FACULTAD DE POSTGRADO

TESIS DE POSTGRADO

MÉTODOS DE CAPACITACIÓN QUE REDUCEN ERRORES HUMANOS EN PÉRDIDA DE INFORMACIÓN SENSIBLE EN GRUPO VESTA SPS, 2026.

SUSTENTADO POR:

BESSIE NOHEMI LOPEZ FERRUFINO

INGRIS CAROLINA MACHADO RUIZ

PREVIA INVESTIDURA AL TÍTULO DE

MÁSTER EN

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

TEGUCIGALPA, F.M, HONDURAS, C.A.

MAYO, 2026

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

MÉTODOS DE CAPACITACIÓN QUE REDUCEN ERRORES HUMANOS EN PÉRDIDA DE INFORMACIÓN SENSIBLE EN GRUPO VESTA SPS, 2026.

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

MÁSTER EN
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

ASESOR METODOLÓGICO

JUAN JACOBO PAREDES HELLER

ASESOR TEMÁTICO

JUAN JACOBO PAREDES HELLER

MIEMBROS DE LA TERNA:
KEVIN EDUARDO FÚNEZ FÚNEZ
ANTHONY STEVE BARAHONA ESPINOZA
ELVIN OSMAN BOBADILLA SALINAS

FACULTAD DE POSTGRADO

MÉTODOS DE CAPACITACIÓN QUE REDUCEN ERRORES HUMANOS EN PÉRDIDA DE INFORMACIÓN SENSIBLE EN GRUPO VESTA SPS, 2026.

BESSIE NOHEMÍ LÓPEZ FERRUFINO
INGRIS CAROLINA MACHADO RUIZ

Resumen

La presente investigación tuvo como finalidad analizar la relación existente entre los métodos de capacitación y la reducción de errores humanos vinculados a la pérdida de información sensible en Grupo Vesta, San Pedro Sula, durante el año 2026. La investigación se fundamenta en la relevancia del factor humano como uno de los principales riesgos en la seguridad de la información, destacando la necesidad de fortalecer la cultura organizacional de ciberseguridad mediante procesos formativos adecuados, continuos y alineados a las funciones del personal. La finalidad de la investigación consistió en la identificación de cuales contribuyen de manera significativa a disminuir conductas inseguras y errores humanos que pueden derivar en incidentes de pérdida de información sensible. En cuanto al proceso metodológico, el estudio adoptó un enfoque cuantitativo, con un diseño no experimental, de tipo descriptivo y correlacional. Se utilizaron encuestas estructuradas con escalas tipo Likert para la recolección de datos cuantitativos. Las variables fueron operacionalizadas mediante dimensiones e indicadores claramente definidos, lo que permitió analizar la relación entre los métodos de capacitación y la reducción del error humano.

Palabras claves: Capacitación en ciberseguridad, Cultura Organizacional de Seguridad, Error Humano, Información sensible, Seguridad de la Información.

GRADUATE SCHOOL

TRAINING METHODS THAT REDUCE HUMAN ERRORS IN THE LOSS OF SENSITIVE INFORMATION AT GRUPO VESTA SPS, 2026.

BESSIE NOHEMÍ LÓPEZ FERRUFINO
INGRIS CAROLINA MACHADO RUIZ

Abstract

The purpose of this research was to analyze the relationship between training methods and the reduction of human errors linked to the loss of sensitive information at Grupo Vesta, San Pedro Sula, during 2026. The research is based on the relevance of the human factor as one of the main risks to information security, highlighting the need to strengthen the organizational cybersecurity culture through appropriate, continuous training processes aligned with staff functions. The aim of the research was to identify which methods significantly contribute to reducing unsafe behaviors and human errors that can lead to incidents of sensitive information loss. Regarding the methodological process, the study adopted a quantitative-methods approach, with a non-experimental, descriptive, and correlational design. Structured surveys with Likert-type scales were used to collect quantitative data. The variables were operationalized through clearly defined dimensions and indicators, allowing for the analysis of the relationship between training methods and the reduction of human error.

Keywords: Cybersecurity training, Human error, Information security, Organizational security culture, Sensitive information.

DEDICATORIA

A Dios, por su amor y misericordia, por ser mi guía y mi sustento a lo largo de mi vida, por iluminar mi camino y darme esa fortaleza que me permitió finalizar con esta investigación. A mi esposo por su apoyo incondicional, y estar conmigo en cada paso de este camino, su impulso, amor y compañía me permitieron afrontar cada etapa con éxito. A mis padres y demás familiares por sus palabras de ánimo, por impulsarme a ser mejor y creer en mí e impulsarme a dar lo mejor de mí. A todos con todo mi amor, cariño y gratitud, les dedico este logro.

Bessie Nohemí López Ferrufino

Primeramente, a Dios por brindarme firmeza, sabiduría, perseverancia y los recursos necesarios para culminar satisfactoriamente esta etapa de mi formación profesional. A mi esposo por su comprensión y apoyo incondicional en esta etapa académica, siendo un pilar fundamental para enfrentar este desafío. A mi persona por esforzarse lo necesario, por confiar en ella, por el sacrificio y creer que todo es posible siempre y cuando se desee cumplir una meta. A mis seres queridos, padres, hermanos y amigos, que siempre tuvieron una palabra de ánimo y un apoyo incondicional que hicieron posible poder equilibrar todas las responsabilidades laborales, académicas y personales y me sostuvieron para no desistir ante los días difíciles. Porque esta meta no es solo mía, sino de todos los que aportaron ese granito de arena para obtener este logro tan anhelado.

Ingris Carolina Machado Ruiz

AGRADECIMIENTO

Estamos agradecidas con todas las personas que de una u otra forma contribuyeron a que este trabajo fuera posible. En primer lugar, a Dios, a nuestras familias, por ser nuestro apoyo en todo momento, por su amor y palabras que nos motivaron a seguir adelante y dar lo mejor de nosotras en cada etapa. Agradecemos a la Universidad Tecnológica Centroamericana por brindarnos los medios y recursos necesarios que fueron de mucha ayuda para finalizar con esta investigación, a cada uno de los docentes que fueron parte fundamental en nuestro proceso de formación académica. A nuestros compañeros de maestría, que durante todo este proceso fueron parte de nuestra formación al expresar sus experiencias que enriquecieron nuestros conocimientos, sus aportaciones hicieron que este viaje fuera más significativo. Finalmente agradecemos de forma especial a nuestro asesor de tesis, por su paciencia, guía y consejos que fueron esenciales para poder culminar con este proyecto, gracias por su confianza y por impulsar nuestras capacidades y habilidades que hicieron posible finalizar con éxito este proyecto de investigación.

ÍNDICE DE CONTENIDO

CAPÍTULO I: PLANTEAMIENTO DE LA INVESTIGACIÓN 1

1.1 INTRODUCCIÓN 1

1.2 ANTECEDENTES DEL PROBLEMA 3

1.3 DEFINICIÓN DEL PROBLEMA 7

1.3.3 PREGUNTAS DE INVESTIGACIÓN 9

1.4 OBJETIVOS DE LA INVESTIGACIÓN 9

1.5 JUSTIFICACIÓN 10

CAPÍTULO II: MARCO TEÓRICO 12

2.1 ANÁLISIS DE LA SITUACIÓN ACTUAL 12

2.2 MARCO CONCEPTUAL 19

2.3 TEORÍAS DE SUSTENTO 22

2.3.1 BASES TEÓRICAS 22

2.3.2 MARCO METODOLÓGICO 25

2.3 MARCO LEGAL 28

CAPÍTULO III: METODOLOGÍA 29

3.1 CONGRUENCIA METODOLÓGICA 29

3.1.1 MATRIZ METODOLÓGICA 29

3.1.2 ESQUEMA DE VARIABLES DE ESTUDIO 31

3.2 ENFOQUE Y MÉTODOS 36

3.3 DISEÑO DE LA INVESTIGACIÓN 38

3.3.1 POBLACIÓN 39

3.3.2 MUESTRA 39

3.3.3 TÉCNICAS DE MUESTREO 41

3.4 TÉCNICAS, INSTRUMENTOS Y PROCEDIMIENTOS APLICADOS 41
3.4.1 TÉCNICAS 41
3.4.2 Instrumentos de recolección de datos 42
3.4.3 PROCEDIMIENTOS 42
3.5 FUENTES DE INFORMACIÓN 43
3.5.1 FUENTES PRIMARIAS 43
3.5.2 ÉTICA DE LA INVESTIGACIÓN 43
3.5.3 LIMITACIONES 44
CAPÍTULO IV: RESULTADOS Y ANÁLISIS 45
4.1 INFORME DE PROCESO DE RECOLECCIÓN DE DATOS. 45
4.2 RESULTADOS Y ANÁLISIS DE LAS TÉCNICAS APLICADAS. 46
4.3 RESULTADOS Y ANÁLISIS DE LOS DATOS ENCONTRADOS. 83
CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES 87
5.1 CONCLUSIONES 87
5.2 RECOMENDACIONES 88
CAPÍTULO VI: APLICABILIDAD 90
6.1 NOMBRE DE LA PROPUESTA 90
6.2 JUSTIFICACIÓN DE LA PROPUESTA 90
6.3 ALCANCE DE LA PROPUESTA 91
6.4 DESCRIPCIÓN Y DESARROLLO A DETALLE DE LA PROPUESTA 91
6.5 MEDIDAS DE CONTROL 97
6.6 CRONOGRAMA DE IMPLEMENTACIÓN 100
6.7 PRESUPUESTO E IMPACTO DEL PRESUPUESTO 101
6.8 CONCORDANCIA DE LOS SEGMENTOS DE LA TESIS CON LA PROPUESTA 104
REFERENCIAS BIBLIOGRÁFICAS 107

ANEXOS 114

ANEXO I – CUESTIONARIO APLICADO AL PERSONAL DE GRUPO VESTA SPS ... 114

ÍNDICE DE TABLA

Tabla 1. Países de América Central en el Índice Global de Exposición a la Ciberseguridad. 17
Tabla 2. Matriz Metodológica 31
Tabla 3. Operacionalización de variables 34
Tabla 4.Distribución de áreas de colaboradores en Grupo Vesta 39
Tabla 5. Estadística de Fiabilidad 46
Tabla 6. Cantidad de colaboradores por área que manejan información sensible. 76
Tabla 7. Estadísticos de prueba 78
Tabla 8. Criterios de evaluación 89
Tabla 9. Frecuencia de prácticas inseguras 90
Tabla 10. Nivel de capacitaciones recibidas 90
Tabla 11. Escala de medición 91
Tabla 12. Nivel de criticidad 91
Tabla 13. Ejemplo tabla de identificación de áreas críticas 91
Tabla 14 . Medidas de control 94
Tabla 15. Cronograma de identificación de áreas críticas 96
Tabla 16. Cronograma de capacitación 97
Tabla 17. Presupuesto 98
Tabla 18. Concordancia de los segmentos de la tesis con la propuesta de investigación 100

