigados mediante educación básica en ciberseguridad dirigida a todos los usuarios del ERP, sin importar su función técnica o administrativa.
Se recomienda implementar capacitaciones periódicas y campañas de sensibilización que aborden amenazas comunes, mejores prácticas y protocolos de respuesta, para fortalecer la cultura organizacional en materia de seguridad.

Figura 22: Nivel de conocimiento sobre phishing entre los usuarios.



Nota: Elaboración Propia

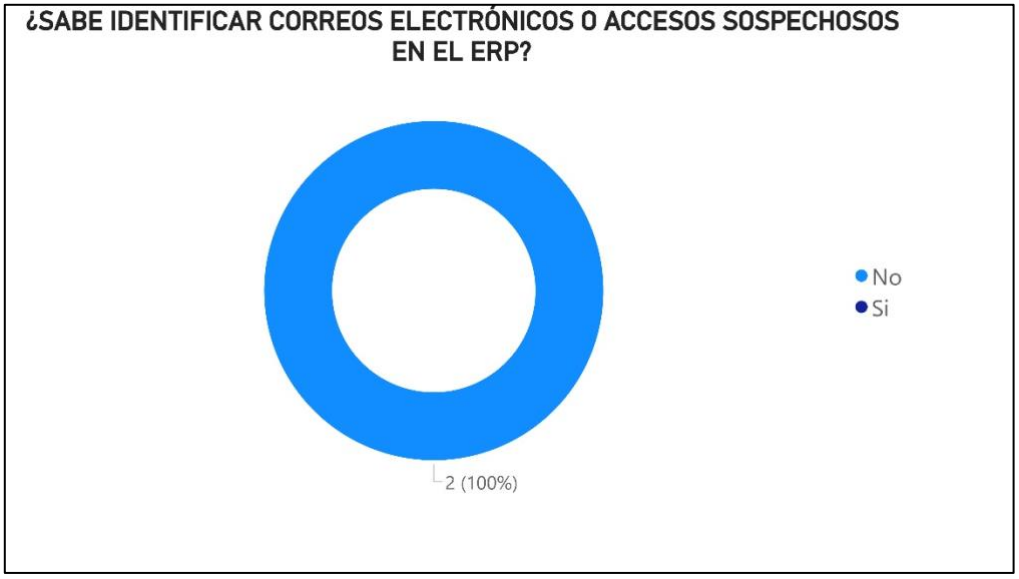
En este indicador se exploró si los empleados están familiarizados con uno de los ataques más comunes: el phishing. En la Figura 22 se muestra que ninguno de los usuarios encuestados tiene conocimiento sobre qué es el phishing ni cómo evitarlo. Es importante señalar que entre los encuestados se incluye personal de TiviTrace que no pertenece al área

de Tecnología de la Información (TI), lo que pone de manifiesto una brecha crítica en la formación en ciberseguridad más allá del ámbito técnico.

El hallazgo es grave, ya que el phishing es un método frecuente para obtener credenciales e infiltrarse en los sistemas empresariales sin que los usuarios lo adviertan. La tendencia evidencia una falta de cultura en ciberseguridad a nivel organizacional, lo cual agrava el riesgo de que las credenciales del ERP sean comprometidas.

Se recomienda que los programas de formación comiencen con temas esenciales como el phishing, brindando ejemplos prácticos, señales de alerta y pasos a seguir ante intentos sospechosos, especialmente dirigidos a usuarios no técnicos que también interactúan diariamente con el sistema.

Figura 23: Capacidad de detección de accesos sospechosos por parte de los usuarios.



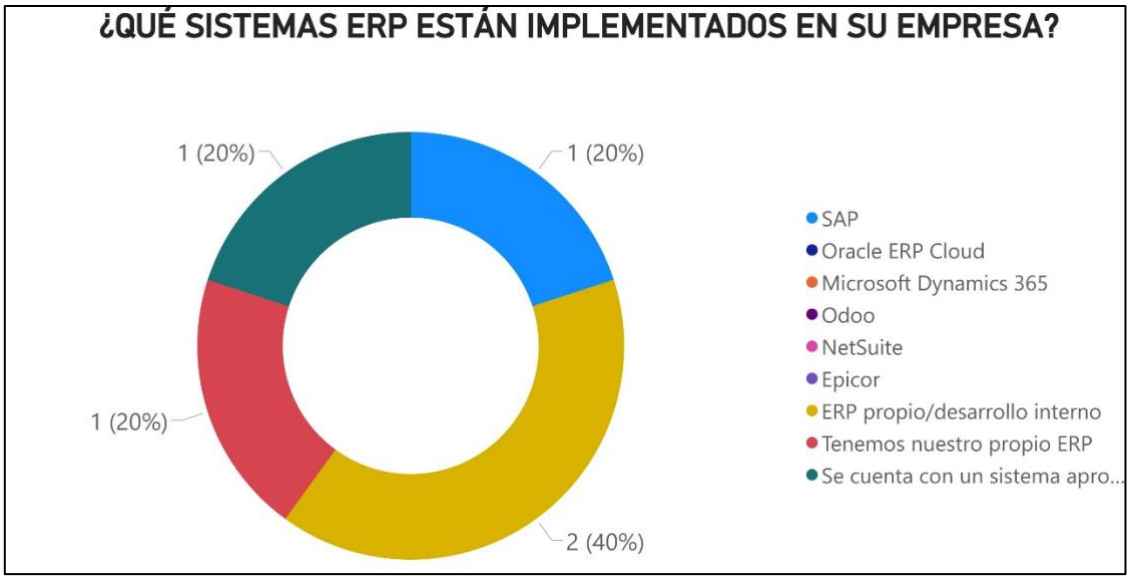
Nota: Elaboración Propia

En este indicador se analizó si los usuarios tienen habilidades para reconocer señales de posibles amenazas. En la Figura 23 se aprecia que ninguno de los encuestados es capaz de identificar correos electrónicos o accesos sospechosos. Es relevante destacar que entre los

encuestados se encuentra personal de TiviTrace ajeno al área de Tecnología de la Información (TI), lo cual pone en evidencia que esta falta de habilidades no se limita al personal técnico, sino que afecta a usuarios operativos que también interactúan con el sistema ERP.

El hallazgo revela un déficit crítico en habilidades básicas de defensa cibernética, lo que convierte a los usuarios en el eslabón más débil dentro del ecosistema de seguridad. La tendencia muestra que esta situación puede derivar en accesos no autorizados, infecciones por malware o suplantación de identidad si no se toman medidas preventivas adecuadas. Es fundamental que la empresa establezca políticas de alerta temprana y herramientas de monitoreo accesibles a todos los usuarios, además de implementar programas de capacitación que fortalezcan la capacidad del personal para detectar e informar posibles incidentes de seguridad.

Figura 24: Tipos de sistemas ERP implementados en las empresas.

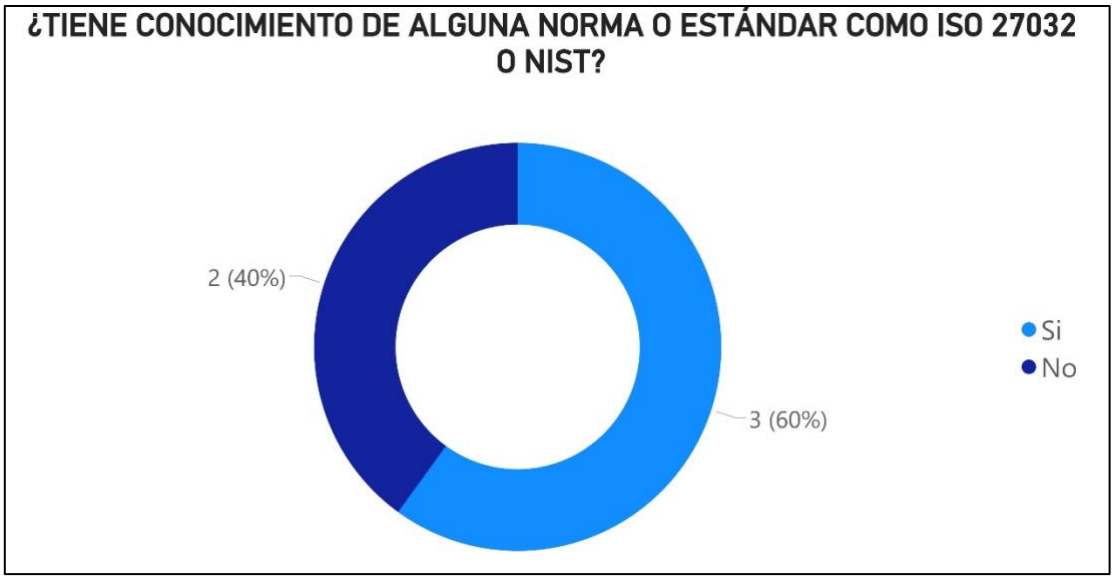


Nota: Elaboración Propia

Análisis:

En este indicador se evaluó el tipo de ERP utilizado en TiviTrace, a partir de encuestas a su personal. La figura 24 muestra que la mayoría emplea ERP desarrollados internamente, mientras que solo una empresa utiliza un sistema comercial como SAP. Esta preferencia por soluciones personalizadas puede estar motivada por necesidades específicas de la organización o limitaciones presupuestarias, lo que refleja un enfoque más flexible pero también presenta ciertos riesgos. Los ERP desarrollados internamente, si bien pueden ajustarse mejor a los procesos propios de la empresa, enfrentan desafíos importantes, como la ausencia de controles estandarizados, falta de actualizaciones regulares y mantenimiento menos riguroso. Esto puede derivar en vulnerabilidades técnicas y brechas de seguridad que incrementan la exposición a amenazas cibernéticas. Además, la dependencia de recursos internos para soporte y gestión puede limitar la capacidad de respuesta ante incidentes. Por otro lado, los ERP comerciales, como SAP, suelen incorporar prácticas de seguridad más robustas, actualizaciones periódicas y alineación con estándares internacionales, lo que contribuye a una mayor madurez en la gestión de riesgos. Sin embargo, su adopción puede implicar costos elevados y menor flexibilidad para adaptarse a requerimientos específicos. Independientemente del tipo de ERP, es fundamental aplicar las mejores prácticas de seguridad establecidas en la norma ISO/IEC 27032, enfocándose en la seguridad durante el ciclo de vida del software, el control estricto de accesos, la gestión adecuada de incidentes y la capacitación constante del personal. Esta combinación es esencial para minimizar riesgos y proteger la integridad, confidencialidad y disponibilidad de los sistemas ERP en entornos empresariales.

Figura 25: Conocimiento de normas o estándares de ciberseguridad como ISO 27032 o NIST.



Nota: Elaboración Propia

Análisis:

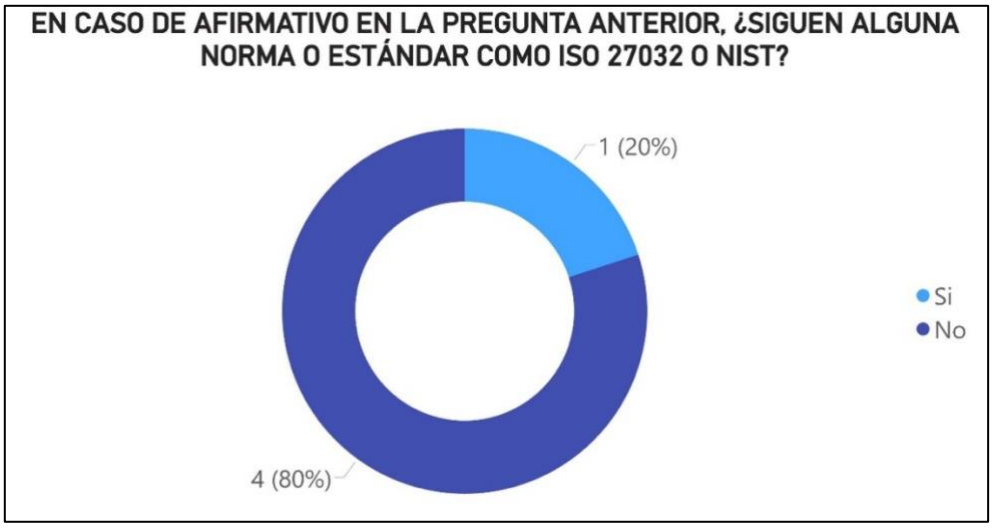
Esta pregunta permite identificar el nivel de conocimiento que poseen los colaboradores o responsables de TI respecto a marcos normativos especializados en ciberseguridad. En la figura 25 se presenta el resultado de esta consulta, donde se observa que 3 de los 5 encuestados manifestaron tener conocimiento de al menos una norma o estándar como ISO 27032 o NIST, lo que representa un 60% del total. Por otro lado, el 40% restante indicó no tener conocimiento alguno.

Este hallazgo es clave, ya que revela que, aunque existe una proporción significativa de personas familiarizadas con normas especializadas, todavía hay una parte considerable del personal que carece de dicho conocimiento. Esto puede limitar la implementación adecuada de medidas estructuradas para la gestión de riesgos, ya que los marcos como ISO/IEC 27032 y NIST proporcionan directrices validadas internacionalmente para enfrentar amenazas,

establecer políticas, desarrollar capacidades de respuesta y promover una cultura de seguridad.

La tendencia observada sugiere una evolución paulatina hacia la adopción de marcos normativos, aunque aún falta consolidar su conocimiento a nivel organizacional. Esto representa una oportunidad clara de mejora a través de procesos de capacitación formal sobre estos estándares, así como su integración en las políticas y procedimientos de seguridad existentes.

Figura 26: Aplicación de normas o estándares como ISO 27032 o NIST en la gestión de ciberseguridad.



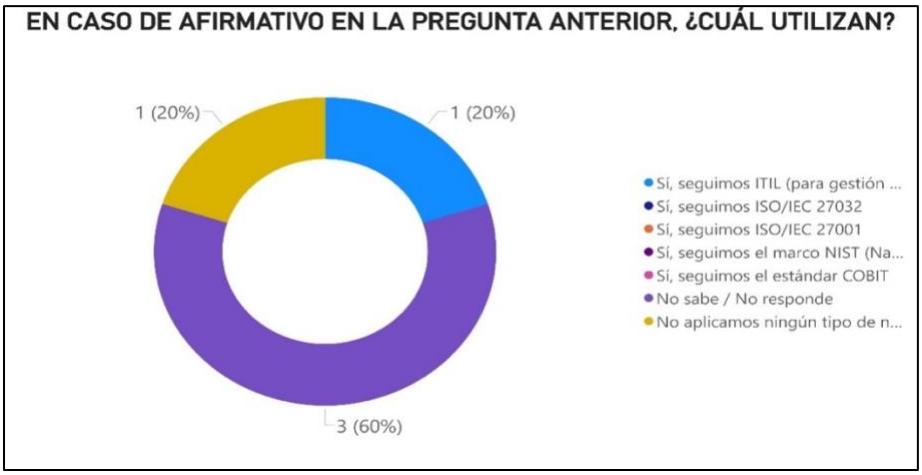
Nota: Elaboración Propia.

Análisis:

Esta pregunta indaga sobre la implementación efectiva de estándares de seguridad. Según la Figura 26, solo uno de los cinco encuestados afirmó seguir alguna norma o estándar como ISO 27032, mientras que los demás no lo hacen. Este resultado evidencia una brecha

significativa entre el conocimiento y la aplicación práctica de normas internacionales en las empresas encuestadas. Aunque el 60% de los participantes tiene conocimiento sobre estas normativas, solo un 20% las aplica en sus procesos de ciberseguridad. Esta falta de implementación limita la efectividad en la gestión y mitigación de riesgos dentro de los sistemas ERP. La tendencia detectada indica que muchas organizaciones aún no integran formalmente estos estándares en sus políticas o procedimientos de seguridad, probablemente debido a deficiencias en capacitación, falta de recursos o baja concientización sobre su importancia. Este hallazgo resalta la urgencia de fomentar un mayor compromiso y respaldo institucional para la adopción de estándares reconocidos, los cuales ofrecen un marco sólido para la protección frente a amenazas cibernéticas y la mejora continua de la postura de seguridad organizacional.

Figura 27: Normas o estándares específicos utilizados en la gestión de ciberseguridad en ERP.

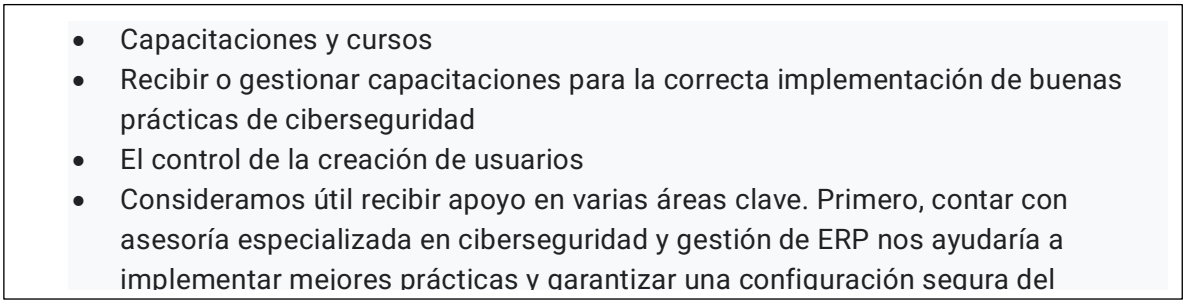


Nota: Elaboración Propia.

Análisis:

Esta pregunta profundiza en qué estándares o marcos normativos están siendo aplicados en la práctica. Según la Figura 27, la mayoría de los encuestados no aplican ninguna norma o estándar específico, o bien desconocen cuál utilizan, con cuatro de cinco respuestas indicando "No aplicamos ningún tipo de norma o estándar" o "No sabe / No responde." Solo un encuestado mencionó seguir ITIL para la gestión de servicios, incluyendo aspectos de seguridad. Este resultado reafirma que, aunque existe cierto conocimiento sobre estándares internacionales, su adopción práctica sigue siendo limitada. ITIL, como marco para la gestión de servicios de TI, es reconocido por facilitar procesos estructurados y alineados con la continuidad y seguridad del negocio, por lo que su mención es significativa. Sin embargo, la escasa adopción de normas específicas como ISO/IEC 27032 o NIST puede estar asociada a barreras como falta de formación, recursos o prioridades en la gestión de ciberseguridad. La tendencia evidenciada indica que las organizaciones aún están en etapas iniciales de madurez en la aplicación formal de estándares, lo que podría afectar la robustez de sus controles y su capacidad para mitigar riesgos complejos en plataformas ERP.

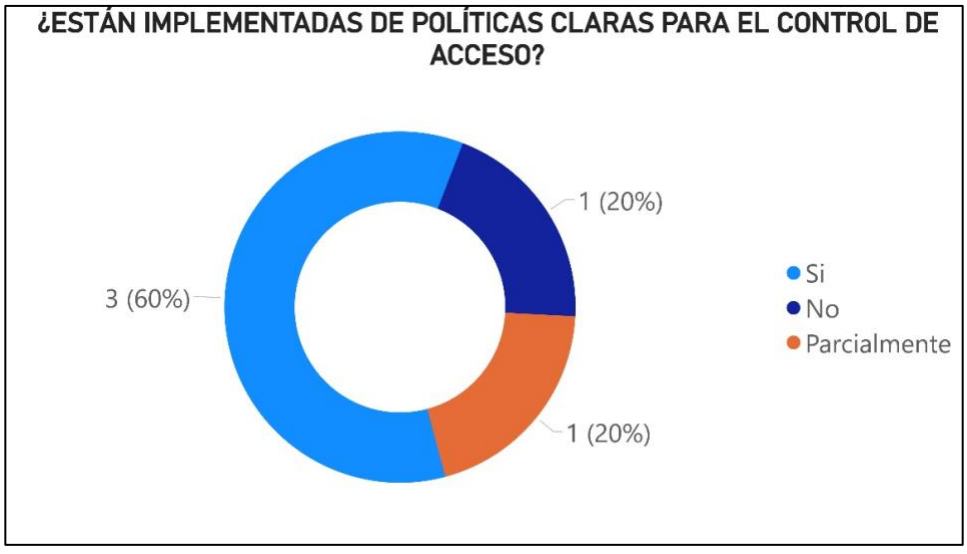
Figura 28: Tipos de apoyo necesarios para mejorar la ciberseguridad y gestión del ERP.



Análisis:

En la Figura 28 se observa que la mayoría de los encuestados coincide en la necesidad de recibir capacitaciones y cursos que faciliten la correcta implementación de buenas prácticas de seguridad. Este apoyo solicitado incluye formación continua y oportuna dirigida a los usuarios finales, aspecto fundamental para fortalecer la cultura de seguridad dentro de la organización y disminuir los riesgos relacionados con el factor humano, tales como errores o vulnerabilidades explotables. Además, se resalta la importancia de contar con asesoría experta para una configuración segura del ERP, que permita aplicar controles adecuados, gestionar correctamente la creación y administración de usuarios, y garantizar que las políticas y procedimientos estén alineados con estándares internacionales. Este tipo de soporte contribuye directamente a optimizar la gestión de riesgos cibernéticos y a alinear las prácticas de seguridad con marcos como ISO/IEC 27032, lo que resulta esencial para diseñar un plan de ciberseguridad efectivo y adaptado a las necesidades específicas del ERP empresarial.

Figura 29: Implementación de políticas claras para el control de acceso.

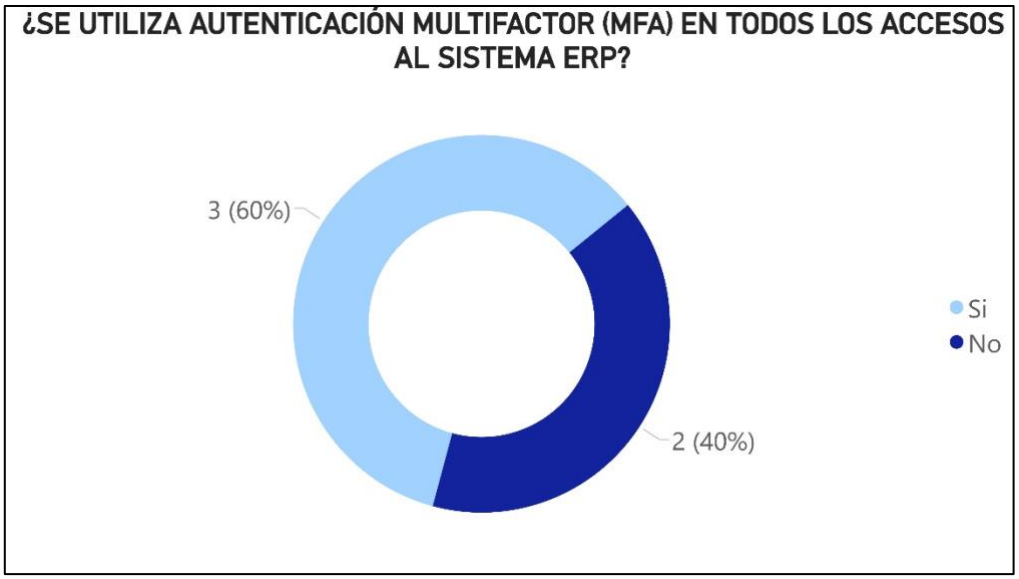


Nota: Elaboración Propia.

Análisis:

En la Figura 29 se muestra la percepción sobre la existencia de políticas claras para el control de acceso en el sistema ERP. De los cinco encuestados, tres afirmaron contar con estas políticas implementadas, uno indicó una implementación parcial, y uno manifestó no tenerlas en absoluto. Este hallazgo evidencia un avance significativo en la adopción de prácticas recomendadas por la norma ISO/IEC 27032, que establece directrices específicas para la gestión segura de accesos. Las políticas claras de control de acceso permiten garantizar que solo los usuarios autorizados tengan acceso a los recursos necesarios, lo cual es esencial para reducir riesgos de violación de datos y accesos indebidos. La tendencia indica que, si bien una mayoría ha adoptado estos controles, todavía existen áreas que requieren formalización y mejora. Esto sugiere una oportunidad para reforzar la estandarización de estas políticas dentro del entorno ERP, promoviendo así una gestión de riesgos más eficaz y alineada con los lineamientos internacionales. Se recomienda continuar fortaleciendo la implementación de estas políticas, asegurando su difusión, comprensión y cumplimiento en todos los niveles de la empresa, como parte esencial de una estrategia integral de ciberseguridad basada en la norma ISO/IEC 27032.

Figura 30: Uso de autenticación multifactor (MFA) en accesos al ERP.



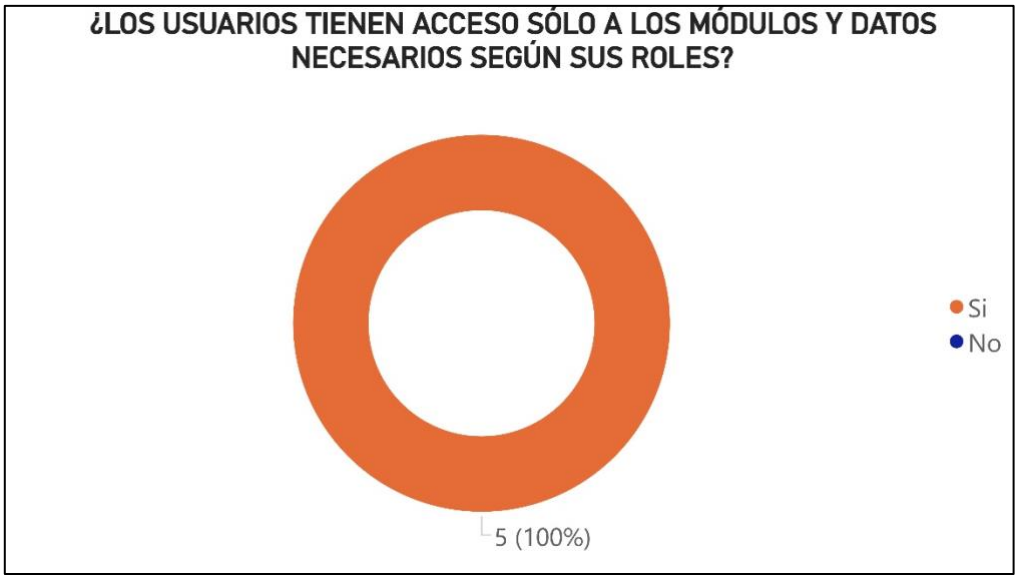
Nota: Elaboración Propia.

Análisis:

En la Figura 30 se presentan los resultados relacionados con la implementación de autenticación multifactor (MFA) en los accesos al sistema ERP. De los cinco participantes, tres indicaron que sí utilizan MFA, mientras que dos afirmaron que no. Este resultado refleja una tendencia positiva hacia el fortalecimiento de los mecanismos de autenticación, pero también pone de manifiesto áreas importantes de mejora que deben abordarse para reducir riesgos. La autenticación multifactor es una medida de seguridad crucial recomendada por la norma ISO/IEC 27032, ya que proporciona una capa adicional de protección que dificulta significativamente el acceso no autorizado al sistema. Esta técnica combina factores como algo que el usuario sabe (contraseña), algo que posee (token o dispositivo móvil) o algo que es (características biométricas), lo que incrementa la dificultad

para que atacantes puedan vulnerar el sistema solo con una contraseña. La adopción parcial de MFA refleja una brecha en la seguridad, pues la ausencia de esta medida en dos de los cinco participantes representa una vulnerabilidad considerable para la integridad, confidencialidad y disponibilidad de la información manejada por el ERP. Esta situación expone a la organización a riesgos de accesos indebidos, robo de identidad o incluso ataques internos. Además, la implementación incompleta de MFA puede ser indicativa de limitaciones en recursos tecnológicos, falta de capacitación o resistencia al cambio, aspectos que deben ser abordados para garantizar una adopción integral y efectiva. Fortalecer esta área contribuirá a elevar el nivel general de seguridad y a cumplir con las mejores prácticas internacionales, reduciendo la probabilidad de incidentes relacionados con la autenticación débil.

Figura 31: Restricción de acceso de usuarios a módulos y datos según roles.