ÍNDICE DE FIGURA

Figura 1.Tasa de participación global en la encuesta de Risk in Focus 2026. 6
Figura 2.Cinco principales riesgos. 7
Figura 3.Cinco principales riesgos por sector. 7
Figura 4.Nivel actual de inversión en formación en ciberseguridad. 14
Figura 5.Preocupaciones en seguridad cibernética. 17
Figura 6.Variable dependiente con sus respectivas dimensiones e indicadores del estudio. 32
Figura 7.Variable independiente con sus dimensiones e indicadores del estudio. 32
Figura 8.Enfoque y métodos de investigación. 38
Figura 9.Género 47
Figura 10.Edad 47
Figura 11. ¿En qué medida considera que el contenido de las capacitaciones en seguridad de la información es claro y fácil de comprender? 48
Figura 12.¿El contenido de las capacitaciones en seguridad de la información es relevante para mis actividades diarias dentro de la organización? 49
Figura 13.¿Qué tan relevantes considera los temas abordados durante las capacitaciones? 50
Figura 14.¿Las sesiones de capacitación incluyeron explicaciones sobre errores humanos comunes y cómo evitarlos? 50
Figura 15. ¿Qué modalidad predominó en las capacitaciones que recibió? 51
Figura 16. ¿Para cada una de las siguientes modalidades de capacitación, indique su nivel de acuerdo según el grado en que esta facilitó su aprendizaje? 52
Figura 17.¿La duración de las sesiones fue adecuada para comprender la información presentada? 53
Figura 18. ¿Cuántas sesiones o módulos de capacitación en seguridad de la información recibió en los últimos 12 meses? 53
Figura 19. ¿Con qué frecuencia recibe recordatorios o materiales de refuerzo sobre buenas prácticas de seguridad? 54
Figura 21. ¿En las capacitaciones recibidas se le aplicó una evaluación o prueba después de la capacitación? (p. ej. quiz, examen, post-test) 56

Figura 22. ¿Las capacitaciones incluyeron ejemplos o casos prácticos aplicables a su trabajo? 57
Figura 23. ¿Qué tan satisfecho(a) está con la calidad general de las capacitaciones recibidas? 58
Figura 24. ¿Las capacitaciones modificaron mis hábitos o rutinas al manejar información sensible? 58
Figura 25. ¿Con qué frecuencia deja visible información sensible en su computadora o documentos impresos al retirarse de su puesto de trabajo? 59
Figura 26. ¿Con qué frecuencia guarda, descarga o comparte información sensible o plataformas no autorizadas? 60
Figura 27. ¿Con qué frecuencia revisa cuidadosamente enlaces o archivos antes de hacer clic para evitar caer en intentos de phishing? 61
Figura 28. ¿Con qué frecuencia utiliza contraseñas seguras (complejas, únicas, y no compartidas) para acceder a sistemas o información sensible? 62
Figura 29. ¿En mi trabajo diario, sigo las políticas y procedimientos de seguridad al manejar información sensible? 63
Figura 30. ¿Antes de enviar información sensible, verificar cuidadosamente que el destinatario sea el correcto? 64
Figura 31. En los últimos 12 meses, ¿con qué frecuencia ha ocurrido que, por error suyo, se perdió, borró o quedó inaccesible información sensible? 64
Figura 32 . En los últimos 12 meses, ¿con qué frecuencia ha ocurrido que, por un error suyo, se envió o expuso información sensible a personas no autorizadas? 65
Figura 33. ¿Considero que un error mío en el manejo de información sensible podría generar consecuencias graves para la organización? 66
Figura 34¿Tengo claro que la información que manejo en mi trabajo se considera sensible? 66
Figura 35¿Me considero capaz de identificar situaciones en las que podría cometer un error que exponga información sensible? 67
Figura 36. ¿Cuándo tengo dudas sobre cómo manejar información sensible, sé a quién consultar o dónde buscar la información correcta para evitar errores? 68
Figura 37¿Después de las capacitaciones, me siento más seguro(a) al manejar información sensible? 68
Figura 38.Métodos de capacitación por área 69
Figura 39.Intensidad de capacitación por área 70

Figura 40. Evaluar qué método genera mayor cambio conductual. 71
Figura 41. Relación entre método y reducción de incidentes. 72
Figura 42. Frecuencia de verificación de destinatario antes de enviar información relacionada con la frecuencia de error humano 73
Figura 43. Identificar si el uso de plataformas no autorizadas está vinculado a pérdida de información. 74
Figura 44.Determinar si el descuido físico está asociado a incidentes reales. 75

CAPÍTULO I: PLANTEAMIENTO DE LA INVESTIGACIÓN

El presente capítulo introduce el núcleo del problema en que se basa esta investigación; la relación entre los métodos de capacitación del personal y la reducción del error humano vinculado a la pérdida de información sensible en Grupo Vesta de San Pedro Sula. En un entorno donde la información es un activo crítico, la preparación del personal se vuelve esencial para fortalecer la seguridad organizacional. Este planteamiento determina el problema central del estudio, y justifica su relevancia para la gestión empresarial en el año 2026. Asimismo, establece las interrogantes, objetivos y alcances que orientarán el desarrollo de la investigación.

1.1 INTRODUCCIÓN

La seguridad de la información hoy en día ha surgido como una necesidad derivada de los cambios que se han presentado en diferentes industrias y en la sociedad en general a través de la digitalización. La creciente dependencia al uso de tecnología ha incrementado el nivel de exposición de las organizaciones a diversas amenazas. Estas amenazas pueden definirse como situaciones que pueden ocasionar un incidente, provocando daños materiales o pérdidas inmateriales de sus activos de información. En este escenario la protección de datos se ha convertido en un factor clave para asegurar la confianza de los clientes.

No obstante, los grandes volúmenes de información que manejan las empresas han complicado la protección de la información confidencial frente a las múltiples amenazas existentes, tal como el error humano se posiciona como uno de los factores más críticos dentro de la seguridad de la información, ya que muchas de las brechas y pérdida de datos se originan por acciones incorrectas, omisiones o decisiones inadecuadas por parte del personal. “El problema del error humano en la ciberseguridad se refiere a una variedad de errores cometidos por los usuarios en lugar de la falla de la computadora, tecnología o máquina que se está utilizando”

Teniendo en cuenta que los datos son uno de los activos más valiosos de las organizaciones, su manejo y cuidado deben ser conocidos por cada uno de los niveles y áreas sin importar el puesto de trabajo. Es requerido que las personas tengan una comprensión profunda que genere cambios en la actitud y comportamiento sobre este tema, ya que, aunque se realicen grandes inversiones en implementar controles para proteger la información, el factor humano continúa siendo uno de los principales factores de vulnerabilidad, según un artículo de IBM, “el costo anual promedio de las violaciones de datos causadas por error humano es de $3,36 millones” (Cost of a Data Breach

Report, 2019).La respuesta a las amenazas cibernéticas no será suficiente si se centra solo en sancionar conductas negligentes o dolosas de las personas empleadas que no cumplan la política de ciberseguridad de la empresa. Según Cadenas (2025). Más importante que la actitud reactiva ante las amenazas del ciberespacio es la actitud proactiva centrada en la prevención, pues el mejor escenario es que el ataque no prospere.

En este contexto, Grupo Vesta, San Pedro Sula, Honduras, como organización con responsabilidades en la gestión de información empresarial y de clientes, enfrenta el reto de minimizar la exposición de sus datos sensibles derivados del error humano. No basta con disponer de equipos de seguridad robustos y sistemas con controles implementados; es imprescindible que el recurso humano conozca y practique conductas seguras en sus actividades operativas.

Además, la organización busca fomentar una cultura de seguridad y protección en el comercio internacional, promoviendo prácticas responsables que fortalezcan la confianza y la integridad de sus operaciones. La eficacia de estas conductas depende principalmente de los métodos de capacitación implementados, su diseño, frecuencia y evaluación por lo que evaluar la relación que existe entre la formación y la reducción de errores humanos resulta clave para la resiliencia de la organización.

Es por ello, que en la presente investigación se delimita a analizar en qué medida los métodos de capacitación del personal influyen en la reducción del error humano vinculado a la pérdida de información sensible en Grupo Vesta, San Pedro Sula, Honduras durante el año 2026. Este enfoque permite realizar un análisis riguroso mediante que permitan verificar cuales son los tipos de capacitación que han dado mejores resultados, es decir, aquellos métodos que disminuyen el error humano en relación con la pérdida de información sensible.

El problema central que aborda este trabajo es la posibilidad de que, sin un enfoque formativo adecuado, el personal de la organización continúe siendo la principal causa de incidentes que derivan en pérdida o exposición de información sensible debido a errores humanos. El propósito es evaluar los métodos de capacitación vigentes. Con ello, se aspira no solo a aportar recomendaciones operativas a Grupo Vesta, San Pedro Sula, Honduras, sino también a generar conocimiento replicable para organizaciones similares en el país.

Por lo que la relevancia científica se manifiesta en la contribución al entendimiento de la interacción entre capacitación y comportamiento seguro en un contexto empresarial poco estudiado. Profesionalmente, los resultados orientarán el diseño de programas de formación más

eficaces; socialmente, fortalecerán la confianza de clientes y socios al reducir riesgos de exposición de datos; metodológicamente, el estudio puede ofrecer un marco evaluativo (indicadores y métricas) aplicable a otras empresas de la región.

En términos de viabilidad, la investigación se apoya en fuentes secundarias sólidas y en la posibilidad de acceder a datos internos de formación e incidentes en la organización. Con esta investigación se busca transformar una vulnerabilidad organizativa en una oportunidad de mejora continua, contribuyendo al resguardo integral de la información y al fortalecimiento de la cultura de ciberseguridad en la organización.

1.2 ANTECEDENTES DEL PROBLEMA

En el apartado siguiente se detallan los antecedentes a nivel mundial y nacional relacionado con la temática de investigación:

En primer lugar, un artículo cuyo objetivo fue el investigar las violaciones atribuidas a errores humanos y comparar las políticas de ciberseguridad, los programas de educación, formación y concienciación en tres escuelas diferentes del Estado de Nueva York, este trabajo demuestra que las políticas de ciberseguridad formuladas y aplicadas, junto con educación, capacitación y concienciación de seguridad dirigidas, son fundamentales para disminuir los errores de los usuarios, reduciendo así la probabilidad de un ciberataque (AMOROSA & YANKSON, 2023).

Amorosa & Yankson (2023), concluyen que el factor humano se está volviendo cada vez más importante para la ciberdefensa de una organización porque el error humano es una de las principales razones de las brechas de seguridad. Para investigaciones futuras en ciberseguridad, detallan que debe haber un cambio del aspecto técnico al aspecto humano para prevenir la ocurrencia frecuente de ciberataques exitosos (pág. 1). Este estudio evidencia que el error humano no debe abordarse como un evento aislado, sino como una consecuencia sino de políticas claras y capacitaciones efectivas lo que implica que la ocurrencia de errores no es únicamente responsabilidad del colaborador.

En segundo lugar, Prümmer et al., (2024) realiza una revisión ordenada y rigurosa de la literatura basada en los métodos de capacitación en ciberseguridad dirigidos al comportamiento de

usuarios finales en entornos organizacionales. El estudio llamado A systematic review of current cybersecurity training methods, tiene su enfoque en sobre como los métodos de capacitación o entrenamiento influyen en las conductas relacionadas con la seguridad de la información, en los temas centrales abordados fueron phishing, gestión de contraseñas, shadow security, y seguridad general de los usuarios.

Este estudio concluye que los programas multifacéticos y con refuerzos periódicos muestran mejores resultados en la reducción de errores humanos, los resultados apoyan a diseñar programas combinados, donde el método más común es el entrenamiento basado en juegos, Prümmer et al., (2024) destaca que aunque los resultados son positivos, hay variabilidad en cómo se define y miden los resultados, lo que dificulta la comparación entre estudios, advierte que hay poca investigación que mida los cambios en la conducta de los usuarios, como ser la reducción de incidentes reales de pérdida de datos, no es un estudio generalizado porque muchas muestras son pequeñas a menudo estudiantes en lugar de empleados reales de una organización.

Algunos estudios como, Enhancing employees information security awareness in private and public organizations: A systematic literature review, de Khando et al.,(2021) logra identificar los distintos métodos de capacitación utilizados en organizaciones para robustecer la concienciación de seguridad de la información de los empleados en organizaciones tanto del sector público como privado, además, en esta revisión sistemática, se identificaron múltiples factores que afectan la conciencia de seguridad, incluyendo factores individuales, organizativos, tecnológicos y contextuales.

> Otro estudio examinó los errores humanos influenciados por acciones, actitudes y comportamientos que afectan a la seguridad general de la información. Los resultados revelaron que los errores humanos repetidos comprometen los principios de seguridad de la información y convierten a los empleados en el eslabón más débil. El estudio explicó los riesgos que suponen los empleados debido a la ignorancia o la mala toma de decisiones, errores técnicos y errores basados en habilidades y políticas (Ncubukezi, 2022, p. 1).

Por otra parte, la OECD (2023), detalla que, en Latinoamérica, la seguridad de la información ante los ciberataques se ha posicionado en un tema de creciente preocupación, en este escenario la capacitación, concienciación y formación del personal constituyen instrumentos

claves para mitigar los riesgos por errores humanos. Para ello el estudio llamado Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciber amenazas a la seguridad nacional y política exterior, Aguilar Antonio (2021), determina que la región latinoamericana presenta rezagos importantes en materia de política nacional de ciberseguridad y construcción de capacidades para enfrentar amenazas que afectan la seguridad nacional. Dado la naturaleza del estudio no presenta datos primarios provenientes de encuestas o entrevistas directas con actores de la región, por lo tanto, hay una brecha de conocimiento en la investigación empírica que involucre directamente países latinoamericanos y sus actores relevantes, así como la escasa diferenciación detallada entre países de la región. Es decir, un análisis que englobe variaciones, mejores prácticas y condiciones contextuales, viendo además la necesidad de un mayor enfoque en la dimensión humana del riesgo cibernético en la región.

Así mismo, se detalla un estudio académico titulado, La brecha existente en la ciberseguridad en Honduras, donde Centeno (2017), examina la situación de la ciberseguridad específicamente en el país, con el objetivo de identificar las brechas estructurales, normativas, institucionales y tecnológicas que impiden al país afrontar de forma adecuada el cibercrimen y las amenazas a la seguridad digital. Se analiza la carencia de políticas nacionales robustas, la falta de equipo especializado en respuesta a incidentes y la limitada capacidad gubernamental, empresarial y de usuarios individuales para responder de forma proactiva a las amenazas.

Centeno (2017), detalla en esta revisión bibliográfica y análisis documental e identifica algunas brechas de conocimiento como desarrollar estudios que cuantifiquen con precisión la magnitud de incidentes de ciberseguridad en Honduras. Además de existir poca investigación sobre la capacidad organizacional interna de las empresas hondureñas para implementar medidas de seguridad, formación personal y cultura de seguridad digital, existe falta de análisis sobre cómo evoluciona la ciberseguridad en Honduras a lo largo del tiempo, y la insuficiente investigación sobre la implementación de buenas prácticas internacionales adoptadas al contexto hondureño. En este sentido, Centeno (2017), proporciona un contexto nacional sobre el estado de la ciberseguridad en el país, identificando que una de las debilidades es justamente la limitada capacidad institucional y organizacional, lo que pone en evidencia que los métodos de capacitación pueden jugar un rol importante para elevar esta capacidad. Aunque no se focaliza exclusivamente en errores humanos y capacitación para reducirlos, el trabajo señala que la debilidad de la

organización incluyendo la formación del personal, constituyen una barrera para la seguridad digital en el país.

Para sustentar los antecedentes anteriormente mencionados se muestran las gráficas del Instituto de auditores Interno con el proyecto Risk in Focus, donde presenta un resumen del informe de Riesgo en América Latina 2026, este proyecto de investigación anual se genera a través de encuestas, mesas redondas, entrevistas a líderes de auditoría interna e identifica los cinco principales riesgos que enfrentan las organizaciones a nivel global y regional (The IIA, 2026).

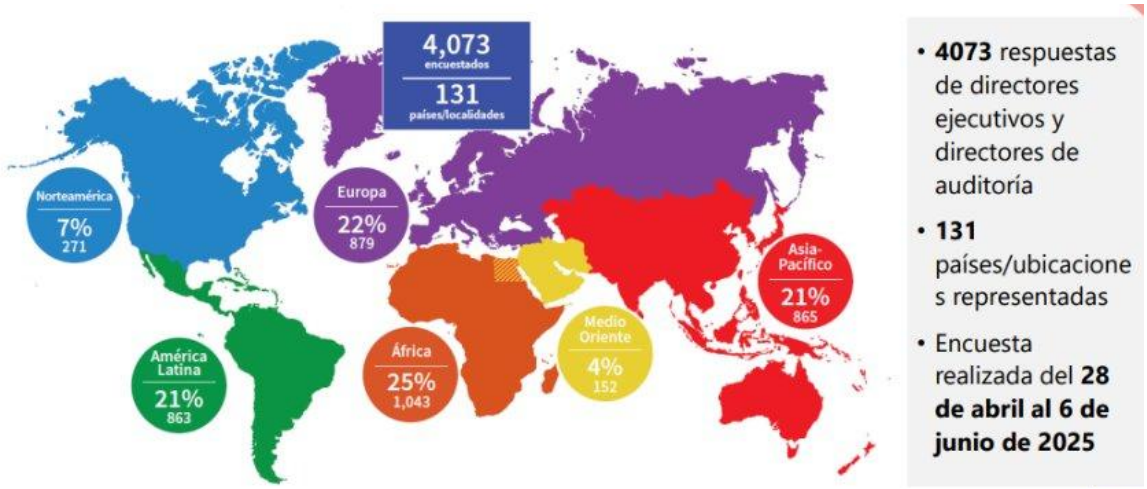


Figura 1.Tasa de participación global en la encuesta de Risk in Focus 2026.
Fuente: (The IIA, 2026).

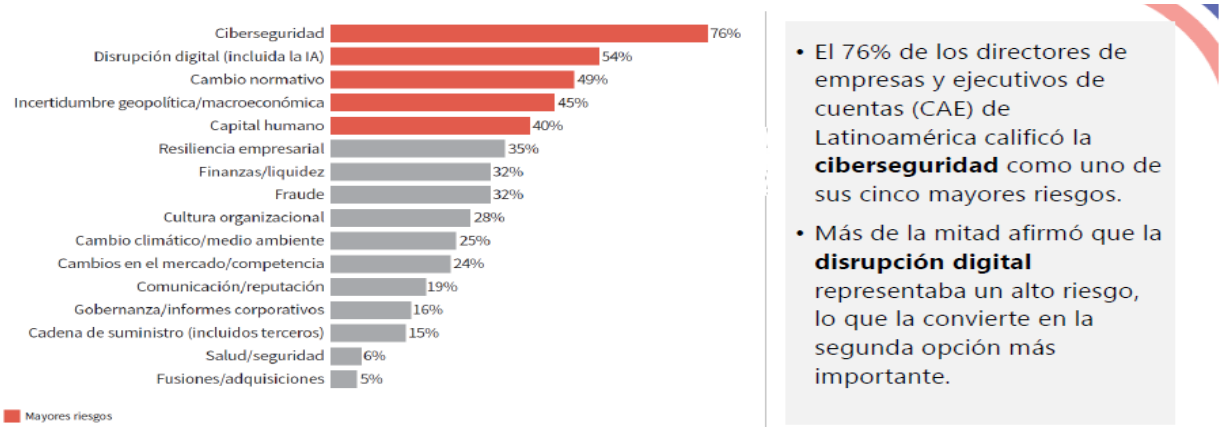
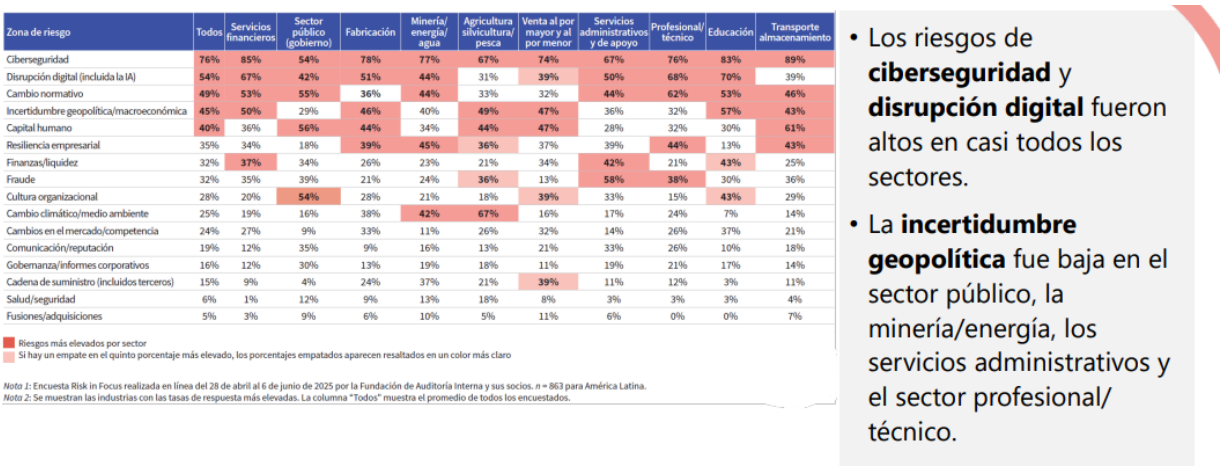


Figura 2.Cinco principales riesgos.
Fuente:(The IIA, 2026).