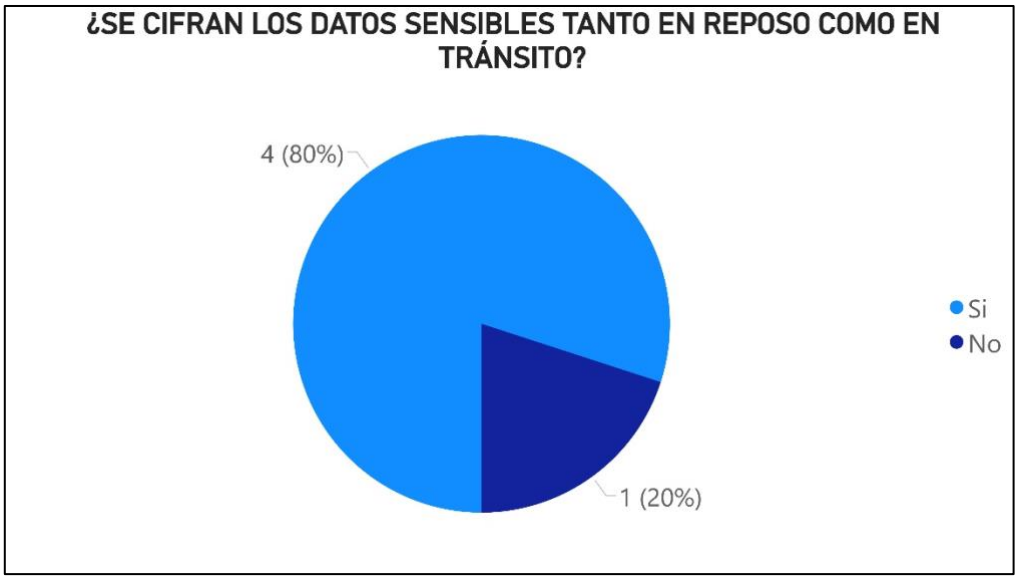
Nota: Elaboración Propia.

Análisis:

En la Figura 31 se observa un consenso total entre los encuestados, ya que todos afirmaron que los usuarios tienen acceso únicamente a los módulos y datos necesarios conforme a sus roles asignados dentro del sistema ERP. Este resultado refleja una práctica alineada con los principios de seguridad que recomienda la norma ISO/IEC 27032, especialmente en la implementación del control de acceso basado en roles. La restricción de acceso según roles es una medida fundamental para limitar la exposición de información sensible y minimizar el riesgo de accesos no autorizados, que pueden resultar en incidentes de seguridad como robo, manipulación o pérdida de datos críticos. Este enfoque contribuye a mantener la integridad, confidencialidad y disponibilidad de la información dentro del sistema ERP, al garantizar que cada usuario solo tenga los privilegios estrictamente necesarios para cumplir sus funciones.

La uniformidad en las respuestas sugiere que en TiviTrace existe una gestión formal y coherente en la asignación de permisos, evidenciando una clara definición de responsabilidades y funciones dentro del sistema. Esto reduce la probabilidad de errores humanos, abusos de privilegios y fugas internas, que son vulnerabilidades comunes en sistemas empresariales complejos. La tendencia observada indica un nivel maduro en la administración de accesos, lo que fortalece la postura de seguridad general del ERP. Esta práctica no solo disminuye la superficie de ataque al limitar las vías de ingreso para actores maliciosos, sino que también facilita la auditoría y monitoreo, permitiendo detectar y responder rápidamente ante posibles incidentes. Finalmente, mantener un control de accesos estricto y actualizado es clave para asegurar la resiliencia y continuidad operacional de la organización frente a amenazas internas y externas.

Figura 32: Cifrado de datos sensibles en reposo y en tránsito.



Nota: Elaboración Propia.

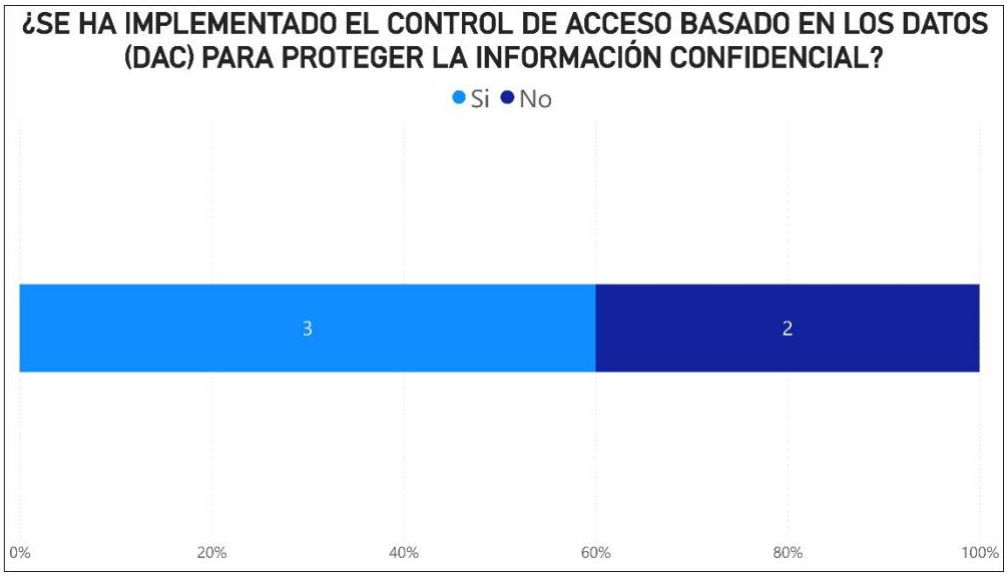
Análisis:

En la Figura 32 se observa que cuatro de los cinco encuestados confirmaron que los datos sensibles en el sistema ERP se cifran tanto en reposo como en tránsito, mientras que uno indicó que no se realiza esta práctica. El cifrado de datos es una medida esencial para proteger la información frente a accesos no autorizados y posibles interceptaciones, garantizando la confidencialidad e integridad de los datos en todas las etapas de su manejo. La mayoría que implementa esta medida refleja un buen nivel de adopción de las mejores prácticas recomendadas en la norma ISO/IEC 27032.

Sin embargo, la existencia de al menos una respuesta negativa señala una brecha de seguridad importante que debe ser atendida, ya que la falta de cifrado expone datos sensibles a riesgos elevados, tanto en almacenamiento como en transmisión, así mismo; la tendencia

general muestra un avance favorable en la protección de datos, pero también evidencia la necesidad de estandarizar esta práctica para lograr una protección uniforme y robusta en todo el sistema ERP.

Figura 33: Implementación del control de acceso basado en datos (DAC).



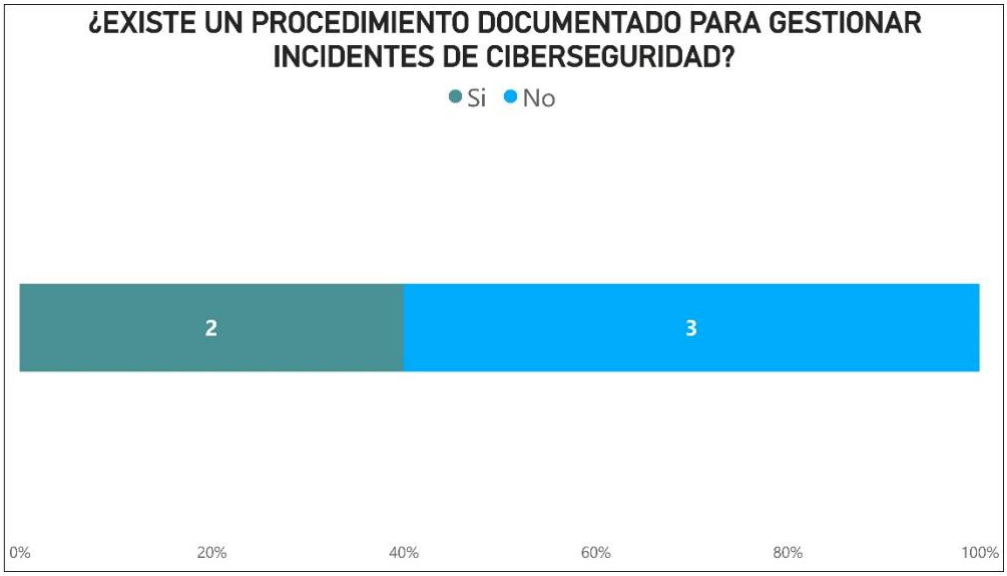
Nota: Elaboración Propia

Análisis:

En la Figura 33 se observa que tres de los cinco encuestados indicaron implementar controles de acceso discrecional (DAC, por sus siglas en inglés), mientras que dos afirmaron no hacerlo. El control DAC es un mecanismo de seguridad que otorga a los propietarios o administradores de recursos la capacidad de decidir quién puede acceder a sus datos, estableciendo permisos basados en criterios específicos y personalizables para proteger información sensible dentro del sistema ERP.

La implementación de DAC contribuye significativamente a la seguridad del ERP al limitar el acceso a información confidencial únicamente a usuarios autorizados, lo que ayuda a prevenir filtraciones, modificaciones no autorizadas o eliminaciones accidentales de datos críticos. Además, permite una mayor flexibilidad para adaptar los controles a necesidades particulares de la organización o de ciertos procesos, favoreciendo un enfoque granular en la protección de activos digitales. Sin embargo, el hecho de que dos encuestados no apliquen este tipo de control revela brechas importantes en la política de seguridad de acceso, que pueden traducirse en riesgos considerables para la integridad y confidencialidad del ERP. La ausencia o deficiente implementación de DAC puede facilitar accesos indebidos, aumentos de privilegios no controlados y una mayor exposición frente a amenazas internas y externas. La tendencia detectada refleja avances en la adopción de prácticas de seguridad, pero también evidencia la necesidad urgente de fortalecer y estandarizar el uso de controles DAC dentro de la organización. Esto implica no solo implementar la tecnología y los procedimientos adecuados, sino también capacitar al personal responsable y monitorear constantemente la efectividad de estos controles para asegurar una protección robusta y continua de los activos informáticos.

Figura 34: Existencia de procedimiento documentado para gestionar incidentes.



Nota: Elaboración Propia

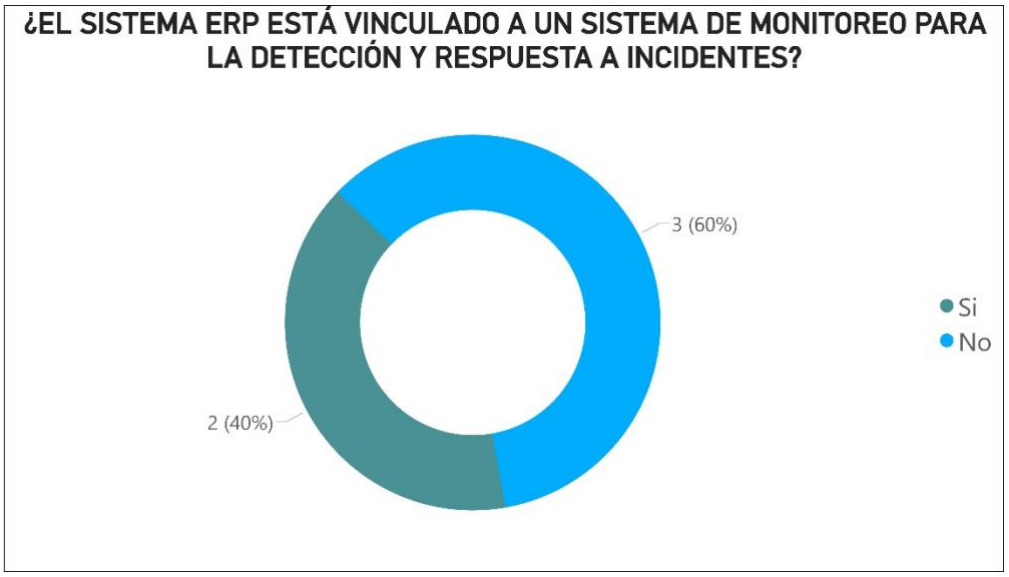
Análisis:

En la Figura 34 se observa que solo dos de los cinco encuestados cuentan con un procedimiento documentado para la gestión de incidentes de seguridad, mientras que los tres restantes carecen de este recurso fundamental. Esta situación revela una carencia significativa en la formalización de procesos críticos para la identificación, respuesta y resolución eficiente de incidentes cibernéticos dentro del entorno ERP. La ausencia de procedimientos documentados puede generar respuestas descoordinadas o tardías ante eventos adversos, aumentando la probabilidad de impactos negativos en la confidencialidad, integridad y disponibilidad de la información. Además, dificulta la asignación clara de responsabilidades, la comunicación interna y externa, así como la trazabilidad y aprendizaje de los incidentes ocurridos.

La tendencia identificada indica que la estandarización y formalización de la gestión de incidentes aún es incipiente en la organización, lo que representa un riesgo para la resiliencia operativa y la capacidad de recuperación frente a ataques o fallos técnicos. Este hallazgo enfatiza la urgencia de diseñar, documentar y socializar protocolos específicos para la gestión de incidentes, asegurando que todo el personal implicado conozca sus roles y procedimientos a seguir.

Implementar un marco formal alineado con buenas prácticas internacionales, como las recomendadas en ITIL V4 e ISO/IEC 27032, permitirá fortalecer la seguridad del ERP y reducir el tiempo de respuesta ante incidentes, minimizando el impacto operativo y reputacional. En conclusión, esta mejora es fundamental para consolidar una postura proactiva y preparada frente a las amenazas cibernéticas.

Figura 35: Vinculación del ERP a un sistema de monitoreo para detección y respuesta.



Nota: Elaboración Propia

Análisis:

En la Figura 35 se constata que únicamente dos encuestados han vinculado su sistema ERP a una solución de monitoreo para la detección y respuesta ante incidentes, mientras que los tres restantes no cuentan con esta integración. Este hallazgo refleja una debilidad importante en la capacidad de vigilancia activa de los sistemas críticos de la organización, lo que pone en riesgo la detección temprana de actividades anómalas, accesos indebidos o posibles ataques cibernéticos. El monitoreo continuo es una práctica esencial recomendada tanto por la norma ISO/IEC 27032 como por los marcos de gestión de servicios como ITIL V4. Estas buenas prácticas promueven la implementación de soluciones que permitan no solo la observación en tiempo real del comportamiento del sistema, sino también la generación automática de alertas ante eventos sospechosos, facilitando así una respuesta oportuna que minimice daños.

La carencia de estas herramientas en la mayoría de los casos analizados implica que los sistemas ERP están operando con una visibilidad limitada de su propio entorno, lo cual impide anticiparse a las amenazas y reduce significativamente la capacidad de reacción. Además, al no contar con registros detallados de eventos, se dificulta la realización de análisis forense posterior a un incidente, así como la mejora continua del sistema. La tendencia identificada indica un nivel incipiente de madurez en la adopción de soluciones de monitoreo, lo que representa una oportunidad de mejora prioritaria. Es fundamental que la organización avance hacia la implementación de plataformas centralizadas de monitoreo y respuesta, capaces de correlacionar eventos y automatizar respuestas ante incidentes, permitiendo una

protección más efectiva y alineada con los requerimientos actuales de ciberseguridad en entornos empresariales. Integrar el ERP a este tipo de soluciones no solo fortalece la postura de seguridad, sino que también optimiza los recursos del área de TI al facilitar una gestión más proactiva y eficiente.

Figura 36: Revisión periódica de incidentes pasados para reforzar la seguridad.

Nota: Elaboración Propia.

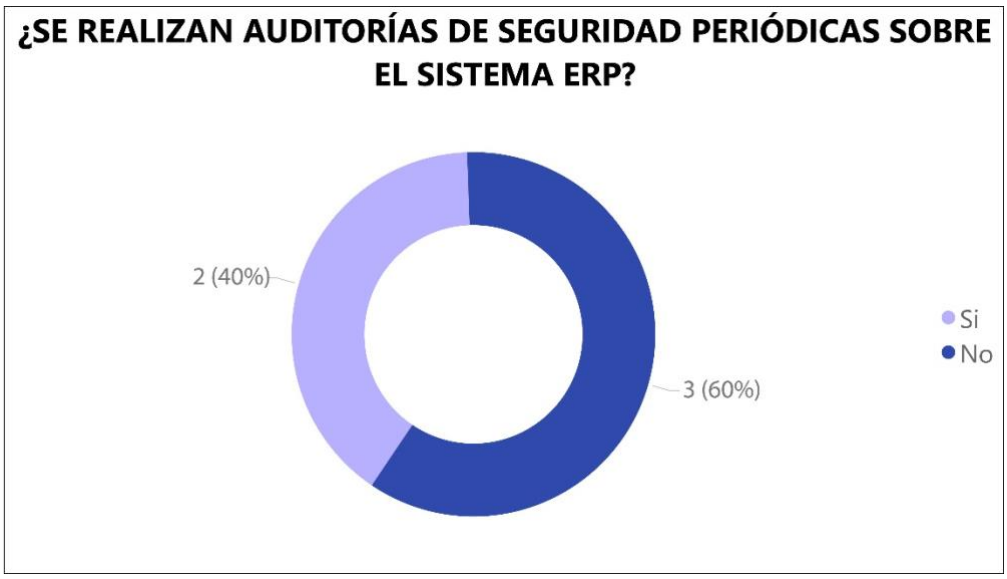
Análisis:

En la Figura 36 se muestra que la totalidad de los encuestados manifestó realizar revisiones periódicas de incidentes previos con el objetivo de mejorar la seguridad del sistema ERP. Este resultado constituye un indicador altamente positivo, ya que refleja una cultura organizacional orientada hacia la mejora continua, en línea con lo establecido por la

norma ISO/IEC 27032 y el marco ITIL V4. Según ISO/IEC 27032, el análisis posterior a los incidentes es una práctica clave dentro de la gestión de ciberseguridad, ya que permite identificar debilidades en los controles existentes, entender el comportamiento de las amenazas y prevenir recurrencias. Asimismo, esta revisión facilita la actualización de políticas, procedimientos y herramientas en función de evidencia concreta, fortaleciendo así la postura de seguridad de la organización. Desde la perspectiva de ITIL V4, esta práctica se alinea con el proceso de gestión de problemas, que busca no solo resolver incidentes, sino también encontrar y eliminar sus causas raíz. El hecho de que todos los participantes reporten realizar este tipo de análisis sugiere un enfoque más maduro y proactivo en la gestión de riesgos, promoviendo un ciclo de retroalimentación que contribuye tanto a la resiliencia operativa como a la continuidad del negocio.

Este hallazgo también indica que, aunque aún existen otras áreas con debilidades como la falta de monitoreo o documentación formal de procedimientos, la revisión post-incidente representa una base sólida sobre la cual construir procesos más robustos y alineados a los estándares internacionales. Implementar sistemáticamente estas revisiones dentro de un marco de gestión formal puede permitir a la organización optimizar la asignación de recursos, priorizar inversiones en ciberseguridad y aumentar la capacidad de respuesta frente a nuevas amenazas.

Figura 37: Realización de auditorías de seguridad periódicas sobre el sistema ERP.



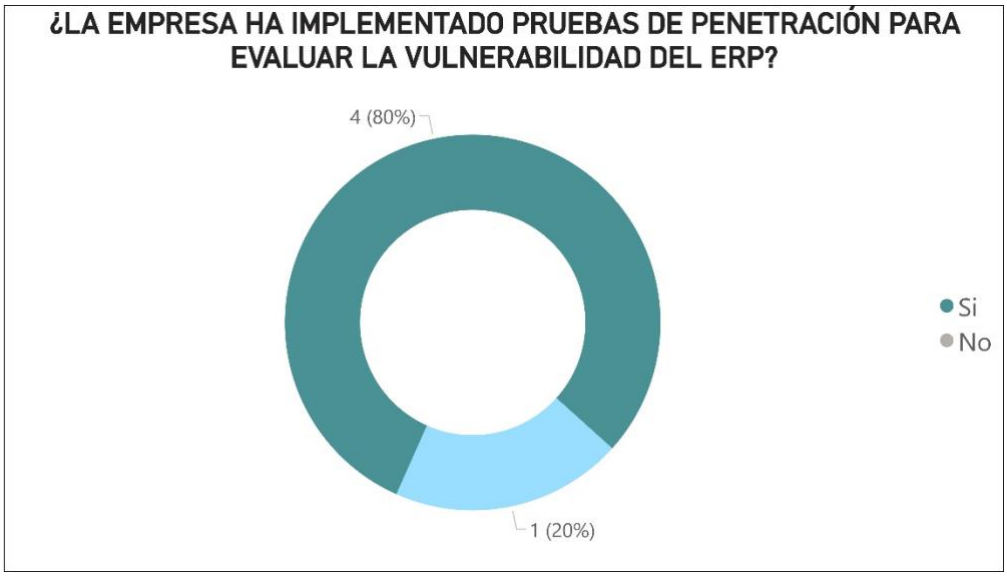
Nota: Elaboración Propia.

Análisis:

La Figura 37 indica que solo dos de los cinco encuestados realizan auditorías de seguridad periódicas en su sistema ERP, mientras que tres no las aplican. Este resultado señala una debilidad importante en la validación continua de la seguridad, lo cual incrementa el riesgo de que brechas no identificadas sean explotadas. Según ITIL V4, las auditorías periódicas forman parte del ciclo de mejora continua y son fundamentales para evaluar el rendimiento, la eficacia de los controles y el cumplimiento de políticas, todo enmarcado en la gobernanza del servicio. Asimismo, la norma ISO/IEC 27032 enfatiza que las auditorías permiten identificar vulnerabilidades latentes, validar la integridad del sistema y asegurar la adecuación de las medidas frente a amenazas emergentes. La ausencia de estas prácticas refleja una baja madurez en la gestión estructurada de la seguridad del ERP y limita la capacidad de anticipación frente a riesgos. Por ello, es necesario incorporar auditorías

regulares como parte del sistema de gestión de ciberseguridad, garantizando alineación con los marcos internacionales y fortaleciendo la resiliencia de la infraestructura tecnológica.

Figura 38: Implementación de pruebas de penetración en el sistema ERP.



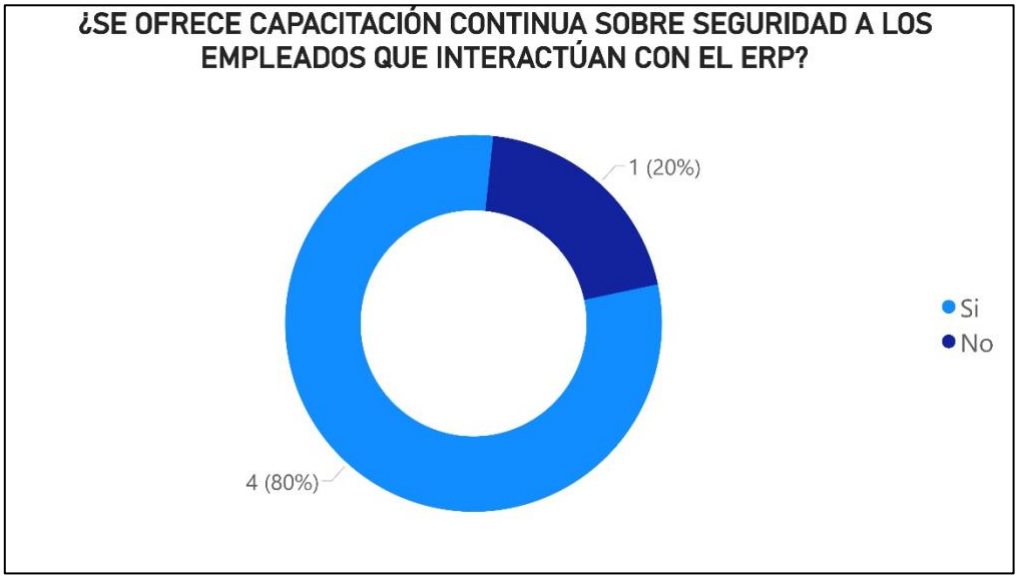
Nota: Elaboración Propia.

Análisis:

La Figura 38 evidencia que cuatro de los cinco encuestados implementan pruebas de penetración en el sistema ERP, mientras que uno no las ha adoptado. Esta tendencia refleja un enfoque positivo hacia la detección proactiva de vulnerabilidades, en línea con las recomendaciones de la norma ISO/IEC 27032, que promueve la identificación temprana de riesgos mediante técnicas ofensivas controladas. Las pruebas de penetración permiten simular ataques reales para evaluar la robustez del sistema, contribuyendo directamente a la gestión de riesgos y al fortalecimiento de los controles preventivos. Desde el enfoque de mejora continua de ITIL V4, estas pruebas también forman parte de la retroalimentación

operativa que impulsa la evolución constante de los servicios de TI. No obstante, el hecho de que uno de los participantes no realice estas evaluaciones sugiere una cobertura aún incompleta, lo cual podría dejar áreas críticas del ERP sin validar. Para alcanzar una postura de seguridad más integral, es esencial que las pruebas de penetración se institucionalicen como parte de las auditorías técnicas periódicas del sistema.

Figura 39: Capacitación continua sobre seguridad en el sistema ERP.



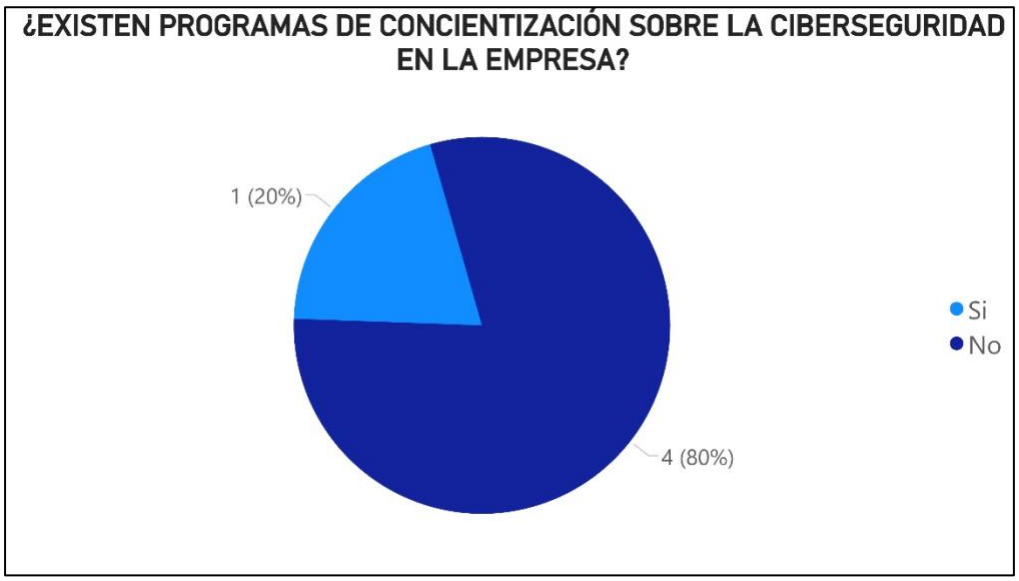
Nota: Elaboración Propia.

Análisis:

En la Figura 39 se analizan las respuestas relacionadas con la capacitación continua en ciberseguridad para los empleados que utilizan el sistema ERP. Cuatro de los cinco encuestados afirmaron que sí se proporciona este tipo de formación, mientras que uno indicó que no. Este resultado revela una tendencia positiva hacia la formación regular del personal, un aspecto clave en la implementación de buenas prácticas recomendadas por la norma ISO/IEC 27032. La capacitación constante es esencial para fortalecer la conciencia en seguridad, minimizar errores humanos y prevenir ataques como el phishing o la fuga de

información. Aunque la mayoría de los participantes señaló contar con estas capacitaciones, la existencia de una respuesta negativa pone en evidencia una posible brecha en la cobertura total de esta práctica dentro de la empresa.

Figura 40: Existencia de programas de concientización sobre la ciberseguridad en la empresa.



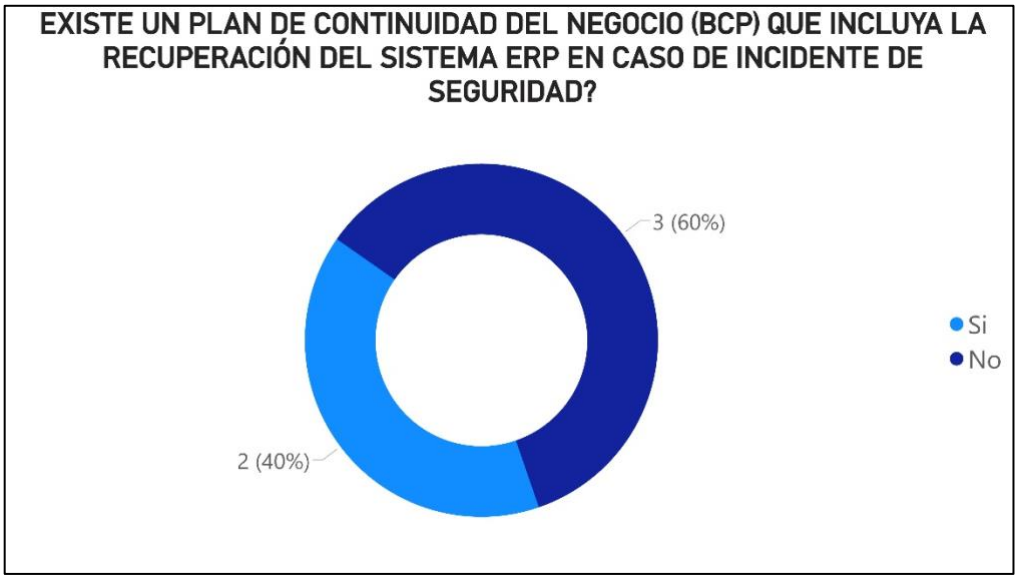
Nota: Elaboración Propia.

Análisis:

En la Figura 40 se presenta la percepción respecto a la existencia de programas de concientización sobre ciberseguridad. De los cinco encuestados, solo uno indicó que sí existen dichos programas en la empresa, mientras que los otros cuatro señalaron que no. Este hallazgo pone en evidencia una debilidad importante en la implementación de las buenas prácticas recomendadas por la norma ISO/IEC 27032, ya que la concientización es una de las herramientas más eficaces para fortalecer la postura de seguridad organizacional. La ausencia de estos programas puede aumentar el riesgo de incidentes provocados por el desconocimiento o el error humano. La tendencia observada refleja que, aunque hay un

primer paso en una de las áreas evaluadas, todavía no se ha consolidado una cultura de seguridad sólida que abarque a todo el personal de la empresa.

Figura 41: Existencia de un plan de continuidad del negocio (BCP) que incluya la recuperación del sistema ERP.



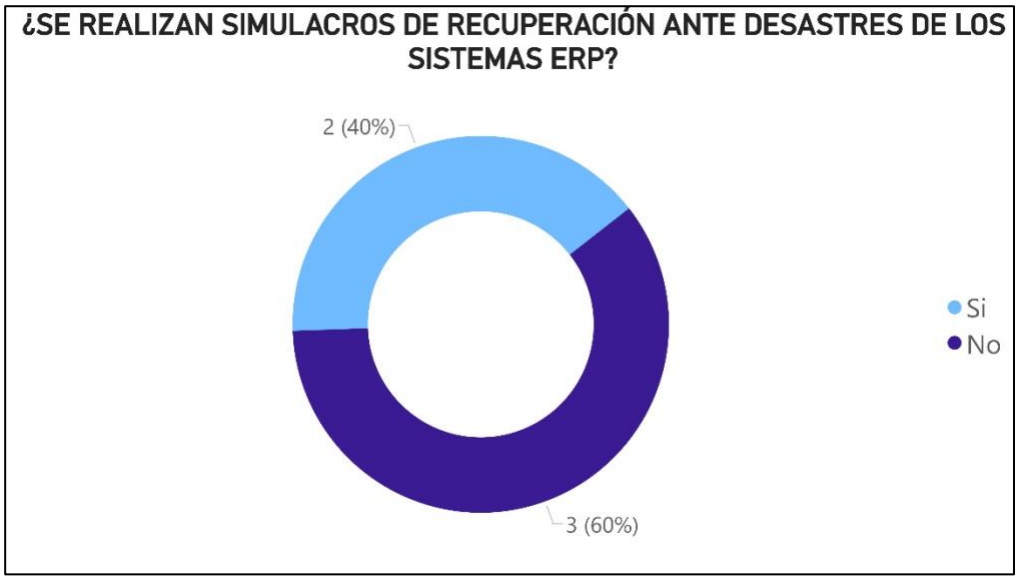
Nota: Elaboración Propia.

Análisis:

La Figura 41 revela que únicamente dos de los cinco encuestados afirmaron contar con un plan de continuidad del negocio (BCP) que incluya la recuperación del sistema ERP en caso de incidentes de seguridad, mientras que tres manifestaron no disponer de esta herramienta crítica. Este resultado pone en evidencia una carencia importante en términos de preparación organizacional frente a escenarios de interrupción, lo cual puede traducirse en mayores tiempos de inactividad, pérdida de datos, impacto financiero y deterioro de la confianza de los clientes y usuarios internos. La existencia de un BCP alineado con las mejores prácticas de ITIL V4 permite garantizar la entrega continua de servicios esenciales, incluso ante fallas mayores, al establecer protocolos claros de recuperación, asignación de roles, análisis de impacto y pruebas periódicas. La falta de este tipo de planificación

estructurada no solo representa un riesgo operativo, sino también un incumplimiento de estándares internacionales que promueven la resiliencia digital como componente central de la gestión de ciberseguridad. Si bien algunos actores han tomado medidas proactivas para incorporar esta práctica, la mayoría aún no ha alcanzado un nivel mínimo de preparación, lo que deja al sistema ERP en una situación vulnerable frente a contingencias que, de materializarse, podrían tener consecuencias críticas para la continuidad del negocio.

Figura 42: Realización de simulacros de recuperación ante desastres de los sistemas ERP.



Nota: Elaboración Propia.

Análisis:

En la Figura 42 se presentan las respuestas relacionadas con la realización de simulacros de recuperación ante desastres en los sistemas ERP. Dos de los cinco participantes afirmaron que sí se llevan a cabo estos simulacros, mientras que tres indicaron que no se realizan. Este resultado muestra que, aunque existe cierta iniciativa en algunos sectores para preparar al personal y al sistema frente a eventos críticos, la mayoría aún no contempla ejercicios prácticos que permitan evaluar la eficacia de sus planes de recuperación. La ausencia de

simulacros puede generar una falsa sensación de seguridad y dificultar la respuesta oportuna ante un incidente real. Además, limita la capacidad de identificar fallos en los procedimientos o tiempos de recuperación, comprometiendo la continuidad operativa.

4.1.9 RECOLECCIÓN DE INSUMOS PARA LA FORMULACIÓN DE ESTRATEGIAS DE DETECCIÓN Y MITIGACIÓN DE AMENAZAS PERSISTENTES AVANZADAS (APT) EN ERP EMPRESARIALES, SEGÚN LA NORMA ISO/IEC 27032.

Para dar cumplimiento al objetivo tres, orientado a definir estrategias de detección y mitigación de Amenazas Persistentes Avanzadas (APT) en sistemas ERP empresariales, se analizó la experiencia, percepción y participación de los usuarios de TiviTrace en relación con la seguridad del sistema. A través de diversas secciones de la encuesta, se identificaron brechas en mecanismos de protección, debilidades en controles de acceso y una necesidad de mayor comunicación sobre las políticas de ciberseguridad. Estos hallazgos sirven como base para delinear estrategias efectivas que se alineen con los controles propuestos en la norma ISO/IEC 27032.

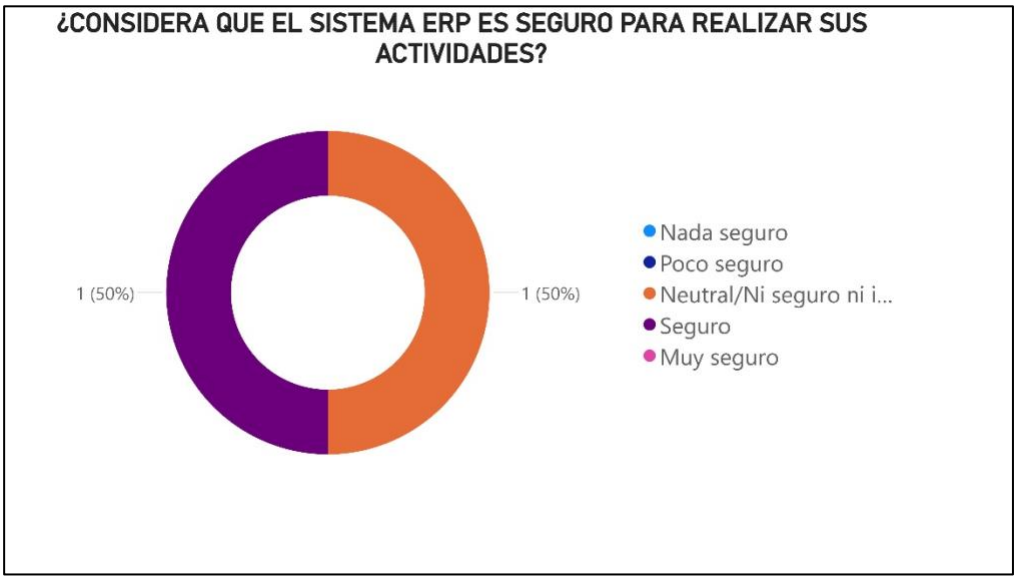
Figura 43: Historial de incidentes de seguridad reportados por los usuarios.

Nota: Elaboración Propia.

Análisis:

Para este indicador se investigó si los usuarios han tenido experiencias previas con problemas de seguridad en el ERP. En la Figura 40 se observa que ningún usuario ha reportado incidentes de seguridad al usar el ERP. Es importante señalar que entre los encuestados se incluye personal de TiviTrace que no pertenece al área de Tecnología de la Información (TI), lo que sugiere que la ausencia de reportes no solo puede deberse a la inexistencia de eventos notorios, sino también a la falta de formación y conciencia entre usuarios no técnicos para identificar y comunicar este tipo de situaciones. El hallazgo apunta a una posible carencia de mecanismos formales para reportar incidentes o a una percepción generalizada de que dichos eventos no son relevantes o no requieren ser informados. La tendencia resalta la necesidad de establecer canales de reporte claros, accesibles y acompañados de campañas internas que fomenten la responsabilidad compartida en la protección del sistema.

Figura 44: Percepción de seguridad del ERP por los usuarios.



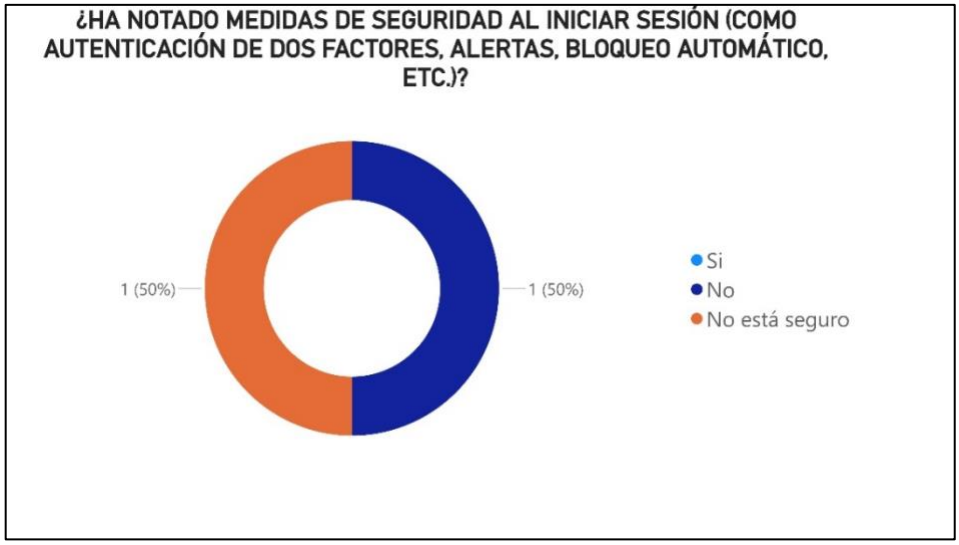
Nota: Elaboración Propia.

Análisis:

Para este indicador se evaluó la percepción general sobre la seguridad del sistema. En la Figura 44 se aprecia una diversidad de respuestas: algunos usuarios consideran el sistema seguro, mientras que otros se mantienen neutrales o inseguros. Es importante destacar que entre los encuestados se encuentra personal de TiviTrace que no pertenece al área de Tecnología de la Información (TI), lo cual revela que la percepción ambigua sobre la seguridad del sistema no se limita al ámbito técnico, sino que abarca a usuarios operativos que interactúan diariamente con el ERP. El hallazgo refleja una percepción mixta y poco clara respecto a la protección del sistema, lo que puede ser indicativo de una carencia de transparencia en los controles implementados o de un desconocimiento general sobre las medidas de seguridad vigentes. La tendencia apunta a una desconfianza parcial, lo cual sugiere que los usuarios requieren mayor información y visibilidad sobre cómo el ERP protege los datos sensibles. Se recomienda fortalecer la comunicación interna sobre las

políticas y mecanismos de ciberseguridad implementados, con el objetivo de reforzar la confianza de todos los colaboradores en la herramienta tecnológica.

Figura 45: Reconocimiento de medidas de seguridad al inicio de sesión.



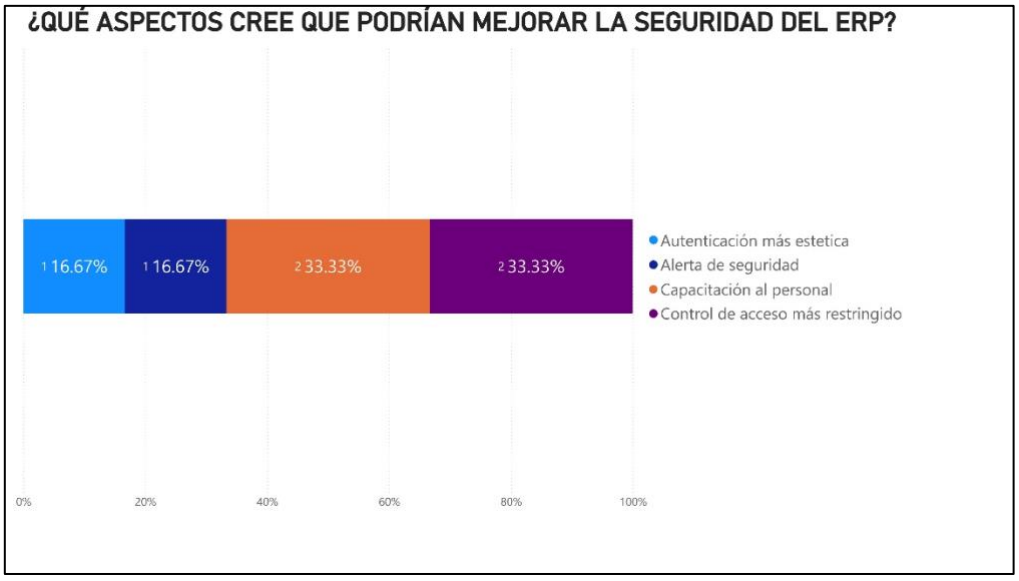
Nota: Elaboración Propia.

Análisis:

Para este indicador se evaluó si los usuarios perciben elementos visibles de seguridad al momento de autenticarse en el sistema. En la Figura 45 se indica que la mayoría de los usuarios no ha notado la presencia de medidas de seguridad evidentes, como autenticación de dos factores o bloqueos automáticos tras intentos fallidos. Cabe señalar que entre los encuestados se incluye personal de TiviTrace que no pertenece al área de Tecnología de la Información (TI), lo que indica que esta percepción no es exclusiva de los usuarios técnicos, sino que también afecta a quienes utilizan el sistema en funciones operativas. El hallazgo evidencia una posible debilidad del sistema en lo referente a barreras de ingreso, lo cual compromete la integridad de los accesos y aumenta la exposición a intrusiones no autorizadas. La tendencia muestra una ausencia de mecanismos avanzados de control de

acceso, lo que abre la puerta a posibles accesos indebidos en caso de que las credenciales de los usuarios sean comprometidas. Como medida correctiva, se recomienda implementar controles de autenticación más robustos y asegurar su visibilidad para los usuarios, con el fin de elevar tanto la protección efectiva como la percepción de seguridad del sistema.

Figura 46: Propuestas de mejora en seguridad del ERP.



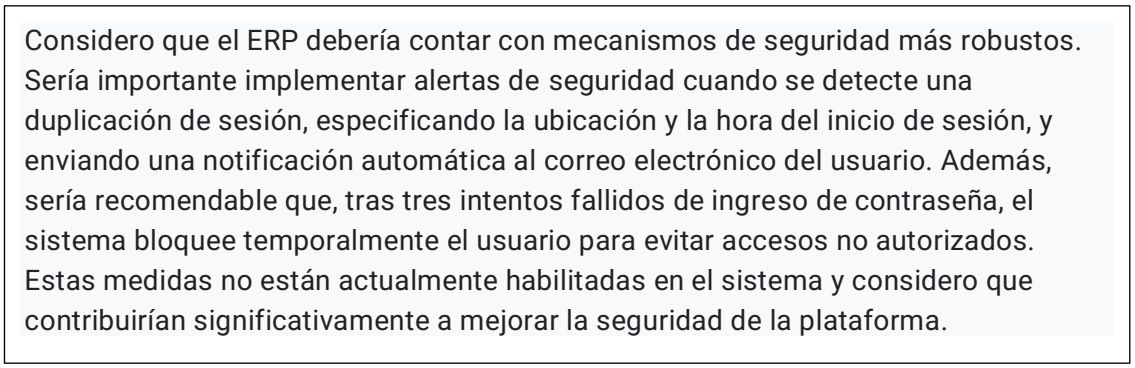
Nota: Elaboración Propia.

Análisis:

La figura 46 muestra las sugerencias de los usuarios para mejorar la ciberseguridad del sistema ERP, entre las que destacan la implementación de mecanismos de autenticación más estrictos, la activación de alertas de seguridad en tiempo real, el bloqueo automático tras múltiples intentos fallidos de acceso y la capacitación constante del personal. Estos aportes reflejan un nivel significativo de conciencia sobre los aspectos críticos que afectan la protección del sistema, especialmente en cuanto al control de accesos, que es identificado como una debilidad clave. Este reconocimiento por parte de los usuarios subraya la importancia de fortalecer las medidas de seguridad técnica y humana, alineándose con las

recomendaciones de estándares como ISO/IEC 27032 e ITIL V4, para minimizar riesgos asociados a accesos no autorizados y errores operativos. La tendencia evidencia una predisposición favorable hacia la adopción de prácticas y tecnologías que pueden elevar la postura de seguridad de la organización, así como la necesidad de programas de sensibilización que refuercen el compromiso de todos los colaboradores con la ciberseguridad del ERP.

Figura 47: Comentarios adicionales sobre la seguridad del ERP.



Nota: Elaboración Propia.

Análisis:

Para esta recolección de datos se solicitó a los encuestados brindar comentarios abiertos relacionados con su percepción sobre la seguridad del ERP. En la figura 47 se presentan diversas opiniones recopiladas por medio de esta pregunta abierta. Entre los comentarios más relevantes destacan sugerencias como la implementación de sistemas de alerta para detectar duplicación de sesiones, bloqueos automáticos tras varios intentos fallidos de ingreso, y el envío de notificaciones a través de correo electrónico ante accesos sospechosos o actividades no usuales en el sistema. Estas observaciones reflejan un conocimiento práctico por parte de los usuarios sobre situaciones que podrían comprometer

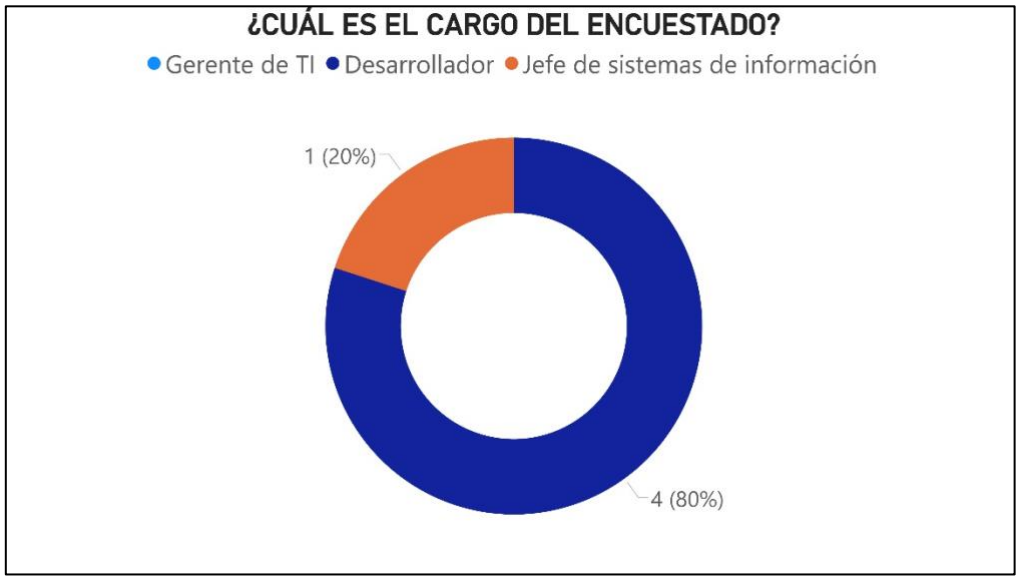
la seguridad y evidencian la necesidad de controles preventivos y de respuesta que fortalezcan la arquitectura del sistema ERP. El hallazgo más significativo es la preocupación generalizada de los usuarios por la ausencia de mecanismos visibles de protección que les brinden confianza. Esta falta de señales de seguridad puede traducirse en una falsa sensación de vulnerabilidad, lo que podría impactar negativamente en la percepción de confiabilidad del sistema. La tendencia observada es un interés activo por parte de los usuarios en contar con políticas de seguridad más robustas, claras y comunicadas, lo cual evidencia la importancia de que los planes de ciberseguridad no solo se implementen técnicamente, sino que también sean socializados con los usuarios finales para fomentar una cultura de seguridad participativa.

4.1.10 IDENTIFICACIÓN DE ACTIVOS POR CATEGORÍA DE RIESGO Y ALTERNATIVAS DE RECUPERACIÓN ALINEADAS CON ITIL V4 PARA LA CONTINUIDAD DEL ERP

Para cumplir este objetivo, se analizó la situación específica de una empresa que utiliza un sistema ERP desarrollado internamente. Se evaluaron distintos aspectos relacionados con la gestión de activos, la estructura del equipo tecnológico, la experiencia en ciberseguridad, los módulos críticos utilizados, así como las prácticas actuales de respuesta ante incidentes, protección de datos y continuidad del negocio. La empresa cuenta con un equipo técnico reducido, principalmente compuesto por desarrolladores, sin roles exclusivos de ciberseguridad ni procedimientos formales para gestión de cambios o respuesta a incidentes. Tampoco dispone de un plan de continuidad del negocio específicamente enfocado en el ERP. A pesar de ello, se aplican controles básicos como el cifrado de datos y el control de acceso por roles. Estos hallazgos permiten clasificar los activos según su criticidad y proponer alternativas de respuesta y recuperación alineadas con ITIL V4, con el

fin de fortalecer la resiliencia operativa del sistema ERP y garantizar la continuidad del negocio frente a eventos disruptivos.

Figura 48: Distribución de cargos de los encuestados en relación con la ciberseguridad ERP.



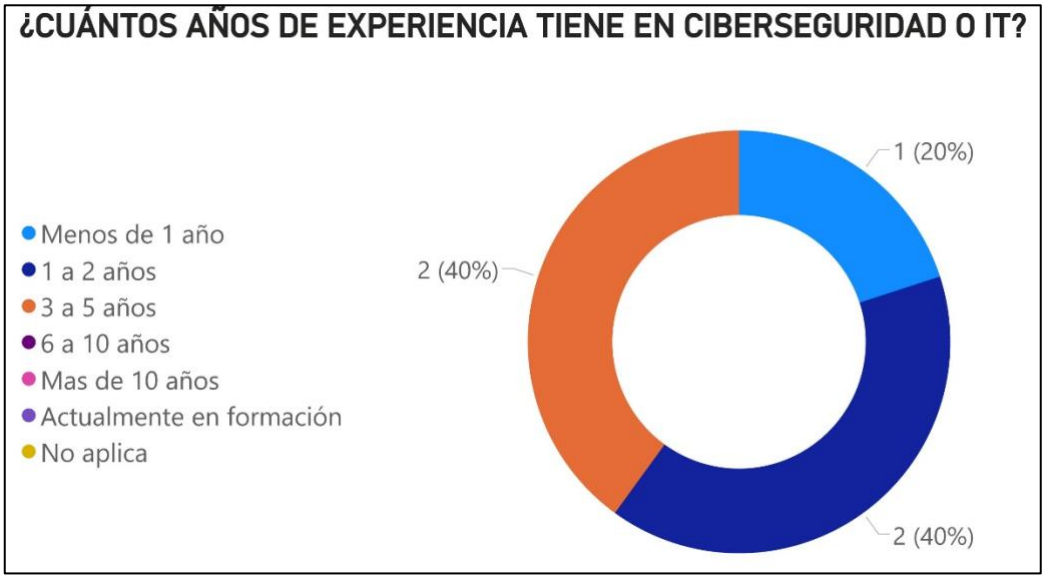
Nota: Elaboración Propia.

Análisis:

Se analizó la distribución de los cargos de los encuestados que interactúan con el ERP empresarial. En la figura 48 se muestra la diversidad de cargos entre los encuestados. Se refleja una perspectiva amplia sobre la ciberseguridad en los ERP empresariales. En este caso, los participantes son mayoritariamente desarrolladores y un jefe de sistemas de información, lo cual indica un enfoque técnico desde la gestión y desarrollo de los sistemas. La presencia mayoritaria de desarrolladores (4 de 5) sugiere que la visión se centra principalmente en la operación y desarrollo del ERP, mientras que la participación del jefe de sistemas añade una visión más estratégica y de gestión. Este equilibrio es importante porque la ciberseguridad requiere tanto la implementación técnica como la planificación y

gobernanza. Sin embargo, el predominio de roles técnicos puede implicar que aspectos como políticas corporativas y estrategia global de seguridad podrían no estar tan desarrollados o percibidos desde una dirección superior. Esta distribución es representativa de muchas empresas pequeñas y medianas en el ámbito tecnológico, donde los equipos son reducidos y los roles se solapan. La información de la anterior subraya la necesidad de que las estrategias de ciberseguridad incluyan más la voz de la alta dirección para fortalecer la gobernanza y asegurar recursos adecuados.

Figura 49: Años de experiencia en ciberseguridad/IT de los participantes.



Nota: Elaboración Propia.

Análisis:

En esta recolección de datos analizó el nivel de experiencia en ciberseguridad e IT de los participantes involucrados en la gestión del ERP empresarial. La Figura 49 muestra los años de experiencia en ciberseguridad e IT oscilan principalmente entre 1 y 5 años, con un participante con menos de un año. Esto revela un nivel moderado de experiencia en el área,

adecuado para empresas en crecimiento o startups tecnológicas. La experiencia relativamente corta puede explicar ciertas limitaciones en la implementación formal de normas, gestión de riesgos y planes de continuidad, detectadas en otras respuestas. El análisis de esta figura indica que el conocimiento sobre mejores prácticas de seguridad puede estar en fase inicial o intermedia en estas empresas, lo que hace imperativo el desarrollo de capacitación continua y asesoría especializada. La presencia de profesionales con experiencia de 3 a 5 años es un aspecto positivo, ya que aporta conocimiento y cierta madurez técnica al equipo. Sin embargo, la ausencia de expertos con más de 5 años señala una posible brecha en la gestión avanzada de la ciberseguridad. Esto puede impactar directamente en la capacidad para anticipar amenazas complejas o implementar marcos normativos robustos.

Figura 50: Descripción general y tamaño de la empresa encuestada.