Zona de riesgo	Todos	Servicios financieros	Sector público (gobierno)	Fabricación	Minería/ energía/ agua	Agricultura silvicultura/ pesca	Venta al por mayor y al por menor	Servicios administrativos y de apoyo	Profesional/ técnico	Educación	Transporte almacenamiento
Ciberseguridad	76%	85%	54%	78%	77%	67%	74%	67%	76%	83%	89%
Disrupción digital (incluida la IA)	54%	67%	42%	51%	44%	31%	39%	50%	68%	70%	39%
Cambio normativo	49%	53%	55%	36%	44%	33%	32%	44%	62%	53%	46%
Incertidumbre geopolítica/macroeconómica	45%	50%	29%	46%	40%	49%	47%	36%	32%	57%	43%
Capital humano	40%	36%	56%	44%	34%	44%	47%	28%	32%	30%	61%
Resiliencia empresarial	35%	34%	18%	39%	45%	36%	37%	39%	44%	13%	43%
Finanzas/liquidez	32%	37%	34%	26%	23%	21%	34%	42%	21%	43%	25%
Fraude	32%	35%	39%	21%	24%	36%	13%	58%	38%	30%	36%
Cultura organizacional	28%	20%	54%	28%	21%	18%	39%	33%	15%	43%	29%
Cambio climático/medio ambiente	25%	19%	16%	38%	42%	67%	16%	17%	24%	7%	14%
Cambios en el mercado/competencia	24%	27%	9%	33%	11%	26%	32%	14%	26%	37%	21%
Comunicación/reputación	19%	12%	35%	9%	16%	13%	21%	33%	26%	10%	18%
Gobernanza/informes corporativos	16%	12%	30%	13%	19%	18%	11%	19%	21%	17%	14%
Cadena de suministro (incluidos terceros)	15%	9%	4%	24%	37%	21%	39%	11%	12%	3%	11%
Salud/seguridad	6%	1%	12%	9%	13%	18%	8%	3%	3%	3%	4%
Fusiones/adquisiciones	5%	3%	9%	6%	10%	5%	11%	6%	0%	0%	7%

Riesgos más elevados por sector
Si hay un empate en el quinto porcentaje más elevado, los porcentajes empatados aparecen resaltados en un color más claro

Nota 1: Encuesta Risk in Focus realizada en línea del 28 de abril al 6 de junio de 2025 por la Fundación de Auditoría Interna y sus socios. *n* = 863 para América Latina.
Nota 2: Se muestran las industrias con las tasas de respuesta más elevadas. La columna "Todos" muestra el promedio de todos los encuestados.

- Los riesgos de **ciberseguridad** y **disrupción digital** fueron altos en casi todos los sectores.
- La **incertidumbre geopolítica** fue baja en el sector público, la minería/energía, los servicios administrativos y el sector profesional/ técnico.

Figura 3.Cinco principales riesgos por sector.
Fuente:(The IIA, 2026).

Considerando los datos anteriores, podemos observar que existe una brecha, en la revisión de la literatura, con respecto a los métodos de capacitación que reducen errores humanos en pérdida de información sensible, específicamente en organizaciones del sector de logística como es el caso de Grupo Vesta SPS, por ende, es necesario realizar la investigación y verificar cual es el método adecuado para esta empresa.

1.3 DEFINICIÓN DEL PROBLEMA

En un entorno en el que las tecnologías son fundamentales para el funcionamiento de una organización, resulta cada vez más crítico gestionar no solo aspectos técnicos de la seguridad informática, sino también la dimensión humana. En el caso de Grupo Vesta en San Pedro Sula, es una organización que administra información sensible como gestión, operación y transformación de cadenas de suministro regionales e internacionales, la pérdida o exposición de datos sensibles puede generar consecuencias operativas, legales y de reputación de gran envergadura. La evidencia científica dice que, en muchos casos los errores humanos han permitido a los hackers acceder a datos confidenciales de las organizaciones, según el informe de Inteligencia de Ciberseguridad de IBM, el 95% de las brechas de ciberseguridad se deben a errores humanos (Alqahtani et al., 2023).

1.3.1 ENUNCIADO DEL PROBLEMA

En un contexto nacional, Grupo Vesta, SPS enfrenta el desafío de garantizar una gestión segura de sus sistemas de información, esto debido a las crecientes amenazas digitales y posibles

fallos en la capacitación del personal. Si bien se cuenta con infraestructura de seguridad, los incidentes que se atribuyen a descuidos, o prácticas inseguras del personal tienen el potencial de derivar, pérdida, divulgación o manipulación de información crítica. La falta de métodos de capacitación adecuados, que integren conocimiento tanto técnicos, como consentimiento de riesgos, puede comprometer la efectividad de los mecanismos de defensa. Por ello es de suma relevancia el estudio de este tema, ya que pocas empresas consideran la capacitación y concientización como un control dentro de sus organizaciones, se subestima que el ser humano es el eslabón más débil y puede provocar incidentes de seguridad que tengan como resultado la pérdida de información.

En la actualidad este tema está tomando auge, ya que los ciber atacantes suelen aprovechar el poco conocimiento de las personas para acceder a la información, mediante la ingeniería social o el phishing. A pesar de esta realidad, existe poca documentación sobre estudios científicos donde se realice una investigación de cuáles son los métodos de capacitación para el personal en temas de seguridad que resulten más adecuados o efectivos para reducir errores humanos que provoquen la exposición de datos confidenciales. En muchos casos las empresas implementan capacitaciones generalizadas sin evaluar verdaderamente si estos están teniendo los resultados esperados en la conducta de su personal. Por lo tanto, esta brecha identificada en la literatura y la falta de concientización resalta una necesidad de desarrollar estudios que sirvan como referencia a poder identificar la percepción de sus colaboradores sobre si en realidad las capacitaciones recibidas han sido comprendidas y por ende su comportamiento y la forma en la que se maneja la información.

1.3.2 FORMULACIÓN DEL PROBLEMA

Analizando el problema desde la perspectiva de la maestría en Gestión de Tecnologías de Información, resulta muy importante evaluar la relación entre los método de capacitación del personal en la reducción del error humano asociado a la pérdida de información sensible dentro de la organización, este análisis permite comprender la relación entre la formación en seguridad y el comportamiento del personal considerando su impacto en la protección de la información, en consecuencia surge la siguiente interrogante ¿En qué medida los métodos de capacitación del personal influyen en la reducción del error humano vinculado a la pérdida de información sensible en la empresa Grupo Vesta en San Pedro Sula en 2026?.

1.3.3 PREGUNTAS DE INVESTIGACIÓN

En este apartado se formulan las interrogantes que orientan el rumbo de la investigación, permitiendo precisar el vínculo entre la capacitación del personal y la reducción del error humano. Las preguntas planteadas sirven como guía para analizar y comprender el fenómeno dentro del contexto organizacional de Grupo Vesta, SPS en 2026.

La siguiente pregunta principal orienta el propósito central del estudio, al buscar comprender el impacto que tienen los procesos formativos en la prevención de fallos vinculados a la seguridad de la información dentro de la organización, la cual se planteó de la siguiente manera: ¿En qué medida los métodos de capacitación del personal influyen en la reducción del error humano relacionado con la pérdida de información sensible en Grupo Vesta de San Pedro Sula en el año 2026?

Las preguntas secundarias planteadas en este apartado pretenden analizar de manera detallada el estudio y dar respuesta al problema de estudio siendo las siguientes: ¿Qué métodos de capacitación en ciberseguridad se implementan y cuántos colaboradores por área manejan información sensible en Grupo Vesta, SPS 2026? y ¿Cuáles son los errores humanos más relevantes que generan pérdida de información sensible en Grupo Vesta, San Pedro Sula, en el 2026?

1.4 OBJETIVOS DE LA INVESTIGACIÓN

A partir del planteamiento del problema es de suma importancia formular los objetivos, ya que estos orientan de manera clara y ordenada el propósito del estudio, estos permiten definir que se pretende investigar. Por ende, su formulación adecuada asegura que la investigación se realice de forma estructurada y acorde a los resultados esperados, asegurando que cada etapa se desarrolle de forma que contribuya a dar una resolución al problema de investigación planteado. Por tanto, en la presente investigación se establecen una serie de objetivos que alinean con el propósito del estudio.

El estudio presente establece una serie de propósitos orientado a comprender y analizar el fenómeno investigado, se presenta seguidamente, el objetivo general que guía la ejecución del estudio de investigación el cual es; Evaluar métodos de capacitación que influyen en la reducción

del error humano relacionado con la pérdida de información sensible en Grupo Vesta San Pedro Sula, 2026.

A fin de orientar el rumbo de la presente investigación se establecen los objetivos que estructuran el proceso de análisis.

Uno de los objetivos es, enumerar métodos de capacitación en ciberseguridad implementados y los colaboradores por área que manejan información sensible en Grupo Vesta 2026.

Así mismo, identificar los errores humanos más relevantes que generan pérdida de información sensible en Grupo Vesta, San Pedro Sula, 2026.