- Empresa de desarrollo de software con más de 20 empleados.
- Empresa de monitoreo GPS y desarrollo de soluciones tecnológicas, y seria de tamaño pequeño, en donde el servicio principal es el monitoreo GPS, y desarrollo de soluciones tecnológicas
- Somos una empresa conformada por 9 personas, enfocada en la gestión de inventario, control de cuentas y administración de procesos internos. Buscamos optimizar y mantener un manejo eficiente de los recursos y actividades de la empresa.
- TiviTrace es una empresa de tecnología enfocada en la automatización y optimización de procesos empresariales. Su principal objetivo es ayudar a sus clientes a simplificar tareas clave como la gestión de inventarios, ventas y otros flujos operativos, mediante soluciones digitales eficientes y personalizadas.
- Empresa de Servicios GPS , productos de tecnología

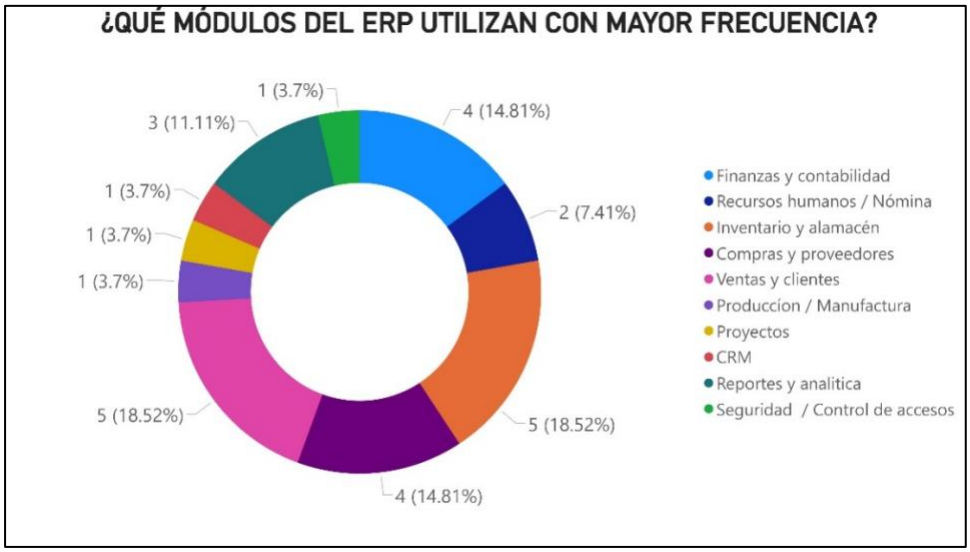
Nota: Elaboración Propia.

Análisis:

La empresa encuestada TiviTrace es principalmente pequeña, con poco más de 20 empleados y orientadas a servicios tecnológicos como monitoreo GPS, desarrollo de software y gestión de inventarios. Esta caracterización indica que la empresa está en etapas tempranas o intermedias de digitalización y adopción tecnológica, lo que puede condicionar los recursos disponibles para ciberseguridad. La mayoría provee soluciones tecnológicas propias o ERP desarrollados internamente, lo que puede ser una ventaja para adaptar la seguridad a las necesidades específicas, pero también un riesgo si no se cuenta con personal experto o estándares sólidos. La variedad de servicios también implica diferentes retos de seguridad según los procesos críticos, como finanzas, recursos humanos y ventas.

El tamaño pequeño limita la capacidad de crear equipos dedicados exclusivos de ciberseguridad, lo que podría llevar a que las funciones se dividan entre pocos empleados, afectando la profundidad en el control y monitoreo. La Figura 50 evidencia esta caracterización organizativa y tecnológica**,** destacando que la ciberseguridad en pymes requiere estrategias adaptadas, capacitación y apoyo externo para cubrir brechas.

Figura 51: Módulos del ERP con mayor uso en las empresas.



Nota: Elaboración Propia.

Análisis:

La figura 51 revela que los módulos más utilizados son finanzas y contabilidad, inventario y almacén, compras y proveedores, ventas y clientes, y reportes y analítica. También se mencionaron módulos adicionales como recursos humanos y nómina, producción, proyectos, CRM y seguridad. Esta información es clave para la categorización de activos y la priorización de acciones de seguridad, ya que los módulos más utilizados concentran procesos críticos y datos sensibles. Por tanto, representan un mayor riesgo en caso de incidentes de ciberseguridad. Una afectación en módulos como finanzas o inventario puede interrumpir operaciones esenciales, comprometer información confidencial o generar pérdidas económicas. Desde el enfoque de ITIL v4, conocer cuáles son los módulos prioritarios permite diseñar planes de recuperación específicos y asignar recursos de respuesta donde más se necesitan. La gestión de incidentes debe tener en cuenta la criticidad

de estos módulos, implementando medidas de protección más rigurosas y simulacros de recuperación enfocados en las áreas de mayor impacto.

Figura 52: Estructura y roles del equipo de tecnología y ciberseguridad.

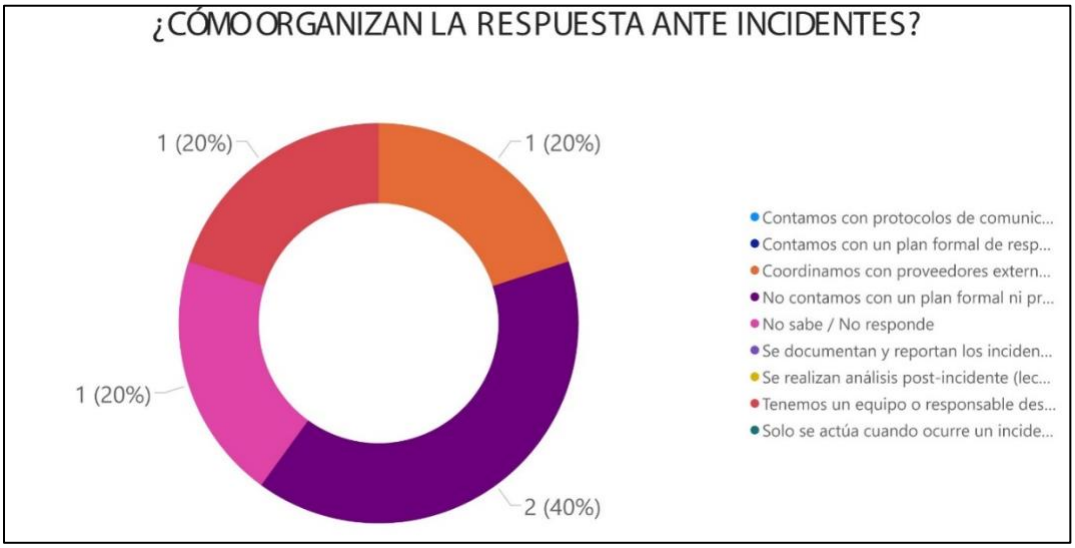
- Departamento de desarrollo y seguridad y departamento de QA.
- Se cuenta con un encargado de TI y tres desarrolladores y un QA permanente y otro temporal.
- El equipo de tecnología y ciberseguridad está conformado por dos personas, quienes comparten responsabilidades en soporte técnico, mantenimiento de infraestructura, administración de sistemas y tareas esenciales de ciberseguridad.
- Equipo de Desarrollo de Software: responsable del diseño, desarrollo y mantenimiento de nuestras aplicaciones y sistemas internos.
- Gerente, Analista, Oficiales de seguridad.

Nota: Elaboración Propia.

Análisis:

La figura 52 muestra que los equipos encuestados dentro de la organización están conformados por pocos miembros con funciones multifuncionales. Los roles de desarrollo, soporte, mantenimiento, calidad y ciberseguridad son asumidos por un grupo reducido de personas, sin contar con un equipo exclusivo para seguridad informática. Esta situación es común en estructuras pequeñas, donde la carga operativa se distribuye entre perfiles técnicos generalistas. Solo un participante indicó la existencia de un gerente y oficiales dedicados a la seguridad, lo que sugiere una estructura más formal y alineada con prácticas avanzadas de gobernanza en ciberseguridad. Desde la perspectiva de ITIL v4, esta limitación puede afectar la eficacia en la respuesta y recuperación ante incidentes, ya que la ausencia de roles especializados y definidos compromete la capacidad de actuar con rapidez, documentar adecuadamente los procesos y sostener una mejora continua en los sistemas ERP.

Figura 53: Organización de la respuesta ante incidentes de ciberseguridad en ERP.



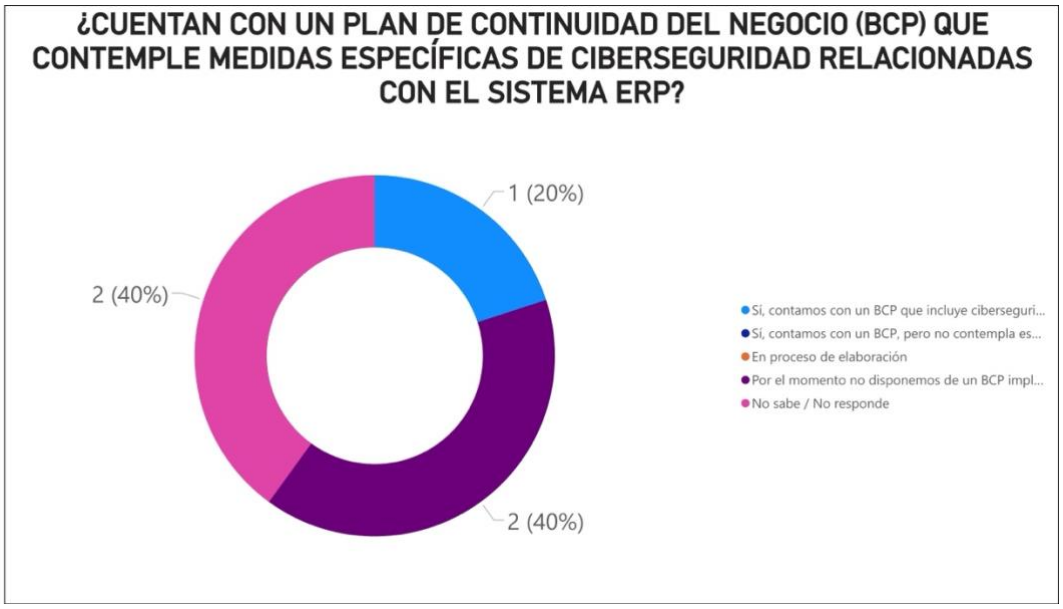
Nota: Elaboración Propia.

Análisis:

Según la Figura 53, la mayoría de los encuestados indicó que no existe un plan formal ni procedimientos definidos para la respuesta ante incidentes dentro de la organización. Solo una persona señaló la existencia de un plan estructurado, y otra mencionó contar con un responsable asignado para estos eventos. Esta falta de preparación formal refleja una debilidad significativa en la capacidad de la empresa para enfrentar incidentes de seguridad, lo que compromete tanto la continuidad operativa como la recuperación efectiva del sistema ERP. La ausencia de políticas claras y roles bien definidos dificulta la coordinación y la respuesta oportuna ante incidentes, incrementando el riesgo de daños mayores y prolongando el tiempo de inactividad. Según las mejores prácticas establecidas en ISO/IEC 27032 e ITIL V4, contar con un plan de respuesta a incidentes formalizado y con responsabilidades asignadas es fundamental para minimizar el impacto de las amenazas cibernéticas y asegurar una recuperación ágil. La tendencia evidenciada indica la necesidad urgente de desarrollar e

implementar políticas, procedimientos y estructuras organizativas que fortalezcan la gestión de incidentes en el entorno ERP.

Figura 54: Disponibilidad de Plan de Continuidad del Negocio (BCP) con enfoque en ciberseguridad para ERP.



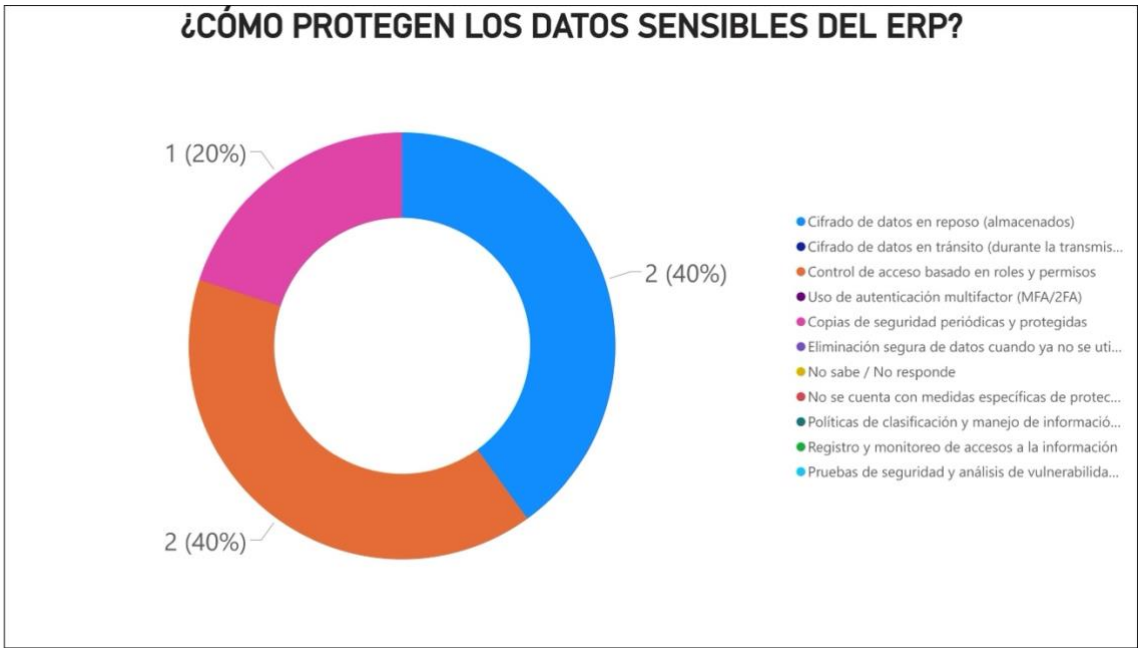
Nota: Elaboración Propia.

Análisis:

Según la Figura 54, la mayoría de los participantes indicó que no existe un Plan de Continuidad del Negocio (BCP) implementado o desconocen su existencia, mientras que solo una persona afirmó que la organización cuenta con un BCP con medidas específicas de ciberseguridad para el ERP. Este resultado evidencia una brecha significativa en la preparación ante posibles interrupciones operativas, lo cual puede afectar gravemente la capacidad de recuperación del sistema y poner en riesgo la continuidad del negocio. La ausencia o desconocimiento del BCP refleja la falta de una estrategia formal para anticipar, responder y recuperarse de incidentes cibernéticos y fallas críticas. Según los lineamientos

de ITIL V4 y las recomendaciones de la ISO/IEC 27032, contar con un plan de continuidad robusto que incluya medidas específicas para proteger sistemas críticos como el ERP es fundamental para garantizar la resiliencia organizacional. La tendencia observada resalta la urgente necesidad de diseñar, implementar y actualizar regularmente planes de continuidad del negocio que integren la gestión de riesgos cibernéticos para mitigar impactos adversos y asegurar la operatividad sostenida.

Figura 55: Medidas para la protección de datos sensibles en ERP.



Nota: Elaboración Propia.

Análisis:

En la Figura 55, la mayoría de los encuestados indican que aplican controles de acceso basados en roles y permisos, y cifrado de datos en reposo, mientras que algunos no proporcionan respuesta clara. Estas medidas reflejan un enfoque básico pero esencial para la protección de la confidencialidad e integridad de la información crítica en los ERP. El control

de acceso por roles asegura que solo usuarios autorizados puedan acceder a datos específicos, limitando riesgos de accesos no autorizados. Por su parte, el cifrado de datos en reposo protege la información almacenada contra accesos indebidos en caso de brechas o ataques físicos. Sin embargo, la falta de respuesta o desconocimiento en algunos casos señala posibles vacíos en la implementación o concientización sobre medidas de protección de datos sensibles. Esto puede representar un riesgo significativo para la seguridad y continuidad operativa, considerando el valor crítico que tienen estos datos en el contexto empresarial.

Figura 56: Procedimientos para la gestión de cambios en ERP empresarial.

Nota: Elaboración Propia.

Análisis:

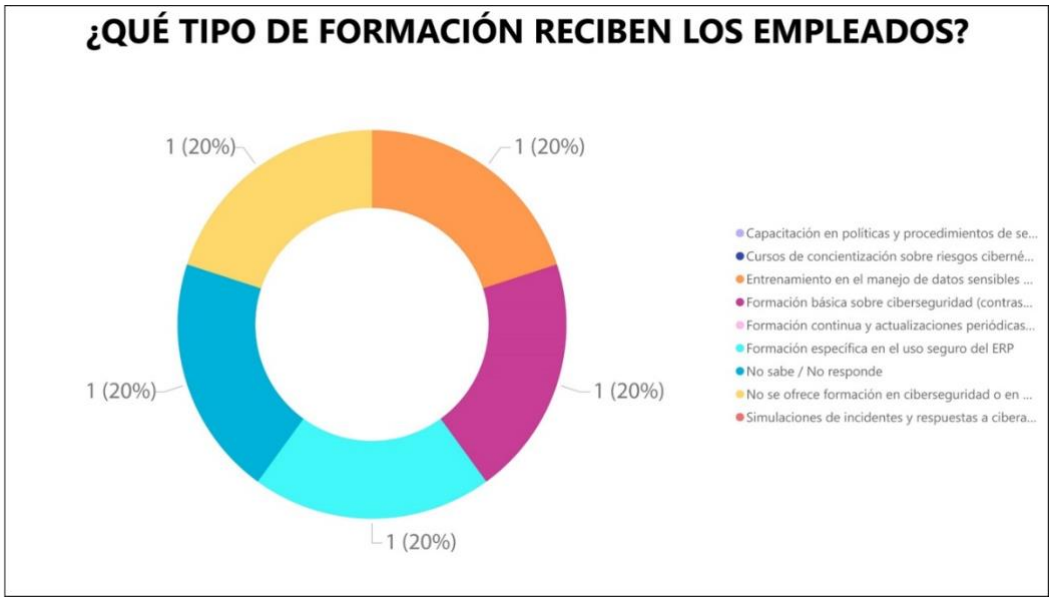
En la Figura 56 se evidencia que ninguno de los encuestados destacó la existencia de procedimientos formales para la gestión de cambios en el ERP empresarial. Esta ausencia generalizada representa una debilidad crítica en la administración del sistema, ya que los cambios no controlados pueden generar vulnerabilidades, afectar la estabilidad operativa y comprometer la disponibilidad del servicio. Aunque algunas organizaciones mencionan prácticas aisladas como respaldos de servidores o bases de datos, estas acciones son reactivas y no reemplazan la necesidad de un proceso estructurado y formalizado. Según ITIL V4, la gestión de cambios es fundamental para minimizar riesgos asociados a modificaciones en sistemas críticos, garantizando que cualquier ajuste se realice de manera controlada,

documentada y aprobada. La falta de un marco claro para gestionar cambios pone en riesgo la continuidad del negocio y limita la capacidad de respuesta eficiente ante incidentes derivados de modificaciones no planificadas. Por tanto, es urgente implementar políticas claras, establecer comités de gestión de cambios y adoptar prácticas alineadas con estándares internacionales para fortalecer la administración del ERP y asegurar la resiliencia organizacional.

4.1.11 EVALUAR EL IMPACTO DEL PLAN DE CIBERSEGURIDAD MEDIANTE INDICADORES CLAVE DE DESEMPEÑO (KPI) PARA MEDIR SU EFECTIVIDAD EN LA REDUCCIÓN DE RIESGOS EN ERP EMPRESARIALES.

Para cumplir con el objetivo 5, que consiste en evaluar el impacto del plan de ciberseguridad mediante indicadores clave de desempeño (KPI) en la reducción de riesgos en ERP empresariales, se recolectaron datos relevantes a través de encuestas. Estos datos incluyen el tipo de formación en ciberseguridad recibida por los empleados, la falta de comentarios adicionales sobre mejoras y la percepción sobre el futuro de la ciberseguridad en ERP. El análisis de esta información permite identificar las fortalezas y áreas de oportunidad para mejorar la capacitación, la comunicación y la adaptación a nuevas amenazas, asegurando así una gestión continua y efectiva de la seguridad en los ERP.

Figura 57: Tipos de formación en ciberseguridad y uso del ERP recibida por empleados.



Nota: Elaboración Propia.

Análisis:

En estos datos revela el nivel de capacitación que reciben los empleados en temas de ciberseguridad y manejo del ERP. En la Figura 57, se observa una diversidad considerable: algunos empleados no reciben formación, otros no responden, y una parte recibe desde formación básica en seguridad, hasta entrenamiento especializado en manejo de datos sensibles y uso seguro del ERP. Esta variedad evidencia una brecha en la estandarización y profundidad de la formación impartida, lo cual impacta directamente en la capacidad del personal para reconocer riesgos, seguir buenas prácticas y responder adecuadamente ante incidentes. La falta de formación puede incrementar la vulnerabilidad del sistema ERP, especialmente ante amenazas como phishing o errores humanos. Por otro lado, la existencia de formación específica en uso seguro del ERP y protección de datos sensibles es un indicador positivo que debe potenciarse, pues fortalece la cultura de seguridad y contribuye

a la reducción de riesgos. En conclusión, para mejorar la gestión de riesgos y la efectividad del plan de ciberseguridad, es esencial implementar programas de formación sistemáticos y actualizados, que cubran tanto aspectos técnicos como conductuales, asegurando que todo el personal tenga las competencias necesarias para proteger el ERP y la información empresarial crítica.

Figura 58: Aspectos adicionales relevantes en ciberseguridad ERP.

No No No Ninguno

Nota: Elaboración Propia.

Análisis:

La Figura 58 muestra que ninguno de los encuestados brindó comentarios adicionales relevantes al finalizar el cuestionario. Esta falta de participación puede interpretarse desde diversas perspectivas. Por un lado, podría reflejar que los temas abordados durante la encuesta fueron lo suficientemente amplios y abarcadores como para responder a las principales inquietudes de los usuarios, sin dejar espacio para nuevas aportaciones. Sin embargo, también podría evidenciar una falta de iniciativa, compromiso o incluso desconocimiento por parte del personal en torno a la importancia de la ciberseguridad y la necesidad de mantener un enfoque proactivo frente a los riesgos. Esta situación es particularmente preocupante si se considera que los aportes voluntarios pueden revelar aspectos no contemplados en la encuesta estructurada, brindando insumos valiosos para el fortalecimiento del sistema de seguridad.

La ausencia de comentarios también puede interpretarse como un síntoma de debilidad en la cultura organizacional, especialmente en lo que respecta a la participación del personal en procesos de mejora continua. En un entorno de riesgo constante como lo es la gestión de un ERP empresarial, fomentar una cultura de comunicación abierta y colaboración es fundamental para detectar vulnerabilidades emergentes, recopilar percepciones del usuario final y generar soluciones más alineadas con la operación diaria del sistema. Cuando no existe este tipo de interacción, se desaprovechan oportunidades clave para enriquecer las estrategias de protección, ya que quienes están en contacto directo con el sistema podrían identificar aspectos que no siempre son evidentes desde el área técnica o administrativa.

Por tanto, más allá de los resultados cuantitativos obtenidos, esta falta de comentarios destaca una necesidad urgente que es fortalecer los canales de retroalimentación y construir un ambiente organizacional que incentive la expresión de ideas, propuestas y preocupaciones en torno a la ciberseguridad. Esto implica no solo abrir espacios formales para la participación, como buzones de sugerencias o reuniones periódicas, sino también asegurar que dichas contribuciones sean valoradas, tomadas en cuenta e integradas en las decisiones estratégicas. Fomentar este tipo de dinámica no solo mejora el diseño del plan de ciberseguridad, sino que también incrementa el sentido de pertenencia del personal y su compromiso con la protección del sistema ERP.

Figura 59: Percepción sobre el futuro de la ciberseguridad en ERP.

Nota: Elaboración Propia.

Análisis:

Los resultados obtenidos reflejan un consenso general entre los participantes respecto a la importancia de establecer planes bien definidos y promover mejoras continuas tanto en la gestión de usuarios como en la seguridad general del sistema ERP. Esta visión compartida confirma que existe una conciencia creciente sobre la necesidad de fortalecer los controles internos, implementar buenas prácticas y mantener una vigilancia constante para proteger los activos de información críticos dentro de la organización.

Además, se percibe una expectativa clara de evolución: se espera que la ciberseguridad deje de ser un proceso reactivo y fragmentado para convertirse en una disciplina mucho más dinámica, colaborativa y orientada a la prevención temprana de amenazas. Este enfoque implica no solo mejorar las herramientas tecnológicas existentes, sino también promover la integración entre departamentos, capacitar al personal de manera

continua y establecer una gobernanza sólida que permita tomar decisiones oportunas y basadas en riesgo. No obstante, esta visión de progreso se enfrenta a un panorama cada vez más desafiante. Los participantes reconocen que la inclusión de tecnologías avanzadas, en especial aquellas basadas en inteligencia artificial, está transformando tanto las capacidades defensivas como ofensivas en el ámbito digital. Si bien estas innovaciones pueden fortalecer la ciberseguridad mediante automatización, detección de anomalías y análisis predictivo, también están siendo utilizadas por actores maliciosos para desarrollar ataques más complejos, difíciles de identificar y altamente dirigidos. Esta dualidad entre oportunidad y riesgo obliga a las organizaciones a mantener una actitud de mejora constante, evaluando periódicamente sus estrategias, procedimientos y herramientas. No basta con tener un plan de seguridad estático; se requiere un enfoque adaptable, con capacidad de respuesta ágil y alineado a estándares internacionales como ISO/IEC 27032. Solo de esta forma será posible enfrentar con éxito los desafíos que plantea el entorno digital moderno y garantizar la protección sostenida del sistema ERP empresarial.

4.1.12 MATRIZ DE ANÁLISIS DE RESULTADOS

OBJETIVO	CLIENTE	CONSULTOR
1. Identificar y clasificar los riesgos de ciberseguridad en ERP empresariales mediante análisis de vulnerabilidades y auditorías documentales de políticas de seguridad, para determinar amenazas críticas.	En TiviTrace, las auditorías documentales revelaron debilidades en el ERP, como falta de controles sólidos y escaso personal en ciberseguridad. Las principales amenazas fueron phishing, errores humanos y accesos no autorizados.	Se recomienda priorizar auditorías periódicas y fortalecer controles de acceso y capacitación en ciberseguridad. La identificación clara de riesgos permitirá enfocar recursos en mitigaciones específicas y efectivas.
2. Analizar las mejores prácticas de seguridad de la norma ISO/IEC 27032 y su aplicabilidad en la gestión de riesgos en ERP empresariales.	La aplicación de controles ISO/IEC 27032 se muestra limitada por la capacidad técnica y recursos en las pymes. Sin embargo, existe interés en adoptar buenas prácticas para proteger activos críticos.	Se sugiere adaptar los controles ISO/IEC 27032 a la realidad de las pymes, con implementaciones escalables y formación especializada para asegurar cumplimiento y mejora continua en la gestión del riesgo.
3. Definir estrategias de detección y mitigación de Amenazas Persistentes Avanzadas (APT) en ERP empresariales, usando controles ISO/IEC 27032.	Actualmente, las estrategias para APT son insuficientes, con poca detección temprana y respuesta tardía. La falta de monitoreo especializado es una brecha significativa.	Implementar soluciones de monitoreo avanzado y sistemas de alerta temprana, capacitando al personal en identificación de patrones de APT. Es vital integrar estas estrategias en el plan de seguridad con controles alineados a ISO/IEC 27032.
4. Identificar activos según su categoría de riesgo para determinar alternativas de respuesta y recuperación ante incidentes	Las empresas pequeñas con ERP desarrollados internamente tienen activos diversos con diferentes riesgos, pero recursos limitados para equipos	Desarrollar un plan de gestión de incidentes basado en ITIL V4 adaptado a la escala de la empresa, con categorización clara de activos y protocolos para respuesta rápida,

alineados con ITIL V4 para mejorar la continuidad del negocio.	dedicados. Esto afecta la capacidad de respuesta y recuperación.	aprovechando recursos internos y apoyos externos. Capacitar al personal en estas prácticas es clave.
5. Evaluar el impacto del plan de ciberseguridad mediante indicadores clave de desempeño (KPI) para medir su efectividad en la reducción de riesgos en ERP empresariales.	Se identificó diversidad en la formación de empleados, falta de comentarios adicionales y una visión optimista pero desafiante del futuro de la ciberseguridad en ERP.	Es necesario implementar programas sistemáticos y actualizados de formación y fomentar comunicación abierta para compartir riesgos y mejoras. Se deben definir KPIs claros para medir avances y ajustar el plan continuamente frente a amenazas emergentes.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

A partir del análisis de los datos recolectados mediante encuestas, entrevistas, FODA, Ishikawa y listas de verificación en la empresa TiviTrace, se identificaron diversos retos en la gestión de riesgos de ciberseguridad asociados al uso del sistema ERP. Los resultados evidencian vulnerabilidades tanto técnicas como humanas, lo que resalta la urgencia de fortalecer las capacidades internas de la organización y adoptar de manera más estructurada marcos de referencia como ISO/IEC 27032 e ITIL v4.