1.5 JUSTIFICACIÓN

Uno de los pilares fundamentales de cualquier estrategia de ciberseguridad de cualquier empresa es la educación y la concientización empresarial. Los programas de concientización deben ser prácticos y adaptarse a las diferentes funciones dentro de cualquier rubro donde quieran implementarse. Es imperativo que las organizaciones apliquen controles para mitigar no solo a la protección de los sistemas, si no a la reducción a la reducción de los errores humanos que pueden comprometer la seguridad de la información, ya que la información no solo se encuentra a nivel de sistemas (software), sino que al ser gestionada por los colaboradores los hace una presa fácil para los ciber atacantes.

Por ende, la implementación de capacitación o concientización sobre seguridad es una herramienta muy útil para las organizaciones que desean proteger sus datos, reducir los incidentes y cerciorarse que sus colaboradores comprendan cómo manejar de forma responsable los datos de sus clientes. Es por ello que, la presente investigación resulta fundamental para Grupo Vesta SPS ya que mediante la identificación de los errores humanos más comunes podrán verificar cuáles son los métodos de capacitación adecuados y cómo estos pueden influir en la reducción de errores humanos que minimicen el riesgo de la pérdida de información sensible, esto puede aportar significativamente a fortalecer la cultura de seguridad interna.

Cuantitativamente la investigación aportará a que Grupo Vesta SPS pueda decidir mediante una base objetiva que métodos de capacitación resultan más eficaces, con qué frecuencia deben aplicarse y cómo estos influyen en la mejora de la seguridad de la información y cultura interna.

En consecuencia, este estudio proporcionará datos que ayudarán a la optimización de recursos destinados a la formación, fortaleciendo los mecanismos de prevención y gestión del riesgo informático en la empresa.

La protección de la información sensible de clientes, proveedores y de la propia empresa fortalece la confianza institucional, mejora la reputación empresarial, y reduce costes asociados a brechas de datos, pérdidas económicas e interrupciones operativas ocasionados por errores humanos. Además, en el entorno del comercio internacional en que opera Grupo Vesta, SPS Honduras, fomentar una cultura de seguridad y protección de datos ofrece una ventaja competitiva e incrementa la resiliencia frente a amenazas globales. Marreos et al., (2023) asegura que las personas que trabajan en las organizaciones deben ser conscientes de la ingeniería social es decir estar alerta ante posibles intentos de engaño o manipulación por parte de personas externas que intentan obtener información confidencial.

Por ende, la viabilidad de realizar el presente estudio en Grupo Vesta SPS durante el año 2026 es alta debido a el apoyo de la empresa en el proceso de investigación. Así mismo resulta factible en términos de recursos y tiempo. También permite brindar una referencia a profesionales de seguridad de la información para diseñar, implementar y evaluar programas adaptados a las necesidades y realidad de las empresas permitiendo la mejora continua en la gestión de seguridad de la información al identificar los errores más comunes a los que están expuestos. Debido a la evidencia que proporcionará la presente investigación se tendrá una base o guía en la toma de decisiones y fortalecimiento de la cultura de seguridad.

Como referencia científica, considerando que el tema de concientización y error humano es un tema que aún no ha sido ampliamente abordado desde la investigación académica y cuya literatura disponible en el país es limitada. La mayoría de las referencias existentes provienen de estudios internacionales que no siempre se ajustan a la realidad técnica y cultural de las empresas hondureñas. Por ello, el presente estudio busca contribuir a llenar ese vacío teórico y empírico**,** proporcionando una base de referencia que oriente futuras investigaciones y estrategias adaptadas al contexto empresarial de Honduras.

CAPÍTULO II: MARCO TEÓRICO

La construcción del marco teórico permite situar el estudio dentro de un contexto conceptual y empírico previamente establecido. A través de la revisión y el análisis de literatura especializada, se identifican los principales enfoques, modelos y hallazgos que han abordado la problemática en cuestión, lo cual facilita comprender el estado actual del conocimiento y reconocer las áreas donde persisten vacíos o controversias.

De esta manera Reidl-Martínez (2012) señala que:

> El plan inicial del desarrollo de un marco teórico que sustente la investigación a realizar incluye no sólo los supuestos teóricos de los que parte el investigador, sino también conforma la manera en la que el investigador recoge sus datos, lo que a su vez determina o establece los límites de las clases de análisis que pueden emplearse.

2.1 ANÁLISIS DE LA SITUACIÓN ACTUAL

El resguardo de la información y la protección se han vuelto una prioridad para las organizaciones, con los avances de la tecnología y la dependencia que las empresas tienen a ella, esto ha aumentado la exposición de la información a ataques de ciberseguridad, que también se ha convertido en una de las prioridades debido al aumento de los ciberataques. Las diferentes técnicas utilizadas por los ciberdelincuentes para obtener información cada día son más sofisticadas, estas tácticas abarcan desde el uso de malware hasta ataques de "ingeniería social que es una técnica que utiliza el cibercriminal, para aprovechar la falta de conocimiento sobre seguridad de la información por parte de los usuarios" (Fueres et al., 2024,p.1).

Entre las técnicas de ingeniería social más utilizada se encuentra el phishing, donde por medio de un correo electrónico se hace pasar por empresas de confianza para obtener la información del usuario la cual puede ser contraseñas, información de tarjetas de crédito o información financiera de la empresa o víctima. Todas estas técnicas van dirigidas a engañar a las personas ya sea por un correo u otro medio con el fin de robar su información, es por ello por lo que se considera al factor humano como uno de los eslabones más débiles en la seguridad de la información.

En este contexto, muchos estudios e investigaciones se centran en temas relacionados a las políticas de seguridad y tecnología, pocos se centran en el factor humano, no se puede negar que

este tema es de relevancia y que puede representar un riesgo para las empresas si no se implementan controles adecuados.

En un contexto global, donde las organizaciones enfrentan un mundo que se caracteriza por la innovación, la seguridad de la información y ciberseguridad se han consolidado como un factor clave cuyo propósito es salvaguardar la integridad, disponibilidad y confidencialidad de la información. La ciberseguridad se conceptualiza como "conjunto de tecnologías, procesos, prácticas y medidas de respuesta y mitigación diseñadas para proteger redes, computadoras, programas y datos frente a ataques, daños o accesos no autorizados, con el fin de garantizar la confidencialidad, integridad y disponibilidad" (Canadian Centre for Cybersecurity, 2020, citado en (Hoong & Rezania, 2024).

Este concepto como tal no solo implica la implementación de medidas tecnológicas que requieran de un software y hardware, también requiere de medidas que involucren la concientización del personal.

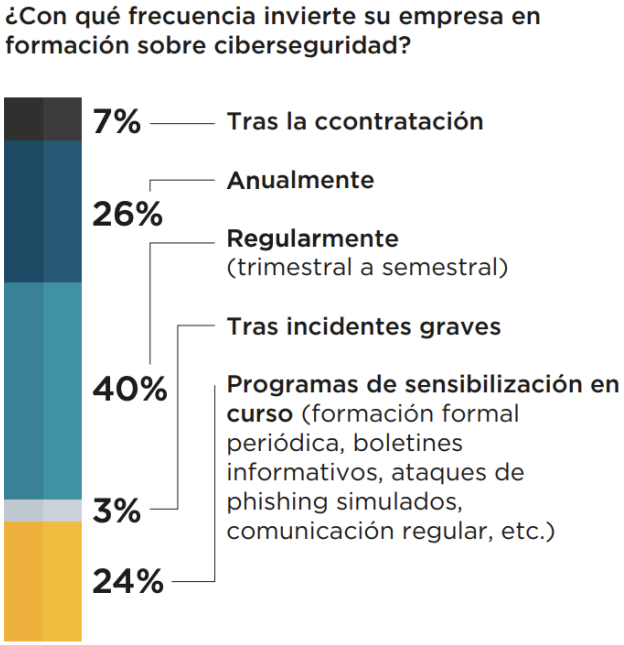


Figura 4.Nivel actual de inversión en formación en ciberseguridad.
Fuente: (HBL Reporte de Ciberseguridad, 2024).

Como lo indica la figura 4, destinar recursos a programas de sensibilización y capacitación de los empleados en temas de seguridad resulta crucial para las organizaciones. Muchas empresas están apostando a brindar conocimiento y reducir las vulnerabilidades que se puedan ocasionar por

errores humanos, esto debido a que el factor humano es una de las preocupaciones y el tener un personal capacitado en ciberseguridad mejora su gestión frente a los ciberataques.

La concientización, capacitación y culturización en temas relacionados a seguridad es de suma importancia, ya que tiene como objetivo proporcionar a los colaboradores habilidades y conocimientos requeridos para proteger la información sensible o confidencial de su organización frente a ataques tales como phishing. Por ello es relevante conocer de qué tratan estas técnicas para así adoptar los programas de concientización a los métodos que los atacantes utilizan.

Álvarez et al., (2024) describe alguna de las técnicas de phishing más habituales como ser:

Comunicación engañosa: estos saben cómo manipular a sus víctimas con mensajes engañosos.

Sensación de necesidad: los usuarios se convierten en víctimas de phishing porque al recibir un mensaje con algún enlace de interés, sienten la necesidad de ver lo que el enlace contiene, por ejemplo, si se recibe un enlace para armar un curriculum vitae y este es engañoso se puede estar entregando información personal a un cibercriminal.

Falsa confianza: los cibercriminales engañan a su víctima creando un ambiente de falsa confianza para que estos les den información personal, así como incluso una tarjeta de crédito, por ejemplo.

Manipulación emocional: los cibercriminales usan técnicas de manipulación emocional para convencer a su objetivo. (pág. 3)

Considerando este escenario muchas de las brechas de ciberseguridad se originan por errores humanos debido a ataques de ingeniería social. Por tanto, las organizaciones deben prestar mucha atención en crear conciencia de lo expuesto que se está a caer a este tipo de ataques y que por medio de sus conocimientos sean capaces de detectarlos y reportarlos, por ello la importancia de implementar programas adecuados de concientización.

Aplicar programas adecuados resulta crucial, ya que elegir el método de capacitación será imprescindible para crear una cultura de ciberseguridad, en tal sentido en “una encuesta aplicada a 1200 empleados el 69% de los encuestados había recibido formación en ciberseguridad de sus

empleadores y, sin embargo, cuando hicieron un cuestionario básico, el 61% falló" (Marousis, 2021). Esto resalta una preocupación más sobre la ineficiencia de muchos programas de capacitación de seguridad, que no se adaptan a las capacidades u otras características del personal.