Los datos cuantitativos obtenidos en las encuestas mostraron que un alto porcentaje del personal reconoce deficiencias en la capacitación y en los controles técnicos implementados, mientras que la información cualitativa de las entrevistas permitió comprender en profundidad las causas y percepciones relacionadas con estas debilidades, además de identificar áreas prioritarias para la mejora. La integración de estas fuentes enriqueció el diagnóstico y fundamentó las propuestas elaboradas.

1. **IDENTIFICACION Y CLASIFICACIÓN DE LOS RIESGOS**

   En cumplimiento del primer objetivo específico, se logró identificar y clasificar los riesgos de ciberseguridad presentes en el ERP, destacando como amenazas prioritarias los ataques de ingeniería social, en particular el phishing, así como los accesos no autorizados provocados por controles débiles y errores humanos. Estas amenazas se ven intensificadas por la escasa implementación de controles técnicos y la ausencia de auditorías periódicas, lo que limita la capacidad de prevención y respuesta. Por tanto, se concluye que es indispensable establecer una priorización de riesgos basada en la

probabilidad e impacto, que permita diseñar estrategias de mitigación adaptadas al contexto de la organización.

1.1. PRINCIPALES AMENAZAS IDENTIFICADAS

Entre las amenazas más relevantes y recurrentes destacan los ataques de ingeniería social, en particular el phishing, que se constituyen como la principal vía de compromiso debido a la interacción directa y frecuente del personal con el sistema ERP. Estas amenazas apuntan a vulnerabilidades en la capa humana, donde la falta de concientización y capacitación facilita la explotación de credenciales y la introducción de malware. Asimismo, se identificaron accesos no autorizados derivados de controles débiles o inadecuados, como contraseñas simples, ausencia de autenticación multifactor, mala gestión de permisos y la carencia de una política clara de control de acceso basada en roles.

1.2. FACTORES AGRAVANTES Y DEBILIDADES EN LA GESTIÓN

El análisis evidencia que la organización TiviTrace presenta una implementación limitada de controles técnicos robustos, tales como cifrado de datos, monitoreo continuo, mecanismos de detección de intrusiones y actualizaciones sistemáticas de software. Esta insuficiencia técnica se agrava por la falta de auditorías periódicas y evaluaciones de seguridad formales que permitan detectar y corregir vulnerabilidades a tiempo. De igual forma, la ausencia de programas de capacitación constante al personal que utiliza el ERP incrementa la exposición a ataques que se

aprovechan del factor humano, configurando un entorno vulnerable ante amenazas internas y externas.

1.3. IMPORTANCIA DE LA PRIORIZACIÓN Y CLASIFICACIÓN DE RIESGOS

Dada la diversidad y complejidad de las amenazas identificadas, así como los recursos limitados con los que cuenta TiviTrace, resulta crítico implementar un sistema de priorización de riesgos que permita enfocar esfuerzos y recursos en aquellos incidentes con mayor probabilidad de ocurrencia y mayor impacto potencial. Esta priorización debe basarse en metodologías objetivas que integren aspectos técnicos, operativos y de negocio, utilizando matrices de riesgo que faciliten la visualización clara y transparente del estado de exposición. Además, esta clasificación es fundamental para desarrollar planes de mitigación efectivos, asignar responsabilidades específicas y mejorar la gobernanza en materia de ciberseguridad.

1.4. ENFOQUE INTEGRAL Y ALINEACIÓN CON NORMAS INTERNACIONALES

Se concluye que para mejorar la postura de seguridad del ERP es imprescindible adoptar un enfoque integral que contemple no solo la implementación de controles tecnológicos sino también el fortalecimiento del factor humano y la formalización de procesos. La norma ISO/IEC 27032 ofrece un marco valioso para esta gestión, destacando la importancia de medidas como la autenticación multifactor, cifrado, segmentación de redes y gestión continua de vulnerabilidades. Paralelamente, la integración con el marco ITIL V4 permite articular la gestión de riesgos con la

continuidad del negocio, garantizando una respuesta ágil y coordinada ante incidentes y reduciendo los tiempos de recuperación operativa.

2. APLICACIÓN DE LA NORMA ISO/IEC 27032

Respecto al segundo objetivo, orientado a analizar las mejores prácticas de seguridad basadas en ISO/IEC 27032, se constató que su aplicación actual en TiviTrace es incipiente. Aunque existe conciencia sobre la necesidad de mejorar la postura de ciberseguridad, su implementación se ve obstaculizada por factores como la falta de personal especializado, la sobrecarga operativa del equipo técnico y una cultura organizacional aún en desarrollo. Por lo tanto, se recomienda una adopción progresiva y escalable de esta norma, ajustando los controles a la realidad de los recursos disponibles, sin desatender la protección integral de los activos digitales.

2.1. ESTADO ACTUAL DE LA ADOPCIÓN DE ISO/IEC 27032

Se evidenció que en TiviTrace no se ha adoptado formalmente la norma ISO/IEC 27032, encontrándose aún en una fase previa a la implementación de sus controles técnicos, organizativos y procedimentales. Aunque el personal involucrado reconoce la importancia de esta norma para mejorar la ciberseguridad, no se han iniciado acciones concretas para su aplicación, lo que representa una brecha significativa en la gestión de riesgos. Entre las principales limitaciones se identifican la ausencia de personal con formación especializada en seguridad informática, lo que

dificulta el diseño, implementación y mantenimiento de controles adecuados; además, la alta carga de trabajo del equipo técnico reduce el tiempo disponible para actividades preventivas y de mejora continua, retrasando aún más la adopción de mejores prácticas basadas en la norma.

2.2. FACTORES ORGANIZACIONALES Y CULTURALES

Además de las limitaciones técnicas, se identificó que la cultura organizacional en materia de seguridad informática aún está en proceso de consolidación. La sensibilización insuficiente y la falta de políticas internas claras contribuyen a que las mejores prácticas recomendadas por ISO/IEC 27032 no se arraiguen plenamente en la operación diaria. Esta situación genera riesgos adicionales, dado que la efectividad de cualquier norma o control depende en gran medida del compromiso y la participación activa de todos los niveles de la organización.

3. ESTRATEGIAS Y HERRAMIENTAS ACTUALES

En atención al tercer objetivo, enfocado en definir estrategias para la detección y mitigación de Amenazas Persistentes Avanzadas (APT), se identificó que actualmente no existen mecanismos específicos ni estructurados para enfrentar este tipo de amenazas dentro del ERP. La falta de herramientas de monitoreo continuo, alertas tempranas y análisis de comportamiento anómalo deja a la organización expuesta frente a posibles ataques sofisticados. Esto subraya la necesidad de fortalecer tanto la infraestructura

tecnológica como las competencias del personal, promoviendo la detección proactiva de amenazas.

3.1. FALTA DE MECANISMOS ESPECÍFICOS Y ESTRUCTURADOS

Se constató que la empresa no ha implementado mecanismos específicos, estructurados y formalizados para enfrentar APT. La ausencia de políticas, protocolos y procesos orientados a la gestión de amenazas avanzadas genera una postura reactiva frente a incidentes, en lugar de una postura proactiva que permita anticipar, detectar y neutralizar ataques en etapas tempranas. Esta situación aumenta la vulnerabilidad del ERP y expone a la empresa a riesgos elevados de compromiso prolongado, robo de información sensible y daños operativos severos.

3.2. CARENCIA DE HERRAMIENTAS TECNOLÓGICAS AVANZADAS PARA LA DETECCIÓN

Actualmente, no se dispone de tecnologías clave para la monitorización continua y la correlación de eventos de seguridad. La falta de sistemas de gestión de eventos e información de seguridad (SIEM), así como la ausencia de mecanismos de detección y prevención de intrusiones (IDS/IPS), limita la visibilidad que el equipo de seguridad tiene sobre el comportamiento de la red y las actividades dentro del ERP. Sin estas herramientas, la detección temprana de patrones anómalos o actividades maliciosas resulta prácticamente inexistente, lo que favorece la permanencia y el avance silencioso de las APT.

3.3. IMPACTO DE LA INFRAESTRUCTURA TECNOLÓGICA INSUFICIENTE

La carencia de una infraestructura tecnológica robusta para la seguridad implica que la organización no cuenta con la capacidad operativa para implementar controles avanzados recomendados por estándares internacionales como ISO/IEC 27032. Esto afecta directamente la capacidad para mantener la confidencialidad, integridad y disponibilidad de los activos digitales. Además, limita la eficacia de la respuesta ante incidentes, prolongando el tiempo de exposición y aumentando el impacto potencial de los ataques.

3.4. DÉFICIT EN LA FORMACIÓN Y COMPETENCIAS DEL PERSONAL

El factor humano también representa un área crítica de mejora. La falta de formación especializada en la detección y respuesta a APT reduce la capacidad del equipo de TI para identificar señales de alerta y actuar con prontitud. La ausencia de programas de capacitación continua y entrenamiento en técnicas avanzadas de análisis forense digital, inteligencia de amenazas y gestión de incidentes contribuye a mantener un nivel bajo de preparación ante amenazas complejas y persistentes.

3.5. REPERCUSIONES PARA LA GESTIÓN DE RIESGOS Y CONTINUIDAD DEL NEGOCIO

La falta de estrategias y herramientas adecuadas no solo aumenta la probabilidad de ataques exitosos, sino que también complica la gestión integral de riesgos y la continuidad operativa del ERP. Ante la creciente sofisticación de las amenazas cibernéticas, es imperativo adoptar un enfoque holístico que integre tecnología, procesos

y personal capacitado para fortalecer la defensa perimetral y la seguridad interna. Sin esta integración, la empresa está expuesta a pérdidas financieras, reputacionales y legales, así como a interrupciones operativas que pueden afectar su competitividad y confianza frente a clientes y socios.

4. IDENTIFICACION Y CATEGORIZACIÓN DE LOS RIESGOS

Con respecto al cuarto objetivo, se abordó la identificación y categorización de activos críticos, lo que permitió evaluar el nivel de exposición al riesgo dentro del ecosistema del ERP. Esta clasificación facilitó la formulación de propuestas para la respuesta y recuperación ante incidentes, alineadas con los principios de ITIL v4. No obstante, se evidenció que la falta de equipos dedicados exclusivamente a estas funciones limita la capacidad operativa de respuesta. Por ello, se plantea la necesidad de planes de recuperación que sean prácticos, flexibles y adaptados a la estructura existente, contemplando incluso opciones de tercerización estratégica para asegurar la continuidad del negocio.

4.1. EVALUACIÓN DEL NIVEL DE EXPOSICIÓN AL RIESGO

La categorización permitió identificar activos esenciales que soportan funciones clave del ERP, tales como bases de datos, módulos de facturación, y sistemas de autenticación. Reconocer estos activos como prioritarios es indispensable para focalizar las medidas de seguridad y garantizar que los recursos técnicos y humanos se asignen de manera eficiente y estratégica. Según los principios de ITIL v4, la gestión de activos y la

clasificación por niveles de criticidad contribuyen a optimizar la gestión de incidentes y la continuidad operativa.

4.2. FORMULACIÓN DE PROPUESTAS PARA RESPUESTA Y RECUPERACIÓN

Basándose en esta categorización, se desarrollaron propuestas específicas orientadas a la respuesta rápida y recuperación efectiva ante incidentes de seguridad. Estas estrategias se alinean con las mejores prácticas de ITIL v4, que promueven la implementación de procesos estructurados para la gestión de incidentes y la continuidad del negocio. La incorporación de planes de contingencia y recuperación que consideren la prioridad de cada activo garantiza una restauración más eficiente y minimiza el impacto operativo.

4.3. LIMITACIONES OPERATIVAS IDENTIFICADAS

Sin embargo, durante el análisis se identificó una limitación significativa: la ausencia de equipos o roles dedicados exclusivamente a la gestión de la respuesta y recuperación ante incidentes dentro de TiviTrace. Esta falta de especialización puede ralentizar la toma de decisiones y la ejecución de acciones correctivas, aumentando el riesgo de impactos prolongados sobre el sistema ERP y los procesos empresariales asociados.

4.4. NECESIDAD DE PLANES PRÁCTICOS Y FLEXIBLES

Dado el contexto organizacional y los recursos disponibles, se destaca la importancia de diseñar planes de recuperación que sean prácticos y adaptados a la estructura actual de la empresa. Estos planes deben ser flexibles para ajustarse a cambios

operativos y tecnológicos, y contemplar la posibilidad de recurrir a la tercerización estratégica de servicios especializados. La externalización puede aportar experiencia técnica y recursos adicionales, fortaleciendo la capacidad de respuesta y asegurando la continuidad del negocio frente a incidentes críticos.

4.5. IMPACTO EN LA CONTINUIDAD DEL NEGOCIO

En conjunto, la identificación y categorización adecuada de activos críticos, combinada con la implementación de planes efectivos de respuesta y recuperación, son pilares esenciales para reducir la vulnerabilidad del ERP y preservar la operatividad empresarial. El cumplimiento de estos procesos es un componente clave dentro del marco de ITIL v4 para garantizar la resiliencia y sostenibilidad de los servicios de tecnología, aspectos fundamentales para mantener la competitividad y confianza en el entorno digital actual.

5. EVALUACIÓN DEL IMPACTO DE UN PLAN DE CIBERSEGURIDAD MEDIANTE KPIS

Finalmente, en lo relativo al quinto objetivo, se evaluó el impacto del plan de ciberseguridad mediante indicadores clave de desempeño (KPIs). Los resultados reflejan deficiencias en los procesos de capacitación y en la consolidación de una cultura organizacional orientada a la seguridad. Las actividades formativas son limitadas y no abordan todas las dimensiones necesarias para afrontar riesgos emergentes, mientras que la comunicación interna sobre protocolos de actuación aún requiere reforzarse. A pesar de ello, se identificó una actitud favorable hacia la mejora

continua, manifestada en el interés por adoptar tecnologías emergentes y prácticas más sólidas que fortalezcan la postura de seguridad de la organización ante futuras amenazas.

5.1. LIMITACIONES EN LA CAPACITACIÓN Y CULTURA ORGANIZACIONAL

Se evidenció que uno de los factores más determinantes en los bajos niveles de cumplimiento de los KPIs es la limitada oferta de actividades formativas**,** tanto en cantidad como en alcance. Las capacitaciones actuales no abarcan los diversos vectores de riesgo contemporáneos, como el phishing, la ingeniería social o las amenazas persistentes avanzadas, lo cual deja vacíos significativos en la preparación del personal frente a incidentes reales. A esto se suma la carencia de mecanismos estructurados para evaluar la retención del conocimiento adquirido y su aplicación práctica en el entorno laboral.

En este contexto, la cultura organizacional orientada a la seguridad aún no se encuentra plenamente consolidada. La seguridad tiende a percibirse como una responsabilidad exclusiva del área técnica, en lugar de ser una práctica transversal a todos los niveles jerárquicos y operativos. Esta visión limitada restringe la capacidad de respuesta proactiva ante incidentes y debilita la resiliencia organizacional.

5.2. FALENCIAS EN COMUNICACIÓN Y GESTIÓN DEL CONOCIMIENTO

Los resultados también reflejaron debilidades en los procesos de comunicación interna sobre protocolos de actuación y flujos de respuesta ante eventos de seguridad. En múltiples instancias, los colaboradores no están plenamente familiarizados con los

procedimientos a seguir en caso de un incidente, lo que podría traducirse en tiempos de reacción lentos y decisiones ineficaces ante una contingencia. Asimismo, se identificó que la documentación de políticas, procedimientos y roles en ciberseguridad es insuficiente o no se actualiza con la frecuencia requerida, generando inconsistencias entre la teoría y la práctica organizacional. Esto impacta directamente en la capacidad de auditoría y seguimiento de los KPIs definidos.

5.2 RECOMENDACIONES

Con base en las conclusiones obtenidas y con el fin de fortalecer la gestión de riesgos y la seguridad en ERP empresariales, se proponen las siguientes recomendaciones:

1. Implementar programas de formación continuos y sistemáticos que incluyan desde conceptos básicos de ciberseguridad hasta entrenamientos especializados para el manejo seguro del ERP y protección de datos sensibles, asegurando que todos los colaboradores adquieran competencias para minimizar errores y fortalecer la defensa ante amenazas.

Ejemplo: Establecer un calendario semestral de capacitaciones internas donde, en el primer trimestre, se aborden temas como contraseñas seguras, detección de correos fraudulentos y prácticas seguras al navegar. En el segundo trimestre, incluir talleres técnicos sobre buenas prácticas al utilizar el ERP, sesiones de simulación de incidentes de seguridad y cursos virtuales especializados por roles (como formación para administradores del sistema o personal de soporte). Complementar con campañas internas de concientización mediante correos electrónicos, afiches y retos interactivos mensuales para reforzar la cultura de ciberseguridad.

2. Adoptar un enfoque escalable y adaptado a la realidad de TiviTrace para la aplicación práctica de la norma ISO/IEC 27032, priorizando controles efectivos y asequibles que se integren sin requerir grandes recursos, facilitando así su implementación y mantenimiento.

Ejemplo: En lugar de implementar la norma completa de una vez, iniciar con un piloto centrado en los procesos más críticos del ERP, como la gestión de usuarios y accesos. Establecer controles básicos como autenticación multifactor, revisión de logs y políticas mínimas de uso aceptable. Utilizar herramientas gratuitas o de código abierto para escaneo de vulnerabilidades y evaluación de cumplimiento. Posteriormente, ampliar progresivamente la cobertura a otros procesos, ajustando las medidas de acuerdo con los recursos disponibles y priorizando los riesgos más relevantes identificados.

3. Desarrollar e implementar sistemas de monitoreo y detección temprana para Amenazas Persistentes Avanzadas (APT), incorporando herramientas tecnológicas y protocolos para la identificación y respuesta rápida, además de capacitar al personal encargado de la seguridad.

Ejemplo: Integrar herramientas como Wazuh o Snort para la monitorización de eventos sospechosos en los servidores que alojan el ERP. Configurar alertas automáticas que notifiquen al personal de TI cuando se detecten comportamientos anómalos como intentos reiterados de acceso fallido, movimientos laterales o escaneo de puertos. Complementar con capacitaciones sobre análisis de logs y respuestas ante señales de compromisos, y realizar ejercicios mensuales de simulación de detección y contención de APTs.

4. Diseñar planes de respuesta y recuperación ante incidentes alineados con ITIL V4, considerando la categorización de activos críticos, la asignación clara de responsabilidades y la colaboración con expertos externos cuando sea necesario, para garantizar la continuidad del negocio ante eventos adversos.

Ejemplo: Crear un documento formal con el paso a paso para actuar ante un incidente de ciberseguridad, como una filtración de datos o un ransomware. Incluir roles asignados a cada miembro del equipo, tiempos estimados de respuesta, responsables de la comunicación interna y externa, y procedimientos técnicos para la contención y recuperación del ERP. Por ejemplo, definir qué hacer si el servidor principal queda comprometido: uso de respaldos automatizados almacenados en la nube, recuperación desde réplica, y notificación a usuarios clave. Realizar simulacros semestrales para validar el plan.

5. Definir y aplicar indicadores clave de desempeño (KPIs) que permitan medir de forma continua la efectividad del plan de ciberseguridad, promoviendo una cultura organizacional de mejora continua basada en retroalimentación y adaptación frente a nuevas amenazas.

Ejemplo: Establecer KPIs como el número de incidentes detectados y resueltos por mes, tiempo promedio de respuesta ante eventos críticos, porcentaje de empleados capacitados en los últimos seis meses, o tasa de cumplimiento de políticas de seguridad. Visualizar estos indicadores en un panel accesible para la dirección y el equipo de seguridad, permitiendo identificar áreas de mejora continua. Por ejemplo, si el KPI de capacitación

muestra un 40% de cobertura, se deberá reforzar la difusión y accesibilidad de los programas formativos.

6. Fomentar una comunicación abierta y la participación activa del personal en temas de ciberseguridad, creando espacios para compartir inquietudes, propuestas y experiencias que fortalezcan el compromiso organizacional con la protección del ERP y la información crítica.

Ejemplo: Crear un canal interno exclusivo en plataformas como Slack o Microsoft Teams donde los colaboradores puedan reportar posibles amenazas (como correos sospechosos) o hacer consultas de seguridad sin temor a represalias. Organizar foros trimestrales de ciberseguridad donde se expongan casos reales, aprendizajes internos y buenas prácticas. Establecer una figura de "embajadores de ciberseguridad" por departamento, responsables de recoger sugerencias y promover comportamientos seguros dentro de sus equipos.

7. Promover la sensibilización y cultura de ciberseguridad desde los niveles más altos de la empresa, involucrando a la dirección en la definición de políticas claras y en la asignación de recursos adecuados para la implementación efectiva del plan.

Ejemplo: Incluir la ciberseguridad como tema permanente en las reuniones estratégicas de la gerencia. Designar a un responsable de seguridad de la información (aunque sea una función compartida) y destinar un presupuesto específico para la implementación del plan. Publicar mensajes de la dirección general en los medios internos subrayando la importancia de la protección de los activos digitales. Establecer compromisos firmes,

como una política que obligue a todos los líderes de área a recibir formación anual sobre gestión de riesgos digitales.

8. Realizar auditorías y evaluaciones periódicas para identificar brechas y ajustar estrategias, asegurando que los controles y planes evolucionen conforme a los cambios tecnológicos y el panorama de amenazas.

Ejemplo: Programar una auditoría semestral en la cual se evalúe la aplicación de políticas de seguridad, la correcta asignación de roles en el ERP, y la existencia de vulnerabilidades técnicas. Utilizar listas de verificación basadas en ISO/IEC 27032 y generar informes con hallazgos y recomendaciones. Incluir en las evaluaciones entrevistas breves al personal sobre su conocimiento de los protocolos y encuestas anónimas sobre la percepción de seguridad. En base a los resultados, actualizar los planes de acción e informar a todos los involucrados sobre los avances.

CAPÍTULO VI. APLICABILIDAD

Según los resultados obtenidos en TiviTrace mediante entrevistas, encuestas y listas de verificación, se identificaron debilidades críticas en la seguridad del sistema ERP, como la falta de autenticación multifactor, escasa capacitación del personal y ausencia de monitoreo activo. En respuesta, se propone un Plan de Ciberseguridad basado en ISO/IEC 27032 e ITIL V4, orientado a reducir riesgos mediante controles técnicos y organizativos.

La propuesta incluye medidas como: implementación de MFA, cifrado de datos, segmentación de red, entrenamientos mensuales, monitoreo con herramientas SIEM, y protocolos de respuesta ante incidentes. Además, se presentan un cronograma, presupuesto y mecanismos de evaluación con KPIs, garantizando un enfoque integral y sostenible de mejora continua en la gestión de ciberseguridad.

6.1. PLAN DE CIBERSEGURIDAD PARA LA GESTIÓN DE RIESGOS EN EL ERP WEB EMPRESARIAL DE TIVITRACE BASADO EN ISO/IEC 27032 E ITIL V4

6.2. JUSTIFICACIÓN DE LA PROPUESTA

El problema central identificado en la empresa **TiviTrace** radica en una gestión deficiente de la ciberseguridad en su sistema ERP web. Entre las debilidades más críticas se encuentra la ausencia de mecanismos de autenticación multifactor (MFA), la falta total de capacitación en ciberseguridad especialmente en amenazas como el phishing, la inexistencia de políticas y procedimientos formalizados para la gestión de incidentes, y la carencia de monitoreo continuo ante riesgos cibernéticos complejos, como las Amenazas Persistentes

Avanzadas (APT). Estas deficiencias no solo aumentan la vulnerabilidad ante accesos no autorizados y pérdida de información sensible, sino que también ponen en riesgo la operatividad y sostenibilidad del negocio, afectando directamente los módulos más críticos del ERP, como Finanzas, Inventario y Recursos Humanos.

El presente plan de ciberseguridad se justifica por las siguientes razones:

- **Evidencia empírica:**

Durante el proceso investigativo, se aplicaron entrevistas y encuestas que revelaron un panorama preocupante: el 100 % del personal encuestado manifestó no haber recibido ningún tipo de formación en ciberseguridad, y se identificaron prácticas inseguras generalizadas. Además, los análisis técnicos mostraron vulnerabilidades explotables dentro del sistema ERP, lo que representa un riesgo inminente de incidentes de seguridad.

- **Fundamentación teórica:**

La propuesta está respaldada por marcos normativos sólidos y reconocidos internacionalmente. La norma **ISO/IEC 27032** proporciona un enfoque integral para la gestión de riesgos cibernéticos, incluyendo pautas sobre protección de sistemas críticos, respuesta a incidentes y concienciación del usuario. Por su parte, **ITIL V4** refuerza la necesidad de alinear la ciberseguridad con la continuidad del negocio, mediante la gestión estructurada de servicios tecnológicos.

- **Relevancia organizacional:**

La implementación de este plan contribuirá a mejorar la postura de seguridad de TiviTrace, garantizando la confidencialidad, integridad y disponibilidad de la

información. Asimismo, permitirá asegurar la operatividad del ERP, evitar interrupciones costosas y fomentar una cultura preventiva de seguridad que se traduzca en resiliencia institucional a largo plazo.

6.3. ALCANCE DE LA PROPUESTA

- **Implementar un mecanismo de autenticación multifactor (MFA)** para reforzar el control de accesos al ERP web, asegurando la validación de identidad conforme a los principios de protección de acceso definidos por ISO/IEC 27032.
- **Diseñar un programa de capacitación continua en ciberseguridad**, que incluya simulacros de ataques de ingeniería social (como phishing), sesiones formativas sobre buenas prácticas y mecanismos de reporte de incidentes, con el fin de fortalecer la concienciación del usuario y reducir el riesgo humano.
- **Proponer la implementación de una plataforma de gestión de eventos e información de seguridad (SIEM)**, con capacidades para detectar amenazas persistentes avanzadas (APT), correlacionar eventos en tiempo real y emitir alertas automatizadas para una respuesta temprana.
- **Desarrollar y formalizar un procedimiento de gestión de incidentes y un Plan de Continuidad del Negocio (BCP)**, estructurado conforme a las guías de ITIL V4, para garantizar la respuesta efectiva y la recuperación oportuna ante incidentes de seguridad en el entorno ERP.
- **Establecer un tablero de indicadores clave de desempeño (KPIs)** para monitorear la eficacia de las medidas implementadas, como niveles de

capacitación, número de incidentes detectados, tiempo medio de respuesta y recuperación ante fallos.

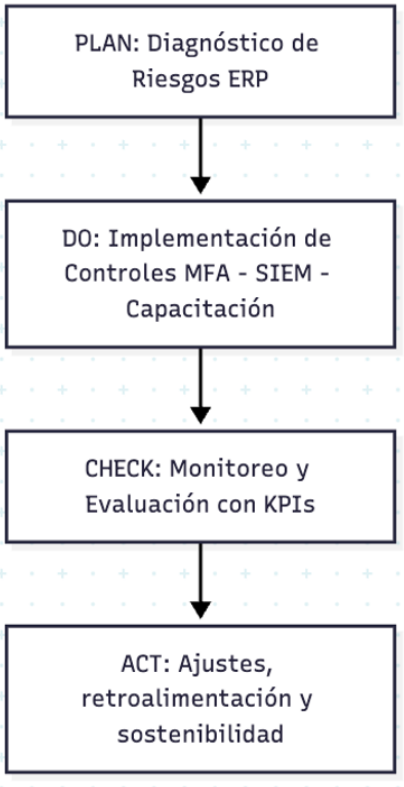
- **Realizar un análisis costo-beneficio del plan de implementación**, incorporando criterios de sostenibilidad técnica y financiera para asegurar su viabilidad a mediano y largo plazo dentro de la estructura operativa de TiviTrace.

6.4. DESCRIPCIÓN Y DESARROLLO A DETALLE DE LAPROPUESTA

6.4.1 ENFOQUE METODOLÓGICO Y ESTRUCTURA DEL PLAN

La propuesta para fortalecer la ciberseguridad en el ERP web empresarial de TiviTrace se fundamenta en el ciclo PDCA (Planificar, Hacer, Verificar y Actuar), el cual garantiza un proceso iterativo de mejora continua. Este enfoque permite una implementación ordenada, evaluable y ajustable del plan de ciberseguridad basado en las mejores prácticas de la norma ISO/IEC 27032 para la gestión de riesgos cibernéticos y el marco ITIL V4 para asegurar la continuidad del negocio y la calidad en la gestión de servicios TI.A continuación, se describe el flujo general de trabajo del plan:

Figura 60: Ciclo PDCA aplicado al plan de ciberseguridad para ERP en TiviTrace.