Frente a este escenario un estudio realizado en Ecuador evaluó la efectividad de las simulaciones de ataques de phishing y planes de concienciación para reducir la vulnerabilidad de los empleados ante ataques cibernéticos en una pequeña empresa. Los resultados revelaron que la edad, experiencia laboral y acceso a información sensible impactaron la capacidad de respuesta, con mejores resultados en empleados jóvenes y tecnológicamente experimentados. Aunque la concienciación redujo la vulnerabilidad, persistieron riesgos asociados al comportamiento humano, sugiriendo la necesidad de formación continua" (Cabezas & Fiallos, 2024, p. 1).

En este artículo observamos que la edad es un factor determinante, en la que los colaboradores con edades mayores poseen menos competencias en tecnología por ende son más susceptibles a las amenazas de seguridad, contrario a aquellos de edades menores con mayor habilidad en el uso de tecnologías y un mayor conocimiento de estas. Esto resalta la importancia de elaborar programas de concientización que se adapten a diferentes grupos en este caso edades similares.

> En consecuencia, desde el punto de vista de los factores humanos, estudios sobre el phishing destacan el impacto de las características psicológicas, los factores demográficos y las experiencias individuales en la susceptibilidad del usuario. Ponen de manifiesto las dificultades continuas en las iniciativas de formación y concienciación, subrayando la necesidad de una comprensión más profunda de la dinámica de la confianza y el desarrollo de tácticas de prevención duraderas para contrarrestar eficazmente las amenazas de phishing (Mutlutürk et al., 2024, p. 7).

Otro estudio realizado en Suecia también hace mención sobre tener en consideración varios factores al momento de elaborar un programa de capacitación en ciberseguridad que se adapte a las necesidades y características de las personas a quien va dirigido y los objetivos de la organización. Ajustar su educación y capacitación a las condiciones de amenaza actuales, a los objetivos actuales de la organización y a las predisposiciones de los usuarios. Además, la capacitación debe proporcionarse de manera continua y basada en ejemplos con los que los

usuarios puedan identificarse. Para responder mejor a la naturaleza heterogénea de los usuarios, idealmente la capacitación debería ofrecerse utilizando diferentes métodos de entrega, como basados en juegos, basados en simulaciones y en línea.

Hallazgos claves

Centroamérica ha registrado en los últimos años un notable aumento en la adopción de la tecnología, un proceso de digitalización acelerado en sectores como el comercio electrónico, telecomunicaciones, banca, logística etc., estos avances han permitido la automatización de procesos y mejorar la atención a los clientes.

No obstante, estos avances también han traído consigo ciberataques, lo que ha puesto en riesgo la integridad, confidencialidad y disponibilidad de la información, casos recientes han evidenciado que muchas instituciones aún presentan brechas en sus mecanismos de seguridad, específicamente en aspectos como la capacitación del personal para identificar y responder ante incidentes de seguridad.

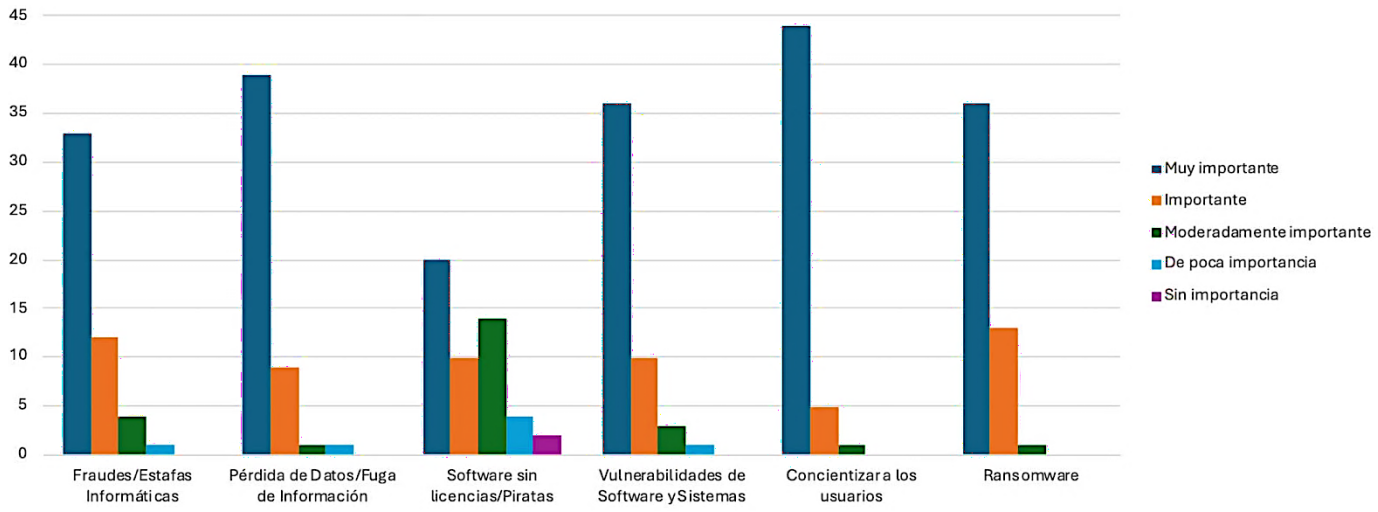


Figura 5. Preocupaciones en seguridad cibernética.
Fuente: (LabCIBE-UNA, 2024).

Estas brechas siguen siendo motivo de preocupación para muchos países centroamericanos, tal es el caso de Costa Rica donde en una investigación realizada con el fin de medir el estado de la ciberseguridad los resultados arrojaron que: El 88% considera muy importante este factor por la relevancia, en cuanto a la prevención de amenazas e incluso por la ausencia de una cultura cibernética sólida.

En segundo lugar, se posiciona la pérdida de datos/fuga de información con 78%, en el sentido que representa una amenaza significativa para las empresas, ya que dicha información puede contener datos sensibles y confidenciales, la cual impactaría de forma negativa a las organizaciones (LabCIBE-UNA, 2024).

Este estudio resalta que la falta de capacitación constituye una debilidad en una gran parte de las empresas, como resultado esto eleva la preocupación e impulsa la necesidad de fortalecer, y aplicar programas de formación en ciberseguridad.

Tabla 1. Países de América Central en el Índice Global de Exposición a la Ciberseguridad.

Country	Global ranking	Score
Costa Rica	37	0.438
Panama	50	0.569
Nicaragua	56	0.600
Honduras	57	0.603
El Salvador	59	0.617

Fuente: (AESA-EY, 2022).

La figura anterior nos muestra el nivel de exposición a la ciberseguridad que tienen los países de Centroamérica donde El Salvador y Honduras lideran esta tabla. Esta exposición puede tener resultados que afecten servicios críticos, por ende, es vital implementar controles de ciberseguridad robustos que permitan prevenir y responder a incidentes.

Considerando las cifras anteriores sobre la exposición a la ciberseguridad, en un estudio relacionado a los ataques cibernéticos dirigidos a individuos con el fin de obtener información de las empresas realizado en El Salvador, entre los datos relevantes de esta investigación resalta que entre "los incidentes de ciberseguridad, los tres principales vectores pertenecen a phishing con 31% de casos, 30% escaneo y explotación de vulnerabilidades, y 29% robo de credenciales de acceso" (Álvarez et al., 2024, p. 5). Estos resultados evidencian que los principales incidentes de seguridad tienen una relación directa con el error humano como ser el caso de phishing y el robo de credenciales, estos dependen en gran medida de la interacción con el usuario que da clic en enlaces sin antes verificar y que gestiona adecuadamente sus credenciales.

Así mismo en Honduras también la ciberseguridad se ha convertido en una preocupación importante para las autoridades. Según la Dirección de Investigación Policial (DPI), cada día se reportan entre 3 y 4 casos de ciberestafas, siendo el "phishing" la estafa más común. (Reyes, 2025, p. 37). En el análisis sobre el impacto del phishing en Honduras, diversos estudios recientes han buscado comprender la percepción ciudadana respecto al incremento de estas amenazas digitales. Una de estas investigaciones es sobre el phishing y el robo de identidad en Honduras donde se

consultó si se considera que el phishing de datos ha aumentado en Honduras en los últimos 5 años el 27% de los encuestados indicó que el tema le es indiferente.

"Estos hallazgos permiten no solo validar la hipótesis, sino también identificar áreas críticas donde es necesario implementar estrategias educativas y preventivas, con el fin de promover un entorno digital más seguro y resiliente para la población hondureña" (Reyes, 2025, p. 77).

La indiferencia ante estos temas nos hace más susceptibles a cometer errores que puedan poner en riesgos nuestra información y la de las empresas para las cuales laboramos, ya que al no estar informados de las amenazas a las que estamos expuestos y cómo prevenirlas nos convierte en un punto débil de los cuales los ciberdelincuentes pueden sacar provecho.

También en el mismo estudio "el 46.8% de la población encuestada respondió que estaría dispuesto a recibir capacitación de cómo protegerse y evitar ataques de phishing lo que demuestra un alto interés en poder detectar este tipo de ataques y poder resguardar la información" (Reyes, 2025, p. 81).

Este interés resalta una oportunidad para implementar programas de educación de ciberseguridad que resalten la detección y prevención de ataques más comunes y pueda crearse una cultura de seguridad que prevenga los errores humanos y la fuga de información en las organizaciones.

Vacíos de investigación

Al ser la innovación parte de su misión, visión y valores de Grupo Vesta, y tener como prioridad su cadena de suministro acelerando el éxito de sus clientes con soluciones innovadoras y experiencia global, también se encuentran expuestos a ciberataques, fuga de información y errores humanos derivados del manejo inadecuado de datos confidenciales. La literatura anterior resalta que el factor humano es uno de los principales vectores de riesgo en la seguridad de la información, estas investigaciones coinciden en que los accesos no autorizados, phishing, entre otros, se originan por la falta de capacitación o programas inadecuados para el personal que maneja información confidencial.

La alineación de estos resultados tanto en el contexto global, centroamericano como regional permite destacar que no solo es implementar programas de capacitación, si no que estos se adapten al contexto de sus objetivos y las características del personal. En la literatura anterior

se puede observar que, aunque a nivel global existen investigaciones relacionadas a este tema en Centroamérica y Honduras aún existen vacíos de información relacionada que permita a las empresas tener una orientación o una referencia para la ejecución de programas de formación del personal y los errores humanos más frecuentes que se dan en su organización que pueden resultar en pérdida de información.

En este sentido el conocer aquellos métodos de capacitación que reducen errores humanos en pérdida de información sensible resulta prioridad para Grupo Vesta SPS, considerando que el factor humano constituye una de las principales causas de incidentes de seguridad, la mitigación de estos errores mediante procesos formativos ayudará a reducir los riesgos.

2.2 MARCO CONCEPTUAL

Según Jabareen,(2009) un marco conceptual se define como una red o un plano de conceptos interrelacionados. El análisis de marcos conceptuales ofrece un procedimiento de autorización para construir marcos conceptuales basado en la metodología de la teoría fundamentada. Las ventajas del análisis de marcos conceptuales radican en su flexibilidad, ya que permite adaptarse a este contexto, en su capacidad de modificación dado que puede ajustarse a medida que avanza la investigación y su énfasis en la comprensión en lugar de la predicción.

En este apartado se definen los conceptos más importantes de la investigación con la finalidad de simplificar la comprensión del tema investigado. Para ello se revisan los siguientes conceptos claves como seguridad de la información, información sensible, error humano en ciberseguridad, métodos de capacitación del personal, concientización, cultura de seguridad, amenazas, gestión del riesgo informático, etc., que permitirán interpretar de mejor manera el problema de investigación, dando una perspectiva sobre cómo estos se relacionan y juegan un papel importante y proporcionan una base sólida para analizar la eficacia de los distintos métodos de capacitación del personal que disminuyan el error humano en la pérdida de información sensible dentro de Grupo Vesta SPS en el año 2026, para ello es necesario comenzar definiendo:

Seguridad de la información

Lundgren & Möller2019) lo define como la condición en la que cada persona tiene el acceso apropiado, a cada parte de un activo de información, según las necesidades y valores de los involucrados. También integra aspectos técnicos como confidencialidad, integridad,

disponibilidad, con los aspectos humanos, éticos organizacionales y contextuales de la seguridad de la información.

Información sensible

León, (2022) define información sensible como aquella cuya divulgación, acceso no autorizado, alteración o pérdida puede generar consecuencias negativas significativas, ya sea para individuos, organizaciones o la sociedad. La sensibilidad de la información depende del contexto, un dato puede volverse más o menos sensible según quien lo maneje, con qué propósito y en qué condiciones es utilizado. Por ello la información sensible es aquella cuya pérdida, mal uso, acceso no autorizado podría afectar negativamente los intereses nacionales, programas federales o la privacidad de las personas (NIST, 2009).

Error humano en ciberseguridad

Según Khadka & Ullah (2025) el error humano se refiere a las acciones no maliciosas de empleados que pueden provocar incidentes de seguridad. Esto incluye descuidos, falta de conocimiento, errores cognitivos o decisiones incorrectas bajo presión. Estudios recientes destacan la relevancia de los factores humanos en la ciberseguridad y proponen marcos centrados en el usuario para fortalecer la resiliencia organizacional.

Métodos de capacitación del personal

Para Prümmer et al.,(2024) son los métodos o estrategias pedagógicas utilizadas por la organización para entrenar a sus colaboradores en buenas prácticas de seguridad. Puede incluir capacitación tradicional, e-learning, simulaciones de phishing, gamificación, talleres, etc. Una revisión sistemática reciente mapea estas metodologías y evalúa su eficacia en reducir riesgos humanos.

Concientización en ciberseguridad (CSA)

Es el proceso educativo continuo para que los empleados reconozcan amenazas, entiendan su papel en la defensa y adopten comportamientos seguros. No se trata solo de conocimiento técnico, sino de inculcar actitudes y responsabilidades. Por ejemplo, Khando et al (2021) muestra como los programas de concientización bien diseñados pueden reducir la explotación de debilidades humanas.

Cultura de seguridad organizacional

Aldulaimi et al., (2023) la define como un conjunto compartido de valores, creencias y comportamientos en una organización que refuerzan la seguridad de la información. Una cultura de seguridad fuerte implica que todos, desde la alta gerencia hasta el personal operativo, ven la ciberseguridad como una responsabilidad colectiva. La literatura resalta que no basta con controles técnicos, la cultura debe abordarse de forma socio-cultural para ser efectiva.

Amenazas cibernéticas

Son acciones intencionales que buscan comprometer la seguridad de sistemas de información, alterando su confidencialidad, integridad o disponibilidad. Estas amenazas pueden originarse en actores maliciosos, que explotan vulnerabilidades técnicas, humanas para causar daño, robo de datos espionaje o interrupciones operativas (Admass et al., 2024).

Conforme a los conceptos anteriores podemos determinar estos se encuentran sumamente relacionados, debido a que la seguridad de la información es fundamental para toda empresa, para que los activos de información sean protegidos de forma adecuada a accesos no autorizados, pérdidas o alteraciones que puedan afectar su integridad y disponibilidad. Por tanto, el manejo inadecuado de la información representa una gran amenaza, dado que su exposición puede representar pérdidas significativas no sólo económicas, también reputacionales y legales. Dicho esto, aunque la infraestructura resulta crucial en la protección de la información, las personas que son quienes manejan dicha información necesitan estar capacitados de cómo protegerla. Por ello es imprescindible que se invierta en programas de capacitación del personal ya que un error puede provocar pérdida de información valiosa para la organización.

Es por lo que hoy en día se habla de concientización y capacitación del personal. Estos conceptos y prácticas juegan un papel importante en la cultura de seguridad de una empresa, ya que una persona con conocimientos puede modificar su conducta y acciones al momento de manejar los datos y hacerlo de forma adecuada, segura y con precaución. Es por ello, que su implementación adecuada es vital para que pueda ser una acción de prevención para la materialización de un incidente.

Este modelo conceptual permite comprender la relación entre los métodos de capacitación, errores humanos y pérdida de información y demás conceptos clave que se interrelacionan con el tema de investigación. Esto sustenta la necesidad de evaluar los métodos de capacitación como un elemento crucial que apoye a mejorar la resiliencia en términos de seguridad de la información.

Este modelo conceptual también permite entender la seguridad de la información como un sistema integrado, donde la formación del personal se convierte en un elemento estratégico para reducir los errores humanos y de esta forma evitar en gran medida la pérdida de la información.

2.3 TEORÍAS DE SUSTENTO

Estas teorías son planteamientos o marcos conceptuales previamente establecidos por la comunidad científica y permite fundamentar y explicar las variables acordados en esta investigación, proporciona una base teórica sólida que orienta el análisis, la comprensión e interpretación del problema de estudio. Diversos estudios han señalado que los incidentes de seguridad de la información se originan de errores no intencionales derivados del desconocimiento, falta de concientización y capacitación del personal que maneja la información. Esta realidad pone en manifiesto una necesidad de abordar este tema desde un enfoque diferente, que considere varios aspectos tales como los tecnológicos, formativos, conductuales, culturales entre otros que influyen en el comportamiento de los colaboradores.

Es por lo que resulta importante detallar las teorías que se relacionan al tema de investigación y nos permitan tener un panorama más amplio de cómo la conducta de las personas al estar preparadas con conocimientos robustos, pueden reducir los errores humanos que provocan la pérdida de la información sensible en las empresas. Así mismo el conocer normativas, marcos, mejores prácticas y estándares internacionales que están integrando en sus estructuras el tema de la concientización y capacitación del personal como un control importante en la seguridad de las empresas que decidan implementarlos.

2.3.1 BASES TEÓRICAS

Muchas empresas están adaptando sus operaciones a normativas, estándares y marcos internacionales con el fin de fortalecer su postura de seguridad, adaptando estas prácticas a su operativa buscan mejorar su capacidad para hacer frente a incidentes de seguridad y proteger sus activos, entre este su activo más valioso la información.

La ISO/IEC 27001, su cumplimiento indica que una organización o empresa ha establecido un sistema para gestionar sus riesgos asociados con la seguridad de la información que posee o administra, en uno de sus anexos establece la educación de seguridad de la información, lo que los prepara para afrontar dichos riesgos.

CIS Controls establece mejores prácticas relacionadas a ciberseguridad cuyo fin es reducir las probabilidades de sufrir un ciberataque, en uno de sus controles detalla que se debe establecer un programa de concientización en seguridad, de tal forma que se influya en la conducta de las personas y se puedan disminuir riesgos.

La teoría de la cultura de seguridad de la información donde da Veiga & Martins, (2015) muestran como un programa de concienciación, mejora la cultura de seguridad de la información en una organización. La capacitación debe diseñarse no sólo como transferencia de conocimiento, sino como un componente para construir cultura, es decir liderazgo, comunicación abierta, responsabilidad compartida y prácticas organizativas.

Por otra parte, el Instituto Nacional de Estándares y tecnología, en su publicación especial denominado NIST SP detalla una guía para desarrollar e implementar programas de formación en ciberseguridad para producir habilidades y competencias en seguridad, de forma que puedan tener una visión y una respuesta proactiva (National Institute of Standards and Technolog, 2024).

Así mismo PCI DSS exige que las entidades que manejan datos de tarjetas mantengan un programa de concientización en seguridad que fortalezca su postura en seguridad.

Estos estándares detallan buenas prácticas para salvaguardar la información de quienes lo implementan y aunque no son de obligatoria adopción, su consideración fortalece los controles internos de seguridad y reducen la posibilidad de que se presenten incidentes debido a errores humanos y que su información pueda estar expuesta.

Teniendo en cuenta que la elección del método de capacitación basado en estas teorías puede ayudar a mejorar el desempeño y conducta de las personas y la cultura en la que estos se desarrollan.

Ortiz Ocaña (2013) describe algunas teorías del aprendizaje y modelos pedagógicos que ayudan a identificar métodos y procedimientos que garanticen la efectividad del proceso productivo de forma que sea más eficiente y menos costoso, los cuales se detallan a continuación:

El conductismo: asocia el esquema de estímulo-respuesta cuyo refuerzo positivo (recompensas) o negativo (evitar castigos) para fomentar conductas específicas.

Teoría constructivista: Su papel fundamental consiste en promover una atmósfera de reciprocidad a través de la enseñanza indirecta y del planteamiento de problemas.

Psicología Cognitiva Contemporánea: Se enfoca en cómo procesamos, organizamos y retenemos información. Introduce conceptos como el aprendizaje significativo y la metacognición.

Enfoque Histórico-Cultural: Introduce la Zona de Desarrollo Próximo (ZDP), donde el aprendizaje guiado es clave.