Nota: Elaboración propia.

La figura 60 ilustra la aplicación del ciclo PDCA (Plan-Do-Check-Act) en el diseño e implementación del plan de ciberseguridad propuesto para el sistema ERP de TiviTrace. Este enfoque secuencial y cíclico, representado de forma descendente, permite estructurar la mejora continua de los controles técnicos y organizativos necesarios para mitigar los riesgos cibernéticos identificados.

- PLAN (Diagnóstico de Riesgos ERP): Esta fase inicial comprende la identificación y análisis de vulnerabilidades en el sistema ERP a través de entrevistas, encuestas y listas de verificación. El diagnóstico permite establecer una línea base sobre la cual definir los objetivos de seguridad y los controles a implementar.
- DO (Implementación de Controles): Con base en los hallazgos, se ejecutan acciones específicas como la implementación de autenticación multifactor

(MFA), el despliegue de un sistema SIEM para monitoreo en tiempo real y la capacitación continua del personal en temas de ciberseguridad.

- CHECK (Monitoreo y Evaluación con KPIs): En esta etapa se revisa el desempeño de las acciones mediante indicadores clave (KPIs), lo cual permite evaluar la eficacia de las medidas implementadas y determinar posibles desviaciones respecto a los objetivos planteados.
- ACT (Ajustes, Retroalimentación y Sostenibilidad): Finalmente, se aplican mejoras correctivas y preventivas basadas en los resultados del monitoreo. Esta retroalimentación permite ajustar el plan, reforzar la sostenibilidad del sistema de gestión de ciberseguridad y reiniciar el ciclo con mayor madurez.

6.4.2 IMPLEMENTACIÓN DE CONTROLES TECNOLÓGICOS Y HUMANOS

Como parte fundamental del plan de ciberseguridad para TiviTrace, se propone la implementación de controles integrados tanto tecnológicos como humanos, que aborden las principales vulnerabilidades identificadas en el diagnóstico. Estos controles forman parte del enfoque integral de protección frente a amenazas cibernéticas, alineados con los lineamientos de la norma ISO/IEC 27032 y las buenas prácticas de continuidad del negocio en ITIL V4.

Una de las medidas prioritarias consiste en implementar un sistema robusto de autenticación multifactor (MFA) para el acceso al sistema ERP, con soporte para aplicaciones móviles y tokens físicos en los perfiles críticos. Esta medida mitigará significativamente los riesgos de accesos no autorizados derivados de contraseñas vulneradas o compartidas, especialmente en cuentas con privilegios administrativos o acceso a datos sensibles.

Actividades propuestas para su implementación:

- Evaluación y selección de un proveedor MFA que sea técnicamente compatible con el ERP actual de TiviTrace (como Duo Security, Google Authenticator o Microsoft Authenticator).
- Integración técnica mediante APIs con la infraestructura actual del sistema ERP.
- Realización de pruebas piloto controladas en un entorno de staging.
- Activación progresiva por niveles de criticidad de perfiles: primero cuentas administrativas, luego financieras, y finalmente operativas.
- Redacción de un procedimiento técnico-operativo para la gestión del MFA, incluyendo recuperación de accesos y auditoría.

Recursos tecnológicos necesarios:

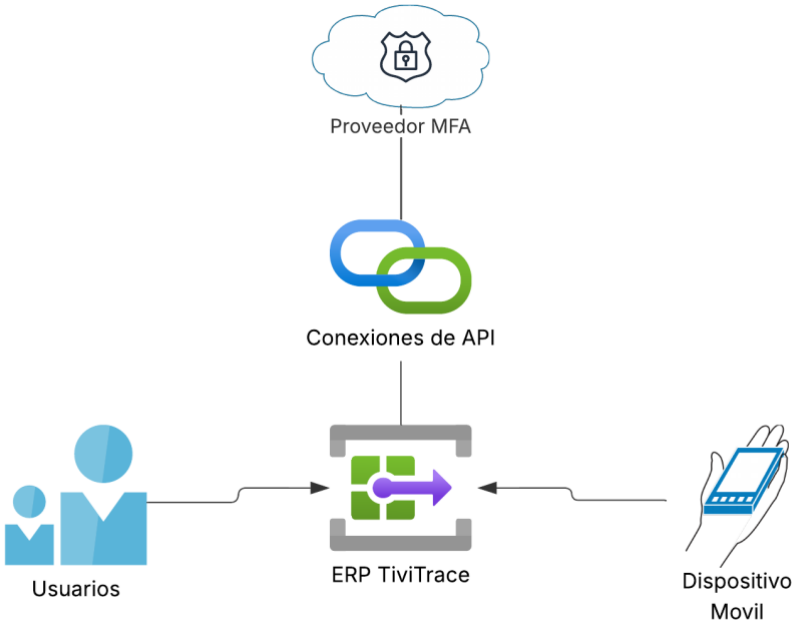
- API del proveedor seleccionado.
- Adaptador de autenticación compatible con el backend del ERP.
- Dispositivos móviles para usuarios finales, o entrega de tokens físicos en casos necesarios.
- Documentación técnica y manuales de usuario adaptados a cada rol.

Tabla 6: Comparativa de proveedores de MFA.

Proveedor	Compatibilidad ERP	Costo estimado	Soporte tokens físicos	App móvil
Duo Security	Alta	Medio	Sí	Sí
Google Auth	Alta	Bajo	No	Sí
Microsoft Auth	Alta	Bajo	Sí	Sí

Nota: **Elaboración Propia.**

Figura 61: Diagrama de arquitectura de implementación del MFA con el ERP de TiviTrace.



Nota: Elaboración propia.

La figura 61 ilustra la arquitectura propuesta para la integración de un sistema de autenticación multifactor (MFA) con el ERP utilizado por TiviTrace. Esta arquitectura contempla una implementación segura y compatible con los estándares actuales de interoperabilidad, mediante el uso de interfaces API entre el ERP y el proveedor de MFA seleccionado.

En la parte superior del diagrama se ubica el proveedor de MFA, que puede ser una solución como Duo Security, Google Authenticator o Microsoft Authenticator, todas con alta compatibilidad comprobada con sistemas ERP según la evaluación previa (ver Tabla 6). Este proveedor se conecta al ERP a través de un módulo de integración vía API, que permite validar el segundo factor de autenticación en cada intento de acceso al sistema.

Una vez validada la autenticación, el ERP permite el acceso a los usuarios registrados. El segundo factor puede ser generado a través de una aplicación móvil instalada en el dispositivo del usuario, o mediante tokens físicos cuando la operación lo requiera.

Esta solución permite una activación progresiva, iniciando por cuentas de alto riesgo como las administrativas y financieras, y extendiéndose posteriormente al resto de usuarios operativos. Además, contempla aspectos clave como la documentación técnica del proceso, la gestión de recuperación de accesos y la trazabilidad de los eventos de autenticación.

La arquitectura presentada asegura que la autenticación MFA se integre de forma no invasiva con el sistema actual, fortaleciendo los controles de acceso sin comprometer la experiencia de usuario ni la operatividad del ERP.

6.4.3 PROGRAMA DE CAPACITACIÓN CONTINUA EN CIBERSEGURIDAD

Con base en las vulnerabilidades detectadas durante la etapa de diagnóstico, particularmente la falta de conocimiento sobre buenas prácticas digitales, se propone la implementación de un programa integral de capacitación continua en ciberseguridad**,** enfocado en prevenir ataques como phishing, ingeniería social y amenazas persistentes avanzadas (APT), los cuales son vectores comunes de entrada en sistemas ERP empresariales.

Este programa estará dirigido tanto al personal operativo como administrativo de TiviTrace**,** y su diseño se adaptará al nivel técnico y rol funcional de cada grupo, asegurando una comprensión efectiva. Además, se establecerán mecanismos de medición del progreso mediante evaluaciones periódicas y seguimiento a través de plataformas LMS (Learning

Management System), asegurando un proceso de mejora continua, alineado con el ciclo de vida del servicio de ITIL V4 y el enfoque de concienciación propuesto por ISO/IEC 27032.

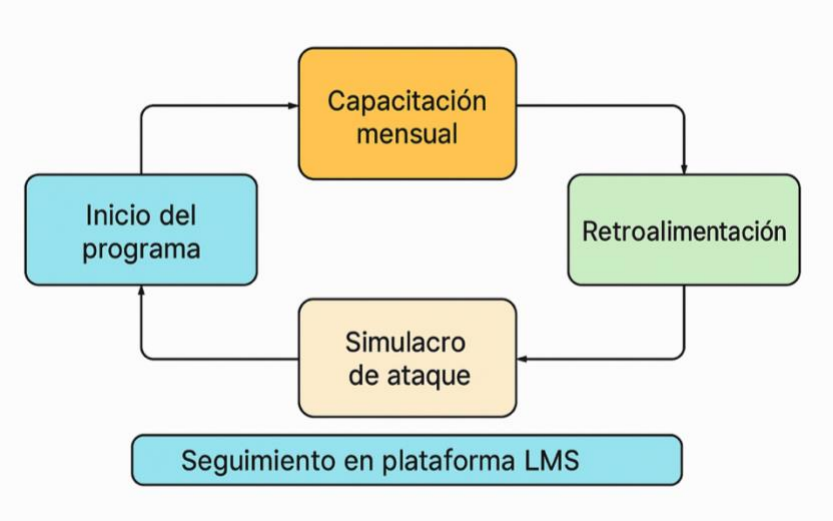
6.4.4 PROPUESTA DE ACCIONES A EJECUTAR:

- **Diseño de un plan de formación estructurado por niveles**: básico, intermedio y avanzado.
- **Sesiones teóricas mensuales** (1 hora), impartidas en formato virtual o híbrido, con material adaptado al entorno y procesos de TiviTrace.
- **Simulacros mensuales de ciberataques (phishing, smishing, etc.)**, para evaluar la capacidad de respuesta del personal y generar alertas tempranas.
- **Implementación de una plataforma LMS** para gestión del contenido, entrega de materiales, seguimiento de avances individuales y aplicación de retroalimentación.
- **Evaluación constante mediante KPIs**: tasa de apertura de correos falsos, porcentaje de respuestas inseguras, mejoras por empleado, etc.
- **Gamificación y microlearning** como metodología pedagógica, fomentando la participación activa y la retención del conocimiento en sesiones breves e interactivas.

6.4.5 MATERIALES SUGERIDOS:

- Videos de corta duración (5–10 minutos) con situaciones reales de TiviTrace.
- Cuestionarios de autoevaluación por módulo.
- Casos prácticos con toma de decisiones simulada.
- Infografías de rápida consulta (buenas prácticas, alertas comunes, rutas seguras).

Figura 62: Flujo del Programa de Capacitación Continua en Ciberseguridad.



Nota: Elaboración propia.

La figura 62 muestra el ciclo propuesto para la capacitación continua en ciberseguridad del personal de TiviTrace. El programa inicia con sesiones mensuales teóricas, seguidas de procesos de retroalimentación individual y simulacros de ataques (como phishing), lo cual permite evaluar la respuesta del personal en situaciones reales.

Este ciclo se repite de forma continua, fortaleciendo progresivamente la cultura de seguridad digital. La estrategia está apoyada por una plataforma LMS y materiales adaptados al contexto organizacional. El enfoque propuesto se alinea con los lineamientos de ISO/IEC 27032 e ITIL V4, y busca mejorar indicadores clave relacionados con el comportamiento humano frente a amenazas cibernéticas.

Resultados esperados:

- Reducción de incidentes de ciberseguridad provocados por errores humanos.
- Mayor cultura organizacional en temas de ciberseguridad.

- Resiliencia digital frente a amenazas de ingeniería social.
- Mejora en indicadores de cumplimiento de controles humanos propuestos por ISO/IEC 27032.
- Alineación con las dimensiones “Personas y Organización” e “Información y Tecnología” de ITIL V4.

6.4.6 IMPLEMENTACIÓN DE SISTEMA DE MONITOREO Y GESTIÓN DE EVENTOS (SIEM)

Para fortalecer la capacidad de detección temprana y respuesta ante incidentes de ciberseguridad en el ERP de TiviTrace, se propone la implementación de una solución SIEM (Security Information and Event Management). Este componente es esencial en un entorno moderno orientado a la protección proactiva, ya que permite capturar eventos en tiempo real, correlacionar múltiples fuentes de datos y generar alertas automatizadas frente a patrones de comportamiento anómalos o maliciosos.

El sistema SIEM se convierte en el núcleo del monitoreo activo, alineado con los controles técnicos recomendados por la norma ISO/IEC 27032 y el enfoque de mejora continua definido en ITIL V4.

Acciones propuestas:

- **Selección e implementación de una solución SIEM robusta**, preferentemente de código abierto o con licenciamiento flexible, como Wazuh, Splunk o Graylog, evaluando compatibilidad con infraestructura existente.

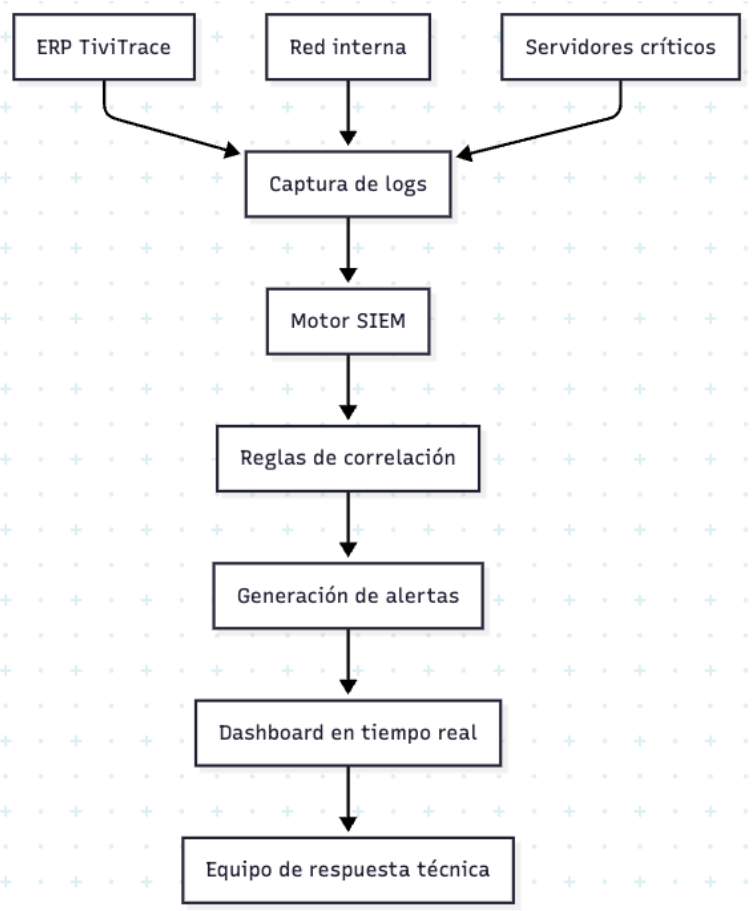
- **Integración del SIEM con los principales activos tecnológicos de TiviTrace**: el sistema ERP, servidores de aplicaciones, bases de datos, red corporativa, puntos de acceso, y endpoints críticos.
- **Definición y carga de reglas de correlación** específicas, orientadas a detectar:
    - Actividades inusuales de login (brute force).
    - Accesos desde ubicaciones geográficas no autorizadas.
    - Elevaciones sospechosas de privilegios.
    - Transferencias de archivos sensibles fuera del horario laboral.
- **Configuración de paneles de control (dashboards) en tiempo real, para el monitoreo por parte del equipo técnico.**
- **Capacitación especializada** para el personal de IT, orientada al análisis de logs, manejo de alertas, respuestas iniciales y documentación de incidentes.

Ejemplos de alertas críticas configurables:

- Más de 5 intentos fallidos de autenticación en un intervalo de 5 minutos.
- Acceso al ERP fuera del horario laboral desde una IP externa.
- Cambio de permisos en archivos críticos sin ticket registrado.
- Acceso simultáneo desde dos ubicaciones geográficamente distantes.

El siguiente diagrama presenta el flujo lógico de integración del sistema ERP con el SIEM, permitiendo la captura de eventos, su correlación, y la activación de alertas dirigidas al equipo de respuesta ante incidentes.

Figura 63: Arquitectura del sistema de monitoreo con SIEM integrado.



Nota: Elaboración propia.

La figura 63 presenta la integración del ERP TiviTrace con un sistema SIEM para la captura, análisis y correlación de eventos de seguridad provenientes del ERP, la red interna y servidores críticos. Los logs son centralizados y procesados por el motor SIEM, que aplica reglas de correlación para identificar actividades anómalas y generar alertas automáticas. Estas alertas se visualizan en un dashboard en tiempo real y son gestionadas por el equipo de respuesta técnica, permitiendo una detección temprana y una respuesta eficaz ante incidentes. La solución está alineada con las normas ISO/IEC 27032 e ITIL V4 para fortalecer la seguridad y continuidad operativa.

6.4.7 PROCEDIMIENTOS FORMALES Y GESTIÓN DE INCIDENTES

Como parte fundamental del plan de ciberseguridad propuesto para TiviTrace, se contempla el diseño, documentación e implementación de un procedimiento formal de gestión de incidentes de ciberseguridad y un Plan de Continuidad del Negocio (BCP), ambos estructurados conforme a las buenas prácticas de ITIL V4, particularmente en los dominios de “Gestión de la continuidad del servicio” y “Gestión de incidentes”, así como en la guía técnica de ISO/IEC 27032 para respuesta ante incidentes.

Estos procedimientos permitirán a TiviTrace responder de forma oportuna y eficiente ante eventos que comprometan la integridad, disponibilidad o confidencialidad del ERP, asegurando una recuperación rápida y una interrupción mínima en las operaciones críticas del negocio.

Objetivos de los procedimientos:

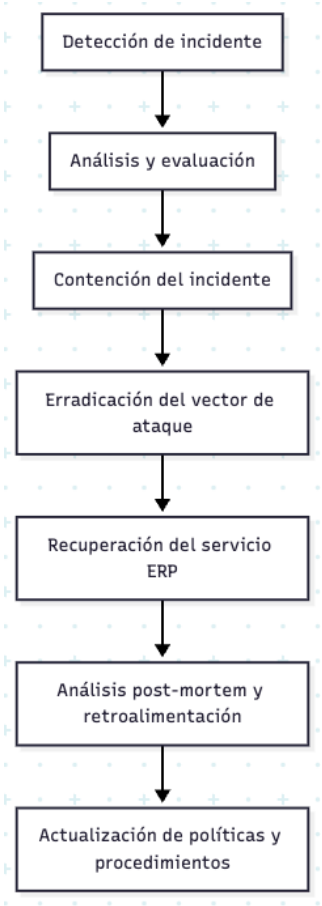
- Establecer roles y responsabilidades claros ante diferentes escenarios de incidentes.
- Definir mecanismos de comunicación interna y externa durante y después del incidente.
- Garantizar la trazabilidad de cada etapa: detección, análisis, contención, erradicación y recuperación.
- Promover la mejora continua a través de evaluaciones post-mortem y retroalimentación.

Documentos a desarrollar como parte de la propuesta:

- Manual de Gestión de Incidentes de Ciberseguridad, con procedimientos paso a paso y políticas internas.
- Checklists específicos por tipo de incidente (acceso no autorizado, malware, pérdida de datos, etc.).
- Plan de Recuperación ante Desastres (DRP): protocolo para restaurar sistemas críticos desde respaldos seguros.
- Plan de Continuidad Operativa (BCP): lineamientos para mantener operaciones mínimas durante incidentes de alto impacto.

  Referencia normativa: Se seguirá el enfoque de ITIL V4 en su componente de "Gestión de la continuidad del servicio" y la guía de ISO/IEC 27035 (gestión de incidentes).

Figura 64: Flujo propuesto para la gestión de incidentes de ciberseguridad en el entorno ERP de TiviTrace.



Nota: Elaboración propia.

El diagrama representa el proceso formal de gestión de incidentes de ciberseguridad diseñado para el entorno ERP de TiviTrace. El flujo inicia con la detección del incidente, seguido del análisis y evaluación del impacto. Posteriormente, se procede a la contención del incidente para limitar su efecto, y a la erradicación del vector de ataque que originó la amenaza. A continuación, se lleva a cabo la recuperación del servicio para restablecer la operatividad del ERP. Finalmente, se realiza un análisis post-mortem que proporciona retroalimentación para la actualización continua de políticas y procedimientos. Esta actualización fortalece la prevención, cerrando el ciclo de gestión y promoviendo la mejora continua.

Este procedimiento está alineado con las buenas prácticas de ITIL V4 y las recomendaciones de la norma ISO/IEC 27032, asegurando una respuesta estructurada, eficiente y documentada que minimiza el impacto de los incidentes y garantiza la continuidad del negocio.

Tabla 7: Flujograma simplificado de gestión de incidentes.

Fase	Acción principal	Responsable asignado
Detección	Recepción de alerta generada por SIEM	Equipo de seguridad informática
Análisis	Verificación de amenaza y evaluación del impacto	Encargado del sistema ERP
Contención	Bloqueo de acceso, aislamiento de sistemas	Administrador de red/ERP
Erradicación	Eliminación de la amenaza y restauración segura	Soporte técnico
Recuperación	Restauración desde backup y validación operativa	Área de infraestructura TI
Lecciones aprendidas	Análisis post mortem y mejoras al procedimiento	Comité de ciberseguridad

6.4.8 MONITOREO Y MEDICIÓN DE RESULTADOS

La correcta implementación de un plan de ciberseguridad no se limita a la ejecución de controles, sino que requiere una medición continua y sistemática de su desempeño. Por ello, se propone el desarrollo de un sistema de monitoreo basado en indicadores clave de desempeño (KPIs) que permita evaluar el nivel de madurez y eficacia de las acciones implementadas en TiviTrace. Este sistema será operado mediante un dashboard dinámico de control, el cual integrará datos provenientes del SIEM, del sistema LMS utilizado para capacitaciones, de auditorías internas y de registros de incidentes, permitiendo así una visualización en tiempo real del estado de seguridad de la empresa.

La medición no sólo facilitará el cumplimiento de los objetivos del plan, sino que también permitirá tomar decisiones basadas en evidencia, realizar ajustes oportunos, y

garantizar una mejora continua, en línea con el ciclo PDCA y las recomendaciones de ITIL V4.

Indicadores clave:

Tabla 8: Indicadores clave de desempeño (KPI) para la ciberseguridad en sistemas ERP.

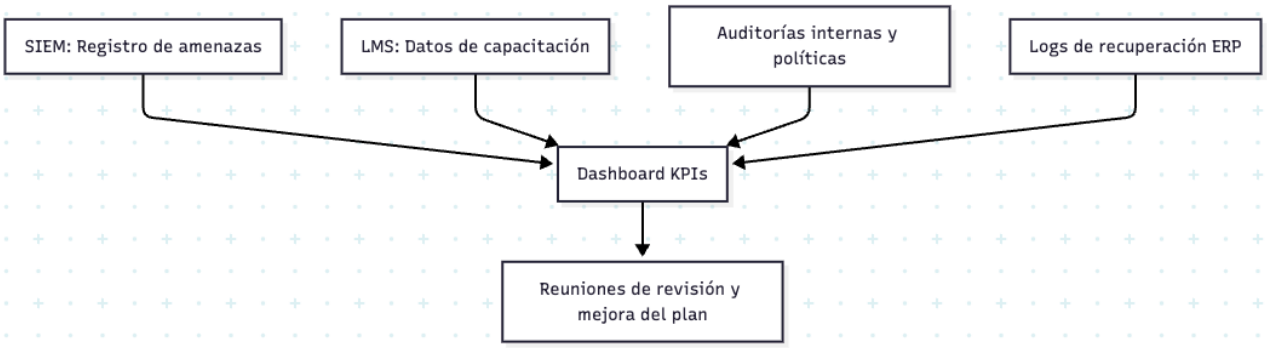
KPI	Meta esperada	Frecuencia de evaluación	Fuente de datos
Porcentaje de empleados capacitados en phishing	100 %	Trimestral	Plataforma LMS
Intentos de phishing detectados y bloqueados	Reducción del 50 %	Mensual	Sistema SIEM
Tiempo promedio de recuperación ante incidentes	Menor a 4 horas	Trimestral	Logs ERP y encuestas post-evento
Nivel de cumplimiento de políticas internas	Mayor al 90 %	Mensual	Auditorías internas
Uso efectivo de MFA en usuarios activos	100 %	Trimestral	Logs de autenticación del ERP

6.4.9 HERRAMIENTAS SUGERIDAS PARA VISUALIZACIÓN DE KPIS

Se recomienda implementar el dashboard mediante plataformas de visualización como Power BI **o** Grafana**,** las cuales permiten conectividad directa con bases de datos, servicios de red y herramientas externas como:

- **SIEM**: para métricas de amenazas e incidentes.
- **LMS**: para seguimiento de avance en capacitaciones.
- **Auditorías internas**: para el cumplimiento de normativas y políticas operativas.

Figura 65: Integración de fuentes de datos para visualización y toma de decisiones.



Nota: Elaboración propia.

La figura 65 muestra la integración de diversas fuentes de información relevantes para la gestión de la ciberseguridad y continuidad operativa en el entorno ERP de TiviTrace. Estas fuentes incluyen registros de amenazas generados por el sistema SIEM, datos de capacitación gestionados a través del LMS (Learning Management System), resultados de auditorías internas y políticas, así como logs relacionados con procesos de recuperación del ERP.

Toda esta información se centraliza en un dashboard de indicadores clave de desempeño (KPIs), el cual proporciona una visualización consolidada y en tiempo real para facilitar la toma de decisiones estratégicas. Este tablero es el insumo principal para las reuniones de revisión y mejora continua del plan de ciberseguridad, permitiendo al equipo responsable identificar áreas de oportunidad y ajustar políticas y procedimientos conforme a los resultados observados. Se recomienda la implementación de esta solución mediante plataformas de visualización avanzadas como Power BI o Grafana, que soportan la conexión directa a múltiples fuentes de datos y facilitan el monitoreo efectivo y la gestión integral del plan.

6.4.10 BENEFICIOS DE ESTE SISTEMA DE MONITOREO:

- Facilita la gobernanza del plan de ciberseguridad mediante evidencia concreta.
- Aumenta la transparencia interna y la rendición de cuentas.
- Reduce tiempos de respuesta ante desviaciones.
- Permite iterar el plan de forma dinámica y adaptativa.
- Refuerza el enfoque de mejora continua propuesto por ITIL V4 y el ciclo PDCA.

6.4.11 EVALUACIÓN FINANCIERA Y SOSTENIBILIDAD

Un componente esencial del plan de ciberseguridad propuesto para TiviTrace es la evaluación financiera, ya que la efectividad de las medidas sugeridas debe ir acompañada de viabilidad presupuestaria y sostenibilidad operativa en el tiempo. Para ello, se ha realizado un análisis detallado de los recursos económicos necesarios para la implementación inicial, así como de los costos recurrentes asociados al mantenimiento y mejora continua del sistema.

La inversión estimada considera los siguientes rubros: licenciamiento e implementación de soluciones tecnológicas (SIEM, MFA), desarrollo de capacidades humanas mediante una plataforma LMS y simulacros, consultorías especializadas para la elaboración de planes de continuidad y gestión de incidentes, y auditorías de documentación para validar los controles implementados.

El enfoque financiero del plan está diseñado con una estrategia escalonada, priorizando aquellas acciones que representan un mayor impacto en la reducción de riesgos y continuidad operativa durante la fase inicial. Este esquema permite un despliegue progresivo que facilita la adaptación organizacional y optimiza la relación costo-beneficio.

Además, se establece un marco para evaluar de forma periódica el retorno de inversión (ROI) en ciberseguridad. Este se calculará a partir de variables como la reducción en la frecuencia de incidentes, el ahorro por mitigación de pérdidas (interrupciones de servicio, fuga de información, recuperación) y las mejoras en el cumplimiento de normativas nacionales e internacionales.

Tabla 9: Presupuesto estimado por componente del plan de ciberseguridad.

Componente	Costo estimado (HNL)
Solución SIEM (Wazuh, Splunk, Graylog)	L. 78,700
Sistema de autenticación MFA	L. 39,300
Plataforma LMS para capacitación continua	L. 26,200
Consultoría en BCP y gestión de incidentes	L. 52,500
Auditoría inicial, pruebas y hardening	L. 39,300
Total estimado inicial	**L. 236,000**

6.4.12 RECOMENDACIÓN DE SOSTENIBILIDAD

Para garantizar la permanencia y efectividad del plan, se sugiere establecer una reserva anual en el presupuesto operativo de TI**,** que permita:

- Renovación de licencias y soporte.
- Capacitación continua del personal ante nuevas amenazas.
- Revisión y actualización de procedimientos (BCP, DRP).
- Auditorías internas o externas periódicas.
- Mejoras tecnológicas conforme evolucione el entorno de amenazas.

6.4.13 ESTIMACIÓN DEL RETORNO DE INVERSIÓN (ROI) EN CIBERSEGURIDAD

La implementación de un plan de ciberseguridad no debe ser vista únicamente como un gasto, sino como una inversión estratégica que protege los activos digitales, reduce riesgos operativos, evita sanciones legales **y** preserva la continuidad del negocio**.** En este contexto, el Retorno sobre la Inversión (ROI) se calcula a partir de la relación entre los beneficios económicos derivados de la reducción de incidentes y los costos de implementación.

El ROI estimado para TiviTrace contempla:

- **Reducción de pérdidas financieras** asociadas a incidentes de seguridad evitados (fuga de datos, interrupciones del ERP, fraudes).
- **Disminución de gastos en recuperación** por eventos cibernéticos no controlados.
- **Ahorros en multas o incumplimientos regulatorios** gracias a la adopción de mejores prácticas alineadas a estándares internacionales.
- **Mejora en la productividad** del personal al contar con sistemas estables y seguros.
- **Reducción del tiempo de inactividad** gracias a la aplicación del plan de continuidad (BCP/DRP) basado en ITIL V4.

Tabla 10: Estimación de beneficios económicos del plan de ciberseguridad y ROI proyectado.

Concepto	Valor estimado (HNL/año)
Incidentes de seguridad evitados (3-5/año)	L. 131,200 – L. 210,000
Tiempo productivo recuperado (en horas)	L. 31,400 – L. 52,400
Reducción de sanciones o pérdidas legales	L. 26,200 – L. 39,300
Costos evitados por pérdida de datos o accesos	L. 52,400 – L. 105,000
Total de beneficios estimados	L. 241,200 – L. 406,600
Inversión inicial (año 1)	L. 236,000
ROI estimado (beneficio / inversión)	102% – 172% (en el primer año)

Conclusión de sostenibilidad financiera

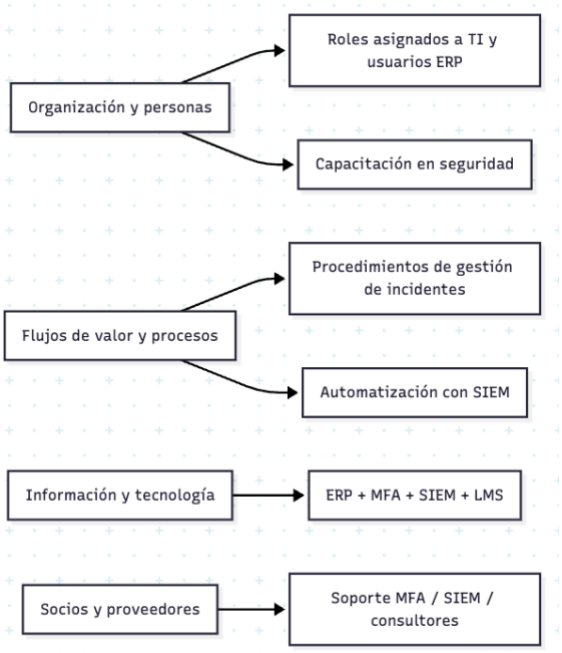
Este análisis confirma que el plan de ciberseguridad no solo es viable técnica y organizacionalmente, sino también financieramente. TiviTrace podría recuperar su inversión inicial en menos de un año, y obtener beneficios sostenidos en el mediano y largo plazo. Esta rentabilidad convierte el plan en un componente clave para la estrategia empresarial, con impacto directo en la resiliencia, reputación y cumplimiento normativo.

6.4.14 DIAGRAMA DEL MODELO DE GESTIÓN ITIL V4 APLICADO

Para visualizar cómo se integran los procesos de gestión de servicios TI en esta propuesta, se recomienda incluir un diagrama que represente las cuatro dimensiones del modelo ITIL V4 adaptadas a TiviTrace:

- **Organizaciones y personas**: roles y responsabilidades en seguridad.
- **Flujos de valor y procesos**: ciclo PDCA, gestión de incidentes, continuidad.
- **Información y tecnología**: herramientas implementadas (MFA, SIEM).
- **Socios y proveedores**: relaciones con proveedores de tecnología y servicios.

Figura 66: Modelo ITIL V4 adaptado para la gestión de ciberseguridad en TiviTrace.



Nota: Elaboración propia.

La figura 66 representa la aplicación del modelo ITIL V4 en el entorno del ERP de TiviTrace, integrando sus cuatro dimensiones clave. Se considera la asignación de roles y responsabilidades en ciberseguridad (organizaciones y personas), la implementación de procesos como gestión de incidentes y mejora continua (flujos de valor y procesos), el uso de herramientas como SIEM y MFA (información y tecnología), y la relación con proveedores tecnológicos estratégicos (socios y proveedores). Esta estructura permite una gestión integral y alineada con las mejores prácticas internacionales, fortaleciendo la continuidad operativa y la resiliencia del sistema.

6.4.15 DIAGRAMA DE DEFINICIÓN DE RESPONSABILIDADES POR EQUIPOS

Una gestión efectiva del plan de ciberseguridad requiere una asignación precisa y documentada de funciones entre los distintos equipos de la organización. En el contexto de TiviTrace, se propone la estructuración de responsabilidades distribuidas entre las áreas clave: Tecnología de la Información (TI), Seguridad de la Información, Desarrollo de Software y Dirección Administrativa.

Cada unidad desempeñará un rol específico en la implementación, operación y monitoreo del plan de ciberseguridad, conforme a los controles establecidos, y alineado con las mejores prácticas de ITIL V4, particularmente en su dimensión de "Organización y Personas". Asimismo, esta distribución de funciones se basa en las recomendaciones más recientes de la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), las cuales destacan la importancia de una coordinación eficaz y una gestión integral de roles frente a incidentes y amenazas digitales (CISA, 2024).

Las funciones están distribuidas de la siguiente manera:

A. **Equipo de TI**

- Integración y mantenimiento del sistema de autenticación multifactor (MFA).
- Configuración y operación técnica de la solución SIEM.
- Soporte técnico en procesos de recuperación ante incidentes.

B. Equipo de Seguridad de la Información

- Monitoreo activo de alertas y eventos críticos de seguridad.
- Configuración y afinación de reglas de detección de amenazas.
- Ejecución de análisis post-mortem y elaboración de reportes de incidentes.

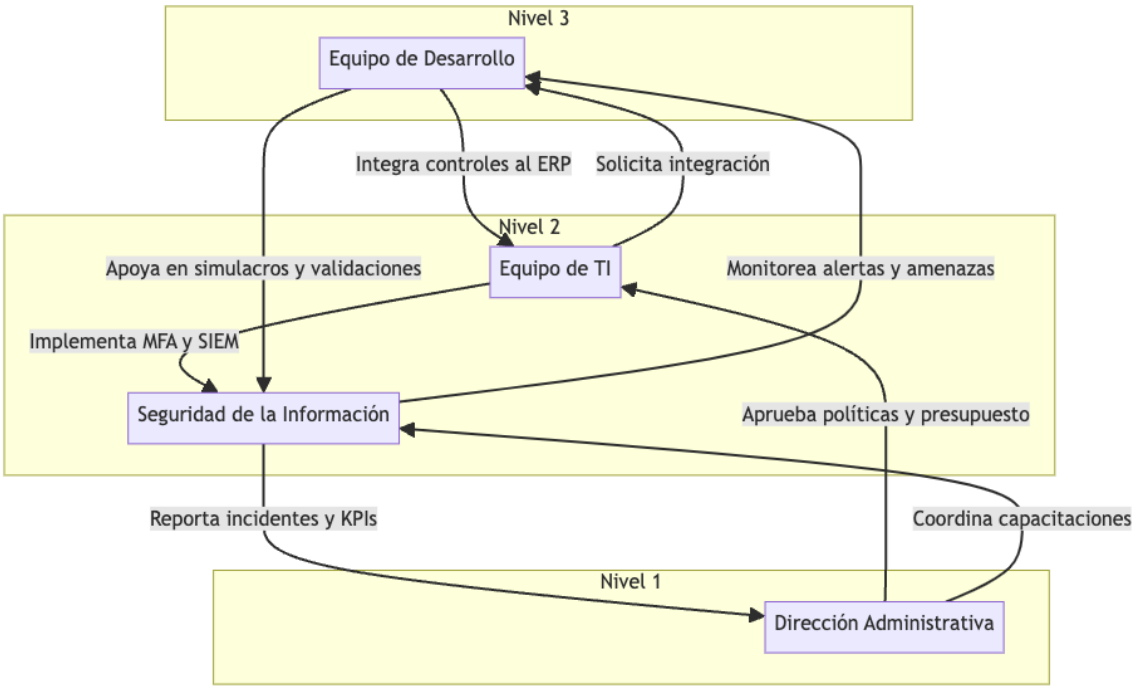
C. Equipo de Desarrollo

- Adaptación del sistema ERP para su integración con herramientas de seguridad.
- Soporte en simulacros de fallos y pruebas de recuperación controladas.
- Validación de criterios de seguridad en el desarrollo de nuevas funcionalidades o módulos del ERP.

D. Dirección Administrativa

- Aprobación de políticas y presupuesto destinados a la estrategia de ciberseguridad.
- Coordinación de programas de capacitación periódica dirigidos al personal.
- Evaluación de indicadores clave de desempeño y toma de decisiones estratégicas en seguridad informática.

Figura 67: Distribución de responsabilidades del plan de ciberseguridad en TiviTrace.



Nota: Elaboración propia.

El diagrama representa la distribución de funciones entre los equipos clave de TiviTrace para la implementación y operación del plan de ciberseguridad. La Dirección Administrativa aprueba las políticas y el presupuesto, además de coordinar los programas de capacitación. El equipo de Tecnología de la Información (TI) se encarga de implementar soluciones técnicas como la autenticación multifactor (MFA) y el sistema SIEM, mientras que el equipo de Seguridad de la Información gestiona el monitoreo de alertas, la detección de amenazas y la generación de reportes. A su vez, el equipo de Desarrollo apoya en la integración de controles dentro del ERP y participa en simulacros de validación. La retroalimentación y los indicadores clave (KPIs) son reportados a la Dirección para facilitar la toma de decisiones estratégicas. Esta estructura funcional está alineada con el marco ITIL V4 y las recomendaciones de CISA, promoviendo una gestión coordinada y eficaz frente a riesgos cibernéticos.

6.4.16 TABLA COMPARATIVA DE RIESGOS Y CONTROLES

Con el objetivo de facilitar el seguimiento y gestión del plan de ciberseguridad, se propone la elaboración de una tabla de trazabilidad entre los principales riesgos identificados en el diagnóstico y los controles implementados para mitigarlos. Esta herramienta permite evaluar de forma continua el estado de cumplimiento de cada medida y proporciona una base para la mejora continua del sistema de seguridad.

La tabla puede actualizarse de manera periódica durante las reuniones de revisión del plan, y será clave para documentar avances, priorizar acciones y comunicar resultados a la dirección de TiviTrace.

Tabla 11: Relación de riesgos identificados, controles implementados y estado de avance.

RIESGO IDENTIFICADO	CONTROL IMPLEMENTADO	ESTADO	COMENTARIOS
Acceso no autorizado al ERP	Autenticación mfa	En progreso	Requiere capacitación adicional
Phishing y ataques de ingeniería social	Programa de capacitación	Implementado	Simulacros mensuales
Ataques persistentes avanzados (apt)	Sistema siem	En progreso	Se integran alertas en tiempo real
Falta de gestión formal de incidentes	Procedimiento y plan bcp	Documentado	Pruebas planeadas trimestrales

6.4.17 MATRIZ DE CORRESPONDENCIA ENTRE LA NORMA ISO/IEC 27032 Y EL PLAN DE CIBERSEGURIDAD

Control ISO/IEC 27032:2023	Descripción breve	Acción del Plan de Ciberseguridad
Políticas para la seguridad en Internet	Definir y mantener directrices de uso seguro de redes y servicios web.	- Crear y aprobar la Política de Seguridad de Internet - Revisión anual en comité de ciberseguridad. - Difusión y aceptación formal por todo el personal.
Control de acceso	Asegurar que el acceso a sistemas y datos esté restringido según roles.	- Implementar RBAC en el ERP para permisos según perfil.
		- Desplegar MFA (apps o tokens físicos) en cuentas críticas y administrativas.
Educación, concienciación y formación	Capacitar a usuarios para reconocer y prevenir amenazas.	- Programa de formación en niveles (básico, intermedio, avanzado), con sesiones teóricas mensuales.
		- Simulacros de phishing trimestrales. - Medición de KPIs de respuesta humana.
Gestión de incidentes de seguridad	Proceder de forma estructurada ante eventos de seguridad.	- Documento de procedimiento de respuesta alineado a ITIL V4 (PDCA).
		- Simulacros de incidente y pruebas de BCP/DRP cada trimestre.
Gestión de activos	Inventariar y clasificar activos según criticidad y valor.	- Catálogo de módulos y recursos del ERP (Facturación, Contabilidad, Inventario).
		- Etiquetado con nivel de criticidad y revisión anual del inventario.
Gestión de la red	Diseñar perímetros y segmentación para aislar sistemas críticos.	- Subredes separadas para módulos financiero y operativo.
		- Firewalls y microsegmentación interna para impedir movimientos laterales.
Protección criptográfica	Usar cifrado sólido para proteger datos en tránsito y reposo.	- Cifrado AES-256 en bases de datos y TLS 1.2+ en comunicaciones ERP.
		- Gestión de claves con políticas de renovación y almacenamiento seguro.
Monitorización	Detectar y correlacionar eventos de seguridad de forma continua.	- Despliegue de un SIEM integrado con ERP, servidores y endpoints.
		- Reglas de correlación para APTs, brute-force y accesos no autorizados; dashboards en tiempo real para SOC inter

6.5. MEDIDAS DE CONTROL

Para asegurar que las acciones propuestas en el plan de ciberseguridad generen los resultados esperados, se establecen un conjunto de medidas de control e indicadores clave de desempeño (KPIs)**.** Estos permitirán monitorear la evolución de la implementación, identificar desviaciones, medir el impacto en la reducción de riesgos y facilitar la toma de decisiones informadas.

Los indicadores estarán estructurados bajo los principios de la gestión basada en resultados (MBR) y estarán alineados con los objetivos del ciclo PDCA (Plan-Do-Check-Act), descrito previamente.

Tabla 12: Indicadores clave de desempeño propuestos para el plan de ciberseguridad.

Indicador KPI	Meta esperada	Frecuencia	Fuente de datos	Responsable
% de usuarios con MFA habilitado	100 %	Mensual	Reporte de autenticación ERP	Equipo de TI
% de personal capacitado en ciberseguridad	≥ 95 %	Trimestral	LMS / Registros de asistencia	Seguridad de la Información
Tiempo promedio de respuesta a incidentes	< 4 horas	Trimestral	Registros SIEM / Logs de incidentes	Seguridad / TI
Reducción de intentos de phishing exitosos	≥ 50 % en el primer año	Mensual	Alertas SIEM / Simulacros	Seguridad de la Información
Nivel de cumplimiento de procedimientos internos	≥ 90 %	Bimestral	Auditoría interna / Checklists	Dirección / TI
N.º de pruebas exitosas del BCP / DRP	2 por año	Semestral	Registros de simulacros	Dirección / Seguridad

6.6. GESTIÓN DE LOS RIESGOS

En el marco de la propuesta de plan de ciberseguridad para la gestión de riesgos en el ERP web empresarial de TiviTrace, la gestión de riesgos se concibe como un proceso integral, continuo y adaptativo, diseñado para mitigar las vulnerabilidades y amenazas

detectadas durante el diagnóstico previo, y así fortalecer la protección de los activos digitales críticos.

Este proceso se basa en la norma ISO/IEC 27032, que provee directrices específicas para la ciberseguridad, y se complementa con el modelo de gobernanza y mejora continua de ITIL V4, lo cual garantiza la alineación estratégica con la gestión del servicio TI y la continuidad del negocio.

6.6.1 CICLO DE GESTIÓN DE RIESGOS PROPUESTO PARA TIVITRACE

Se plantea implementar un ciclo de gestión de riesgos con las siguientes fases operativas y alineadas con las condiciones y recursos de TiviTrace:

1. Identificación de riesgos

- Realización de auditorías internas y entrevistas focalizadas con áreas clave (TI, operaciones, RRHH).
- Uso del sistema SIEM para detección temprana de eventos y amenazas como accesos no autorizados, phishing dirigido, vulnerabilidades en el ERP y malas prácticas internas.
- Registro activo y actualización permanente en una plataforma digital interna que permita trazabilidad.

2. Análisis y evaluación del riesgo

- Aplicación de una matriz de probabilidad × impacto para cada riesgo detectado, priorizando los riesgos críticos que afecten la disponibilidad, confidencialidad e integridad del ERP.
- Validación con responsables de área para contextualizar el impacto operativo y económico.

3. Tratamiento del riesgo

- Definición de planes de acción específicos para cada riesgo priorizado:
    - Implementación de controles técnicos como MFA, firewalls, segmentación de red para accesos remotos.
    - Capacitación periódica en seguridad para todo el personal, con énfasis en prevención de phishing.
    - Procedimientos documentados para incidentes y continuidad, incluyendo pruebas de BCP/DRP.
    - Contratación de seguros cibernéticos para riesgos residuales o de difícil mitigación.

4. Monitoreo y revisión

- Establecimiento de KPIs clave para medir la efectividad de los controles, como número de incidentes, tiempo de respuesta, resultados de auditorías internas.
- Revisión trimestral formal con reportes a la dirección, ajustes de estrategia y actualización del registro de riesgos.

5. Comunicación y documentación

- Formalización de protocolos para la comunicación interna y externa ante incidentes.
- Documentación detallada y actualizada del proceso de gestión de riesgos, accesible para auditorías y cumplimiento normativo.

6.6.2 HERRAMIENTAS Y MECANISMOS DE APOYO

Para asegurar la efectividad del proceso, la propuesta contempla la integración de las siguientes herramientas y mecanismos:

- **Matriz de riesgos digitalizada:** Herramienta para evaluación dinámica de riesgos con actualización en tiempo real, accesible a stakeholders clave.
- **Sistema SIEM integrado con dashboards:** Para la supervisión continua y alertas tempranas, con capacidad de correlacionar eventos y generar reportes automatizados.
- **Software de gestión documental:** Para mantener registros de riesgos, incidentes, planes de acción y auditorías con control de versiones y acceso restringido.
- **Reuniones periódicas de revisión:** Comité de gestión de riesgos con participación de TI, seguridad, operaciones y dirección para evaluar avances y definir prioridades.

- **Programas de capacitación continua:** Materiales didácticos, simulacros y campañas de concientización orientados a reducir el factor humano como riesgo.

6.6.3 TABLA COMPARATIVA DE RIESGOS Y CONTROLES APLICADOS EN LA PROPUESTA

Tabla 13: Tabla comparativa de riesgos priorizados con controles propuestos e indicadores de éxito.

Riesgo identificado	Probabilidad	Impacto	Nivel de Riesgo	Control propuesto	Indicador de éxito
Acceso no autorizado al ERP	Alta	Alta	Crítico	Implementación de MFA y políticas estrictas	Reducción de incidentes de acceso no autorizado en 90%
Phishing dirigido al personal	Alta	Media	Alto	Capacitación y simulacros trimestrales	Disminución en reportes de phishing y pruebas exitosas
Ataques APT a servidores	Media	Alta	Alto	Configuración avanzada de SIEM y parches regulares	Tiempo medio de detección menor a 15 minutos
Fuga de información interna	Media	Media	Medio	Políticas de control de acceso y monitoreo continuo	Auditorías sin hallazgos críticos
Interrupción del servicio ERP	Baja	Alta	Alto	Procedimientos de BCP y DRP, respaldo automatizado	Pruebas de recuperación exitosas en <1 hora

6.6.4 ALINEACIÓN ESTRATÉGICA CON ISO/IEC 27032 E ITIL V4

- **ISO/IEC 27032:** La propuesta se fundamenta en esta norma para la evaluación continua y la mitigación efectiva de las amenazas cibernéticas específicas al entorno ERP de TiviTrace, promoviendo una cultura colaborativa entre áreas técnicas y de negocio, y facilitando la respuesta coordinada ante incidentes.
- **ITIL V4:** La implementación del plan se integra con las prácticas de gestión del servicio, enfocándose en la creación de valor mediante la resiliencia y la mejora continua, alineando la gestión de riesgos con la estrategia de TI y la continuidad del negocio, garantizando un servicio seguro y confiable para usuarios internos y externos.

6.7. ANÁLISIS Y ESTRATEGIAS DE MITIGACIÓN DE LA MATRIZ FODA

La Matriz FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) constituye una herramienta fundamental para analizar de manera integral el entorno interno y externo que rodea la gestión de la ciberseguridad en TiviTrace. Este análisis permite identificar los factores clave que pueden influir en la implementación del plan de ciberseguridad propuesto, facilitando la formulación de estrategias que potencien los recursos existentes, aprovechen las oportunidades del entorno, corrijan debilidades estructurales y enfrenten eficazmente las amenazas emergentes.

En el contexto específico de TiviTrace, la aplicación de la matriz FODA ha permitido evidenciar tanto capacidades internas relevantes como la conciencia institucional sobre la importancia de la ciberseguridad y el compromiso de la alta dirección, como limitaciones operativas relacionadas con la escasa implementación de controles técnicos avanzados y la falta de personal especializado. Asimismo, se han identificado oportunidades externas como el acceso a tecnologías asequibles y la disponibilidad de formación virtual, frente a amenazas crecientes como el aumento global de ataques dirigidos a sistemas ERP y la evolución constante de técnicas de ingeniería social como el phishing.

A partir de este diagnóstico, se han desarrollado estrategias combinadas que se agrupan en cuatro categorías fundamentales:

- Estrategias FO (Fortalezas + Oportunidades): Diseñadas para aprovechar al máximo las fortalezas internas de TiviTrace y capitalizar las oportunidades disponibles en el entorno tecnológico y normativo.
- Estrategias DO (Debilidades + Oportunidades): Orientadas a reducir o eliminar debilidades internas mediante el aprovechamiento de recursos y soluciones externas accesibles.

- Estrategias FA (Fortalezas + Amenazas): Enfocadas en utilizar las fortalezas internas como escudo frente a las amenazas externas identificadas.
- Estrategias DA (Debilidades + Amenazas): Dirigidas a mitigar los efectos negativos de las debilidades internas que podrían ser agravadas por amenazas del entorno.

El propósito de este análisis estratégico es proporcionar un marco estructurado para la toma de decisiones, que sirva como base para la priorización de acciones dentro del plan de ciberseguridad. De este modo, se busca asegurar que la propuesta esté alineada con las capacidades reales de la organización, contribuya a su continuidad operativa, y refuerce su resiliencia ante incidentes de seguridad que puedan comprometer el funcionamiento del sistema ERP.

Tabla 14: Análisis FODA aplicado a la gestión de ciberseguridad en el ERP empresarial.

Fortalezas (F)	Debilidades (D)
F1. Conciencia institucional sobre la importancia de la ciberseguridad	D1. Falta de personal especializado en seguridad informática
F2. ERP parcialmente adaptado a procesos internos	D2. Escasa implementación de controles técnicos avanzados
F3. Compromiso de la alta dirección hacia la mejora continua	D3. Capacitación irregular y limitada en ciberseguridad
F4. Existencia de políticas básicas de acceso y contraseñas	D4. Ausencia de monitoreo en tiempo real y protocolos contra APTs
F5. Adopción progresiva de marcos normativos (ISO/IEC 27032, ITIL V4)	D5. Brechas regulatorias por incumplimientos de protección de datos
F6. Disponibilidad de soluciones tecnológicas asequibles	D6. Pérdida de reputación por incidentes anteriores
F7. Posibilidad de alianzas con proveedores TI	D7. Evolución constante de técnicas de phishing (difícil actualización constante)
F8. Acceso a formación especializada (plataformas virtuales)	D8. Dificultad en retención y actualización de personal TI

Oportunidades (O)	Amenazas (A)
O1. Acceso a cursos y certificaciones virtuales especializadas	A1. Aumento global de ciberataques dirigidos a ERP
O2. Nuevas tecnologías de ciberseguridad disponibles (IA, SIEM, Zero Trust, etc.)	A2. Phishing y ataques de ingeniería social más sofisticados

O3. Mayor regulación en protección de datos (impulsa cumplimiento normativo)	A3. Riesgo de sanciones legales por incumplimiento
O4. Incentivos financieros o fiscales a empresas con ciberseguridad avanzada	A4. Daño reputacional ante incidentes públicos
O5. Cooperación interinstitucional en ciberdefensa	A5. Escalabilidad del ERP sin controles adecuados incrementa exposición
O6. Fondos regionales o donaciones para digitalización segura	A6. Dependencia de proveedores externos sin acuerdos de nivel de servicio (SLA)

6.7.1 ESTRATEGIAS DERIVADAS DEL ANÁLISIS FODA

Estrategias FO (Fortalezas + Oportunidades)

Aprovechan fortalezas internas para explotar oportunidades externas.

ESTRATEGIA	DESCRIPCIÓN
FO1	Desarrollar un programa continuo de formación en ciberseguridad utilizando plataformas virtuales especializadas (como Coursera, Udemy, ESET, etc.), aprovechando el compromiso institucional y la disponibilidad de acceso a formación digital.
FO2	Implementar herramientas tecnológicas asequibles y de bajo costo como Wazuh (SIEM open-source), Fail2Ban o firewalls UTM de código abierto, integrándolas a las políticas básicas de acceso existentes para reforzar la seguridad técnica del ERP.
FO3	Impulsar un proyecto institucional de adopción formal de ISO/IEC 27032 con apoyo de la alta dirección, buscando además incentivos fiscales, financiamiento o beneficios regulatorios vinculados a cumplimiento normativo.

Estrategias DO (Debilidades + Oportunidades)

Reducen debilidades internas aprovechando oportunidades del entorno.

ESTRATEGIA	DESCRIPCIÓN
DO1	Suplir la falta de personal especializado mediante convenios con proveedores externos de servicios de ciberseguridad (outsourcing), o mediante contratación de consultores certificados en ISO/IEC 27032 o Ethical Hacking.
DO2	Implementar un sistema de monitoreo en tiempo real, como SIEM en la nube, que no requiera infraestructura compleja, para superar la ausencia de controles avanzados y aumentar la visibilidad frente a amenazas.
DO3	Formalizar un plan institucional de capacitación obligatoria para todo el personal, incluyendo cursos básicos de concientización sobre amenazas y simulacros de phishing, aprovechando los recursos de formación gratuita en línea.
DO4	Crear un comité de cumplimiento normativo que evalúe y aplique las nuevas exigencias legales en materia de protección de datos, reduciendo las brechas regulatorias actuales y previniendo posibles sanciones.

Estrategias FA (Fortalezas + Amenazas)

Usan fortalezas internas para enfrentar amenazas externas.

ESTRATEGIA	DESCRIPCIÓN
FA1	Aplicar controles definidos en la norma ISO/IEC 27032 para proteger el ERP ante ciberataques dirigidos (como APTs), aprovechando la familiarización institucional con marcos normativos y la existencia de políticas iniciales.
FA2	Aprovechar el compromiso de la alta dirección para establecer un plan de respuesta a incidentes que contemple gestión reputacional y comunicación de crisis, minimizando el impacto ante posibles ataques públicos o filtraciones.
FA3	Usar la posibilidad de alianzas estratégicas con proveedores para formalizar contratos con SLAs y cláusulas de ciberseguridad, mitigando los riesgos relacionados con la dependencia de servicios externos sin garantías.

Estrategias DA (Debilidades + Amenazas)

Reducen debilidades que pueden ser explotadas por amenazas externas.

ESTRATEGIA	DESCRIPCIÓN
DA1	Diseñar protocolos específicos para la detección, análisis y contención de ataques persistentes avanzados (APT), y reforzar la protección contra técnicas de phishing evolucionadas mediante simulacros y actualizaciones constantes.
DA2	Crear e implementar un plan de gestión de incidentes y continuidad del negocio (BCP/DRP), incluyendo escenarios de crisis reputacional, pérdida de datos o ataques mediáticos, con enfoque preventivo y comunicacional.
DA3	Establecer auditorías periódicas legales y técnicas para asegurar el cumplimiento normativo en protección de datos (como la Ley de Protección de Datos Personales), reduciendo los riesgos legales y económicos asociados.

6.8. ANÁLISIS DEL DIAGRAMA DE ISHIKAWA

El Diagrama de Ishikawa o diagrama de causa-efecto (ver Figura 18: Diagrama de Ishikawa del Proyecto) permitió identificar las causas raíz que contribuyen a la alta vulnerabilidad ante ataques de ingeniería social (especialmente *phishing*) en el uso del sistema ERP de TiviTrace. Estas causas se agrupan en seis categorías clave: Tecnología, Entorno, Recursos, Personas, Procesos y Políticas.

A partir del análisis detallado de estas causas, se desarrolla el siguiente Plan de Mitigación, que propone acciones concretas y viables para abordar cada problemática. Este plan tiene como objetivo:

- Reducir el riesgo de incidentes de phishing, mediante medidas técnicas, organizativas y de concientización.
- Fortalecer la postura de ciberseguridad del sistema ERP sin requerir inversiones desproporcionadas.
- Alinear las acciones con la propuesta basada en ISO/IEC 27032 e ITIL V4, contribuyendo a una gestión integral y proactiva de los riesgos cibernéticos.

La siguiente tabla presenta las acciones de mitigación propuestas para cada categoría, garantizando que el enfoque se mantenga alineado con las buenas prácticas en ciberseguridad y con los objetivos estratégicos de TiviTrace.

Tabla 15: Problemas identificados y acciones de mitigación por categoría en la gestión de ciberseguridad ERP.

Categoría	*Problema Identificado*	*Acción de Mitigación*
Tecnología	Falta de herramientas antiphishing integradas en el ERP	Integrar filtros antiphishing con alertas automáticas y sandboxing en el ERP.
Tecnología	Deficiente encriptación de datos en correos o portales	Aplicar cifrado TLS para comunicaciones y políticas de uso de correo seguro.
Tecnología	Ausencia de doble factor de autenticación (2FA)	Implementar autenticación multifactor (MFA) para todos los accesos críticos.
Tecnología	Uso de dispositivos personales no seguros	Aplicar políticas de BYOD con control de acceso y escaneo de seguridad.
Entorno	Aumento de amenazas externas como phishing dirigido	Activar un sistema SIEM con reglas específicas para detección de phishing.
Recursos	Inversión limitada en ciberseguridad	Priorizar controles críticos en fases e identificar soluciones open-source.
Recursos	Falta de presupuesto para actualizaciones	Establecer un plan de actualización trimestral ajustado a recursos disponibles.
Recursos	Ausencia de personal exclusivo de ciberseguridad	Designar un responsable interno con apoyo externo parcial (outsourcing).

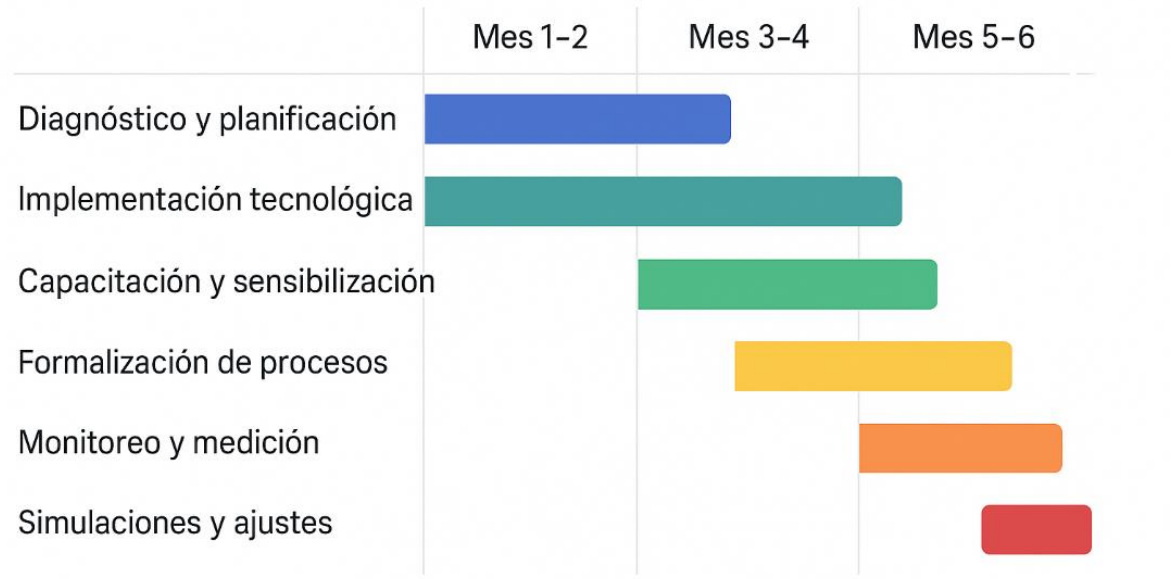
Personas	Desconocimiento de procedimientos ante ataques	Realizar simulacros de phishing y entrenamientos mensuales con retroalimentación.
Personas	Baja sensibilización ante correos sospechosos	Implementar campañas educativas gamificadas y boletines de alerta.
Personas	Inter confianza en remitentes conocidos	Reforzar la verificación de remitentes mediante políticas claras y ejemplos prácticos.
Personas	Respuesta lenta ante incidentes	Crear un protocolo de respuesta rápida con responsables definidos por área.
Procesos	Falta de validación en accesos remotos	Establecer controles geográficos y horarios para accesos, y validación previa.
Procesos	Inexistencia de protocolos de verificación	Documentar y aplicar procedimientos para manejo seguro de información sensible.
Políticas	Ausencia de políticas internas para correo electrónico	Diseñar y publicar una política institucional de uso seguro del correo.
Políticas	Poca vigilancia del cumplimiento de normas ISO/IEC	Realizar auditorías internas semestrales con checklist basado en ISO/IEC 27032.
Políticas	Ausencia de política de seguridad de la información	Elaborar una política integral de seguridad de la información y difundirla internamente.

Nota: *Elaboración propia con base en el análisis del Diagrama de Ishikawa aplicado al contexto de TiviTrace.*

6.9. CRONOGRAMA DE IMPLEMENTACIÓN Y PRESUPUESTO ESTIMADO

La implementación del plan de ciberseguridad se realizará de forma escalonada en un período estimado de 6 meses, permitiendo ajustes progresivos, pruebas y evaluación continua. El cronograma se estructura en cuatro fases principales, siguiendo el ciclo de vida de implementación de servicios recomendado por ITIL V4**:**

Figura 68: Cronograma de implementación del plan de ciberseguridad.



Nota: *Elaboración propia.*

Tabla 16: Presupuesto estimado por componente del plan.

Componente	**Valor estimado (HNL)**
Implementación de SIEM (licencia, soporte, setup)	L. 78,800
Licencias y soporte del sistema MFA	L. 39,400
Plataforma LMS y contenido de capacitación	L. 26,300
Consultoría en BCP y gestión de incidentes	L. 52,500
Auditoría documental y pruebas de seguridad	L. 39,000
Total de inversión estimada (año 1)	**L. 236,000**

6.10. CONCORDANCIA DE LOS SEGMENTOS DE LA TESIS CON LA PROPUESTA

CAPÍTULO I			CAPÍTULO II	CAPÍTULO III			CAPÍTULO V	CAPÍTULO VI	
Título de la Investigación	**Preguntas de Investigación**	**Objetivos Específicos**	**Metodología**	**Instrumentos**	**Variables**	**Indicadores**	**Conclusiones**	**Nombre de la Propuesta**	**Objetivo Propue**
Plan de ciberseguridad para la gestión de riesgos en ERP web empresariales basado en ISO/IEC 27032 e ITIL V4	1. ¿Cuáles son los principales riesgos de ciberseguridad en ERP empresariales?	1. Identificar y clasificar los riesgos de ciberseguridad en ERP mediante análisis de vulnerabilidades y auditorías	Mixto	Guía de Entrevista Semiestructurada sobre Ciberseguridad en ERP Empresariales, Lista de Verificación ISO/IEC 27032 para Sistemas ERP, Encuesta sobre Ciberseguridad en el uso del ERP Empresarial	Tipos de riesgos: phishing, accesos no autorizados, errores humanos	Frecuencia de incidentes, criticidad de amenazas	Se detectaron amenazas prioritarias: ingeniería social (phishing), accesos no autorizados y falta de auditorías.	PLAN DE CIBERSEGURIDAD PARA LA GESTIÓN DE RIESGOS EN ERP WEB EMPRESARIALES BASADO EN ISO/IEC 27032 E ITIL V4	Detecta priorizar ri críticos p diseña control efectiv
	2. ¿Cómo pueden aplicarse las mejores prácticas de ISO/IEC 27032 en la gestión de riesgos en ERP?	2. Analizar la aplicabilidad de ISO/IEC 27032 en la gestión de riesgos en ERP	Mixto	Lista de Verificación ISO/IEC 27032 para Sistemas ERP, Guía de Entrevista Semiestructurada sobre Ciberseguridad en ERP Empresariales	Nivel de implementación de controles ISO/IEC 27032	Grado de adopción y cumplimiento de prácticas recomendadas	Aplicación incipiente de ISO/IEC 27032; limitaciones por falta de personal y cultura organizacional.		Adapta control ISO/IEC 2 progresiva a la reali organizac

	3. ¿Qué estrategias pueden implementarse para detección y mitigación de Amenazas Persistentes Avanzadas (APT) en ERP?	3. Definir estrategias para detección y mitigación de APT usando controles ISO/IEC 27032	Mixto	Guía de Entrevista Semiestructurada sobre Ciberseguridad en ERP Empresariales	Existencia de herramientas y procesos para detección de APT	Número de alertas, capacidad de respuesta temprana	Ausencia de mecanismos estructurados para APT; necesidad de mejorar infraestructura y competencias.		Integrar SI monitoreo detecció respues temprana a
	4. ¿Cómo puede un plan alineado con ITIL V4 contribuir a la continuidad del negocio en ERP?	4. Identificar activos y definir planes de respuesta y recuperación alineados con ITIL V4 para mejorar continuidad	Mixto	Guía de Entrevista Semiestructurada sobre Ciberseguridad en ERP Empresariales, Lista de Verificación ISO/IEC 27032 para Sistemas ERP	Categorías de activos y niveles de riesgo	Tiempo medio de respuesta, efectividad de planes BCP	Falta de equipos limita capacidad operativa; se recomienda planes flexibles y tercerización estratégica.		Formali procedimi y Plan Continui alineados a V4
	5. ¿Cómo medir la efectividad del plan en la reducción de riesgos en ERP?	5. Evaluar impacto del plan mediante KPIs para medir efectividad en reducción de riesgos	Mixto	Encuesta sobre Ciberseguridad en el uso del ERP Empresarial	Indicadores KPI: capacitación, incidentes, tiempos de respuesta	Mejora en capacitación, reducción de incidentes, reducción de tiempos de respuesta	Deficiencias en capacitación y cultura organizacional; actitud favorable hacia mejora continua.		Estable tablero de para moni y mejo continu

BIBLIOGRAFÍA:

1. **Splashtop**. (s. f.). *Caso práctico: Monitor ERP*. https://www.splashtop.com/es/resources/case-studies/monitor-erp-dramatically-reduces-cybersecurity-risks-while-remotely
2. **Jackley, M.** (2023, 10 de enero). *3 ERP implementation case studies*. Oracle Sénégal. https://www.oracle.com/sn/erp/what-is-erp/erp-implementation-case-study/
3. **Partner Perspectives**. (s. f.). *Hormel Foods modernizes their back office with KPMG and Oracle Cloud*. https://partnerperspectives.libsyn.com/hormel-foods-modernizes-their-back-office-with-kpmg-and-oracle-cloud
4. **Brown, C.** (2022, 14 de diciembre). *Hormel Foods collaborates with Crisp and Google Cloud to provide real-time visibility into sales & supply chain data*. Hormel Foods. https://www.hormelfoods.com/newsroom/news/hormel-foods-collaborates-with-crisp-and-google-cloud-to-provide-real-time-visibility-into-sales-supply-chain-data/
5. **Guitart, I., & Carolina, R. H. E.** (2024, 15 de enero). *Implantación de un sistema ERP en una empresa de ciberseguridad: «DataSentinel S.L.»* https://openaccess.uoc.edu/handle/10609/149526
6. La Prensa. (2023). *Honduras: Ataques cibernéticos causan pérdidas millonarias en 2023.* La Prensa. Recuperado de https://www.laprensa.hn/honduras/honduras-ataques-ciberneticos-causan-perdidas-millonarias-2023-NK16498702
7. Advice Group Latam. (2021). *Estadísticas de ciberseguridad en Centroamérica y Colombia.* Advice Group. Recuperado de https://advicegroup-latam.com/estadisticas-de-ciberseguridad-en-centroamerica-y-colombia

8. Bautista Chimarro, F. F., Flores Ruiz, A. E., & Aguirre Inga, R. G. (2023). Ciberseguridad en pymes: Caso de estudio en Cayambe. *Dominio de las Ciencias, 9*(4), 388-402. https://dominiodelasciencias.com/ojs/index.php/es/article/view/3597
9. **Instituto Nacional de Estándares y Tecnología** (NIST). (2020). *Controles de seguridad y privacidad para sistemas y organizaciones de información (SP 800-53 Rev. 5).* U.S. Department of Commerce. Recuperado de https://csrc.nist.gov/pubs/sp/800/53/r5/final
10. **ISO/IEC.** (2022). *ISO/IEC 27032:2022 - Directrices para la ciberseguridad.* Organización Internacional de Normalización. Recuperado de https://www.iso.org/standard/44375.html
11. **Tarlogic Security.** (2023). *Auditoría de seguridad: Conocer las vulnerabilidades.* Recuperado de https://www.tarlogic.com/es/blog/auditoria-seguridad-vulnerabilidades/
12. **Revista Seguridad 360**. (2023). *Evaluación de riesgos de ciberseguridad en grandes empresas: Estrategias y mejores prácticas.* Recuperado de https://revistaseguridad360.com/noticias/ciberseguridad/evaluacion-de-riesgos-de-ciberseguridad-en-grandes-empresas-estrategias-y-mejores-practicas/
13. **Chen, Y., Lin, J., & Wang, L.** (2021). Threat Management in Enterprise Resource Planning Systems: A Cybersecurity Perspective. Computers & Security, 110, 102396. https://doi.org/10.1016/j.cose.2021.102396
14. **International Organization for Standardization (ISO).** (2023). ISO/IEC 27032:2023 - Guidelines for Cybersecurity. ISO.

15. **National Institute of Standards and Technology (NIST).** (2022). NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations. U.S. Department of Commerce.
16. **Sommers, J., & Bensoussan, A.** (2023). Information Security Governance: Implementing ISO/IEC Standards in Corporate Environments. Information Systems Journal, 28(3), 217-235. https://doi.org/10.1080/1034567.2023.217235
17. **Almeida, J.** (2022). Cybersecurity in Enterprise Resource Planning Systems: Challenges and Solutions. Cybersecurity Journal, 18(4), 45-62.
18. **National Institute of Standards and Technology [NIST].** (2022). Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations. U.S. Department of Commerce.
19. **Latam, P. (2024, 23 mayo).** ***Ciberseguridad en Honduras*****.** Pentesting Latam. https://www.pentestinglatam.com/ciberseguridad-en-honduras/
20. **Burgos, J. (2021, 23 diciembre).** ***Ciberataques aumentan impulsados por la transformación digital de las organizaciones***. Criterio.hn. https://criterio.hn/ciberataques-aumentan-impulsados-por-la-transformacion-digital-de-las-organizaciones/
21. **ISO/IEC 27032:2012**. *Information technology Security techniques Guidelines for cybersecurity*
22. Peikari, H., & Becerra, G. (2021). "Cybersecurity Governance: A Theoretical Framework for Organizational Risk Management in the Age of Digital Transformation." *Journal of Cybersecurity*, 3(2), 129-145.
23. Schwab, Klaus. (2016). *The Fourth Industrial Revolution*.
24. AXELOS. (2019). *ITIL 4 Foundation*. London: AXELOS.

25. Saha, A., & Smith, K. (2020). "Adapting ITIL for the Fourth Industrial Revolution: Strategies for Digital Transformation." *Journal of Information Technology and Management*, 31(1), 42-58.

26. Schwab, Klaus. (2016). *The Fourth Industrial Revolution*.

27. Comisión Nacional de Telecomunicaciones (CONATEL). (2024). *Plan estratégico institucional 2022-2026*. Recuperado de https://www.conatel.gob.hn/wp-content/uploads/2024/06/PLAN-ESTRATEGICO-INSTITUCIONAL-2022-a-2026.pdf

28. El Heraldo. (2023, enero 21). *Instituciones del Estado vulnerables a ciberataques en Honduras*. El Heraldo. Recuperado de https://www.elheraldo.hn/honduras/instituciones-estado-vulnerables-ciberataques-honduras-HL20818492

29. La Prensa. (2022, diciembre 15). *Empresas hondureñas, en riesgo por ciberataques de phishing e inteligencia artificial*. La Prensa. Recuperado de https://www.laprensa.hn/premium/empresas-hondurenas-riesgo-ciberataques-inteligencia-artificial-GE23636303

30. Seguridad y ciberseguridad. (2020, 17 septiembre). Comisión Nacional de Bancos y Seguros. https://www.cnbs.gob.hn/documentos-fintech/seguridad-y-ciberseguridad/

31. Redacción. (s. f.). Incidentes de Ciberseguridad más relevantes del 2022. https://eldiariodehonduras.hn/index.php/tech/4526-incidentes-de-ciberseguridad-mas-relevantes-del-2022

32. Zapata, D. (2024, 12 agosto). Ciberataques en Honduras: 1.8 millones de incidentes en 2023. *www.laprensa.hn*. https://www.laprensa.hn/honduras/ciberataques-honduras-1-8-millones-incidentes-HJ20835013
33. AXELOS. (2020). *ITIL® 4: Digital and IT Strategy.* The Stationery Office. Recuperado de https://www.axelos.com
34. International Organization for Standardization (ISO/IEC). (2023). *ISO/IEC 27032:2023 Information technology – Cybersecurity – Guidelines for internet security.* Recuperado de https://www.iso.org/standard/44375.html
35. OWASP Foundation. (2023). *OWASP ZAP.* Recuperado de https://www.zaproxy.org
36. Tenable. (2023). *Nessus Vulnerability Scanner.* Recuperado de https://www.tenable.com/products/nessus
37. Splunk. (2023). *Splunk Enterprise Security.* Recuperado de https://www.splunk.com/en_us/software/enterprise-security.html
38. IBM. (2023). *IBM Security QRadar SIEM.* Recuperado de https://www.ibm.com/products/qradar-siem
39. Hernández-Sampieri, R., Fernández-Collado, C., & Baptista-Lucio, M. P. (2014). *Metodología de la investigación*. McGraw-Hill Education.
40. Arias, F. G. (2012). *El proyecto de investigación: Introducción a la metodología científica* (6.ª ed.). Episteme.
41. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa
42. Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th ed.). SAGE Publications.

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

44. George, D., & Mallery, P. (2019). *IBM SPSS Statistics 26 Step by Step: A Simple Guide and Reference* (16th ed.). Routledge. https://doi.org/10.4324/9780429056765

45. Hernández-Sampieri, R., Fernández-Collado, C., & Baptista, P. (2014). *Metodología de la investigación* (6.ª ed.). McGraw-Hill.

46. Hernández-Sampieri, R., Mendoza, C., & Mendoza, P. (2022). *Metodología de la Investigación* (7.ª ed.). McGraw-Hill.

47. International Organization for Standardization. (2012). *ISO/IEC 27032:2012 Guidelines for cybersecurity*. https://www.iso.org/standard/44375.html

48. International Organization for Standardization. (2023). *ISO/IEC 27032:2023 Cybersecurity Guidelines*. https://www.iso.org/standard/84992.html

49. Instituto Nacional de Estándares y Tecnología (NIST). (2020). *Controles de seguridad y privacidad para sistemas y organizaciones de información (SP 800-53 Rev. 5)*. U.S. Department of Commerce. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

50. Sampieri, R. H., Collado, C. F., & Lucio, M. P. B. (2020). *Metodología de la investigación* (7.ª ed.). McGraw-Hill.

51. C*ybersecurity and Infrastructure Security Agency. (2023).* Cybersecurity Incident Response | CISA. *Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/topics/cybersecurity-best-practices/organizations-and-cyber-safety/cybersecurity-incident-response*

ANEXOS

A. ANEXO 1: GUÍA DE ENTREVISTA SEMIESTRUCTURADA

GUÍA DE ENTREVISTA SEMIESTRUCTURADA

DESCRIPCIÓN

Esta entrevista está dirigida a responsables de ciberseguridad, IT Managers y otros profesionales involucrados en la gestión de sistemas ERP. Su objetivo es explorar la seguridad en los ERP empresariales, identificando amenazas, medidas de protección y mejores prácticas

---

CONSENTIMIENTO DE PARTICIPACIÓN

Su participación en esta entrevista es voluntaria. La información será utilizada únicamente con fines académicos y se garantizará su confidencialidad. Al continuar con la entrevista, usted acepta participar de manera informada en este estudio.

INFORMACIÓN SOCIODEMOGRÁFICA

Nombre del entrevistado: _____

Cargo: _____

Empresa: _____

Años de experiencia en ciberseguridad / IT: _____

SECCIÓN 1: CONTEXTO DE LA EMPRESA

1.¿Puede describir brevemente su empresa, su tamaño y los servicios principales que ofrece?
2.¿Qué sistemas ERP están implementados en su empresa? ¿Qué módulos o funcionalidades utiliza más su empresa de este sistema?
3.¿Cuál es la estructura del equipo de tecnología y ciberseguridad en la empresa?
Propósito: Identificar la responsabilidad dentro de la empresa en términos de ciberseguridad en ERP.

SECCIÓN 2: CIBERSEGURIDAD EN EL ERP

4.¿Cuál considera que es la mayor amenaza cibernética para su empresa en relación con el uso del ERP?
5.¿Existen medidas de seguridad específicas que se implementen en su sistema ERP (como autenticación multifactor, encriptación de datos, etc.)?
6.¿Cuáles son las políticas y procedimientos de seguridad que sigue su empresa para proteger los datos dentro del ERP?
7.¿La empresa realiza auditorías periódicas de seguridad en los sistemas ERP? ¿Cómo son gestionadas y qué herramientas se usan para ello?
8.¿Cómo maneja la empresa el control de acceso dentro del ERP? ¿Se limitan los privilegios de los usuarios según su rol?

SECCIÓN 3: GESTIÓN DE RIESGOS Y CUMPLIMIENTO

9.¿Cómo gestiona su empresa los riesgos de ciberseguridad asociados a los sistemas ERP? ¿Existen evaluaciones de riesgos periódicas?
10. ¿Su empresa sigue alguna norma o estándar de ciberseguridad como ISO 27032 o NIST? ¿Cómo se aplican estos marcos dentro del ERP?
11. En cuanto a la gestión de incidentes de ciberseguridad, ¿cómo está organizada la respuesta ante un incidente dentro del ERP?
12. ¿Su empresa tiene un plan de continuidad del negocio (BCP) relacionado con los sistemas ERP? Si es así, ¿cómo se ha integrado la ciberseguridad dentro de este plan?

SECCIÓN 4: IMPLEMENTACIÓN DE MEDIDAS DE CIBERSEGURIDAD EN ERP

13.¿Cómo asegura su empresa la protección de los datos sensibles dentro del ERP (información financiera, datos de clientes, etc.)?

14.¿Qué tipo de formación o capacitación reciben los empleados sobre seguridad cibernética, especialmente en relación con el uso de ERP?

15.¿Su empresa realiza pruebas de penetración o simulacros de ciberseguridad sobre el ERP? ¿Cómo se gestionan los resultados de estas pruebas?

16.¿Existen procedimientos claros para la gestión de cambios en el sistema ERP (parches, actualizaciones, cambios en la configuración)?

SECCIÓN 5: DESAFÍOS Y OPORTUNIDADES

17.¿Cuáles han sido los mayores desafíos para implementar y mantener la ciberseguridad en su ERP?

18.En su opinión, ¿qué oportunidades existen para mejorar la ciberseguridad dentro del ERP de la empresa?

19.¿Qué tipo de apoyo considera que sería útil para mejorar las prácticas de ciberseguridad en los ERP?

SECCIÓN 6: CIERRE

20.¿Hay algún otro aspecto de la ciberseguridad que considera relevante en relación con el uso de sistemas ERP y que no hayamos abordado hasta ahora?

21.Finalmente, ¿cómo ve el futuro de la ciberseguridad en ERP dentro de su empresa y en la industria en general?

B. ANEXO 2: LISTA DE VERIFICACIÓN ISO 27032

LISTA DE VERIFICACIÓN ISO 27032

Objetivo:

La Lista de Verificación ISO 27032 es una herramienta para verificar que los controles de seguridad del sistema ERP se ajusten a los estándares internacionales definidos por la norma ISO/IEC 27032. El propósito de este anexo es proporcionar un marco para auditar las políticas, procedimientos y controles en el sistema ERP, garantizando que se sigan las mejores prácticas de seguridad cibernética.

Sección	Pregunta	Propósito	Comentario
Control de Acceso	¿Están implementadas políticas claras para el control de acceso?	Evaluar las políticas de control de acceso en el ERP.	
Control de Acceso	¿Se utiliza autenticación multifactor (MFA) en todos los accesos al sistema ERP?	Verificar el uso de MFA para mayor seguridad en los accesos.	
Control de Acceso	¿Los usuarios tienen acceso sólo a los módulos y datos necesarios según sus roles?	Asegurar la segregación de roles para evitar accesos innecesarios.	
Protección de Datos	¿Se cifran los datos sensibles tanto en reposo como en tránsito?	Comprobar la protección de datos críticos en el ERP.	
Protección de Datos	¿Se ha implementado el control de acceso basado en los datos (DAC) para proteger la información confidencial?	Verificar la implementación de controles de acceso sobre los datos.	
Gestión de Incidentes	¿Existe un procedimiento documentado para gestionar incidentes de ciberseguridad?	Asegurar que la empresa tenga un plan claro para incidentes.	
Gestión de Incidentes	¿El sistema ERP está vinculado a un sistema de monitoreo para la detección y respuesta a incidentes?	Confirmar la existencia de un sistema de monitoreo para responder a incidentes.	
Gestión de Incidentes	¿Se realiza una revisión periódica de incidentes pasados para mejorar la seguridad?	Evaluar la revisión de incidentes pasados para mejorar procedimientos.	
Auditorías	¿Se realizan auditorías de seguridad periódicas sobre el sistema ERP?	Confirmar la ejecución de auditorías de seguridad regulares.	

Sección	Pregunta	Propósito	Comentario
Auditorías	¿La empresa ha implementado pruebas de penetración para evaluar la vulnerabilidad del ERP?	Verificar que se hagan pruebas para identificar vulnerabilidades.	
Capacitación y Concientización	¿Se ofrece capacitación continua sobre seguridad a los empleados que interactúan con el ERP?	Confirmar si se capacita a los empleados sobre seguridad.	
Capacitación y Concientización	¿Existen programas de concientización sobre la ciberseguridad en la empresa?	Asegurar que exista un programa de concientización sobre ciberseguridad.	
Planificación y Continuidad del Negocio	¿Existe un plan de continuidad del negocio (BCP) que incluya la recuperación del sistema ERP en caso de incidente de seguridad?	Confirmar la existencia de un plan de continuidad del negocio relacionado con el ERP.	
Planificación y Continuidad del Negocio	¿Se realizan simulacros de recuperación ante desastres de los sistemas ERP?	Verificar que existan simulacros de recuperación ante incidentes.	