Teorías Humanistas: Centrada en el desarrollo personal, la autorrealización y el bienestar emocional del empleado. Promueve el aprendizaje autodirigido y la motivación intrínseca.

Modificabilidad Cognitiva Estructural: Propone que la inteligencia puede desarrollarse mediante mediación e intervención. Introduce el Programa de Enriquecimiento Instrumental para mejorar habilidades cognitivas.

Conectivismo: El aprendizaje se basa en la conexión entre redes (personas, tecnologías y fuentes de información). Se adapta a un mundo interconectado donde el acceso a la información es constante. Promueve la habilidad de aprender y desaprender en contextos digitales.

Así mismo Hernández & Medina (2023), detalla que existen enfoques para el estudio del error humano tal como ser:

Enfoque cognitivo: como exponente de este enfoque se destaca el modelo de habilidades, reglas y conocimientos (SRK, por sus siglas en inglés) desarrollado por Rasmussen. Es un modelo conceptual que ha tenido gran éxito al esbozar los mecanismos del error. Según su propuesta, previo a la ejecución de la tarea se suceden varias etapas, cuyo número dependerá del nivel de funcionamiento que le exija cada tipo de tarea al individuo. el autor establece una tipología del error humano, derivado de la clasificación de los niveles de ejecución humana en actividades complejas: errores basados en habilidades, errores basados en reglas y errores basados en conocimientos, siendo los últimos los que alcanzan mayor frecuencia de ocurrencia

Enfoque ergonómico: los estudios ergonómicos vinculados a la seguridad se concentran, fundamentalmente, en estudios sobre la carga de trabajo. Se basan en el análisis de la interrelación entre las exigencias de la tarea y los recursos físicos y mentales movilizados por el trabajador para cumplir con estos requerimientos de manera exitosa.

Enfoque sistémico: El enfoque sistémico asume que en el ámbito laboral el individuo comete errores que deben ser considerados como consecuencias y no como causas. En este sentido, aporta una serie de postulados que son útiles para la gestión de riesgos:

- El error es inherente a la condición humana.
- No es posible cambiar la condición humana, pero sí optimizarla.
- Las condiciones en las que el trabajador realiza sus funciones sí se pueden modificar, con lo cual se contribuye a optimizar la condición humana.
- Introducir barreras y defensas permitirá minimizar el error humano en todos los niveles, así como sus consecuencias.

2.3.2 MARCO METODOLÓGICO

McMeekin et al., (2020) define el marco metodológico como una guía estructurada para completar un proceso o procedimiento. Esta estructura sistemática guía el desarrollo del estudio de la investigación mediante la selección y organización de métodos, técnicas y procedimientos que permiten responder a las preguntas y objetivos planteados.

Es importante considerar investigaciones similares que han sido desarrolladas por expertos y profesionales de seguridad de la información para tener en cuenta las técnicas e instrumentos utilizados en otras investigaciones que permite identificar cuáles son los métodos de capacitación que influyen en la disminución de errores humanos en la pérdida de información sensible. Asimismo, el análisis de estas investigaciones apoyará como referencia para el desarrollo de la presente investigación de modo que pueda alinearse con prácticas ampliamente verificadas en el ámbito académico y profesional. Y así, asegurarse que los datos obtenidos sean precisos y que las conclusiones sean coherentes con las variables de estudio. Teniendo en cuenta que el error humano es un riesgo que puede materializarse provocando la fuga de información relevante; conocer qué investigaciones se han realizado al respecto permiten fortalecer los métodos de capacitación implementados en Grupo Vesta, San Pedro Sula, y como medida preventiva en el ámbito de la seguridad de la información y ciberseguridad.

Un estudio realizado en Ecuador para explorar las estrategias, tecnologías y patrones específicos para mitigar los ciberataques, con énfasis en la ingeniería social, utilizó una metodología cualitativa basada en entrevistas a docentes investigadores y expertos en ciberseguridad, seleccionados mediante un muestreo aleatorio simple.

> Los resultados muestran que la falta de capacitación en ciberseguridad convierte a los usuarios en blancos fáciles para los atacantes, a esto se suma la ausencia de estrategias adecuadas y tecnologías que mitiguen las amenazas (Fueres et al., 2024, P.1).

Estos resultados denotan la realidad que enfrentan las empresas no solo de estos países sino de todo el mundo, las personas son blanco fácil, y el no tomar medidas adecuadas como la concientización puede resultar en la pérdida de la información. La situación se vuelve más riesgosa cuando tampoco se cuenta con estrategias organizacionales claras que conlleven a la elaboración de programas de concientización efectivos.

El tema de la cultura de seguridad ha sido ampliamente estudiado, tal es el caso de México donde se implementó un proceso de evaluación mediante encuestas en línea anónimas entre empleados de múltiples sectores, como empresas de servicios, negocios mayoristas, industrias manufactureras, empresas de construcción y establecimientos de comercio minorista.

Se concluyo que "adaptar sus programas de formación en ciberseguridad para alinearlos con distintos niveles educativos, asegurando una cobertura integral y estrategias efectivas de mitigación de riesgos" (García et al., 2024, p. 14). Considerar las características de los empleados, tales como su nivel educativo, experiencia laboral, y funciones y responsabilidades dentro de la organización, apoya a la implementación de técnicas adecuadas, que apoyaran a consolidar los conocimientos en seguridad. En conclusión, cuando la capacitación es inclusiva, adaptada y orientada a desarrollar competencias en base a las características de los colaboradores, se mejora la cultura de seguridad y por ende la reducción de errores al momento de manejar la información.

Esto se puede observar en otro estudio donde se evaluó la efectividad de las simulaciones de ataques de phishing y planes de concienciación para reducir las vulnerabilidades.

> La investigación incluyó la simulación de ataques de phishing a través de correos electrónicos, mensajes de texto y otros medios, implementados en fases dentro de una organización. Se empleó una metodología experimental para evaluar la efectividad de los planes de concienciación sobre phishing en una organización. Los resultados también destacan la necesidad de planes de concienciación más personalizados y diferenciados (Cabezas & Fiallos, 2024, p. 13)

Otro estudio relacionado con el error humano examinó los errores humanos influenciados por acciones, actitudes y comportamientos que afectan a la seguridad general de la información.

> Se utilizó muestreo intencionado dentro del enfoque cualitativo para seleccionar treinta (30) pequeños gestores de pequeñas empresas. Los datos se recopilaron mediante una encuesta cualitativa en línea como formulario de Google. El estudio utilizó análisis temático. Los resultados revelaron que los errores humanos repetidos comprometen los principios de seguridad de la información y convierten a los empleados en el eslabón más débil. El estudio explicó los riesgos que suponen los empleados debido a la ignorancia o la mala toma de decisiones, errores técnicos y errores basados en habilidades y políticas (Ncubukezi, 2022, p.1).

Según lo anterior el procedimiento metodológico seleccionado para este estudio es no experimental y se establece en base a las metodologías desarrolladas y aplicadas por investigadores en estudios similares o que tienen relación con el tema de investigación en el análisis del factor humano, la capacitación del personal, pérdida de información sensible y la seguridad de la información en entornos corporativos o similares. Muchas investigaciones académicas y científicas han demostrado mediante sus resultados que un enfoque cuantitativo es una opción viable y adecuada si se pretende analizar la relación entre los métodos de capacitación del personal y la reducción del error humano que provocan la pérdida de información sensible en las empresas. Sobre todo, este enfoque es relevante cuando se busca obtener resultados estadísticos sobre percepciones, comportamientos, experiencias, acciones de las personas en un entorno empresarial.

La revisión de la literatura señala que los estudios relacionados a métodos de capacitación y error humano en ciberseguridad y seguridad de la información emplean la encuesta como técnica principal para la recolección de información. Considerando este método por su capacidad para recolectar información directamente del personal que participa en los procesos de capacitación o la muestra seleccionada. Permitiendo capturar mediante preguntas estructuradas su percepción, conocimiento y demás información relevante que alimenta con resultados confiables y permite brindar un marco de referencia para futuras investigaciones.

En base a lo anterior, el procedimiento metodológico adoptado en esta investigación se justifica por su relación con metodologías previamente probadas en estudios con temas similares en diferentes partes del mundo. Su alineación con las teorías de sustento en base a marcos, estándares y mejores prácticas internacionalmente adoptados por grandes organizaciones sobre

temas de concientización y capacitación en seguridad de la información justifica su implementación y garantiza la compatibilidad con investigaciones previas, que han tenido resultados importantes y significativos que aportan una idea al tema de investigación.

2.3 MARCO LEGAL

Honduras enfrenta retos importantes relacionado con la seguridad digital, a medida avanza la digitalización y las empresas adaptan estas tecnologías a sus necesidades, se vuelve imprescindible contar con marco legal que brinde protección efectiva frente al cibercrimen y las amenazas a las que se está expuesto, por ello es importante que la educación y concientización en materia de seguridad y ciberseguridad se establezcan obligatoriamente como herramientas que ayude a prevenir ataques.

Hasta el momento no existen leyes en Honduras relacionadas a concientización de ciberseguridad, sin embargo, ciertos sectores están prestando atención al aumento de incidentes de seguridad en el país, y sectores como la banca ya toman en cuenta la implementación de concientización del personal.

En este contexto la Comisión Nacional de Banca y Seguros (2022) en la circular No.025/2022 Normas para la gestión de tecnologías de información, ciberseguridad y continuidad del negocio, del capítulo V de la gestión de seguridad de la información y ciberseguridad, artículo 23, establece la aplicación de programas de concientización y capacitación tanto para el personal interno como para sus clientes, esto de aplicación para los de las instituciones supervisadas y autorizadas por la CNBS.(Pág. 14).

Esta normativa resalta la importancia de fortalecer una cultura de seguridad en todos los sectores, y apunta a que la formación continua en todos los niveles es esencial para hacer frente a los riesgos asociados al robo de información por errores humanos.

CAPÍTULO III: METODOLOGÍA

En este apartado se describe el camino metodológico seguido para el desarrollo del estudio, detallando la coherencia entre los elementos metodológicos, el enfoque metodológico utilizado, el diseño y alcance de la investigación, así como las técnicas, instrumentos y procedimientos utilizados para la obtención y análisis de la información. La metodología de la investigación se entiende como la estructura de los métodos y estrategias que se aplican de forma lógica y planificada para garantizar el cumplimiento de los objetivos del estudio. Dentro del proceso investigativo, la metodología constituye una fase esencial, ya que en ella se establecen las decisiones relacionadas con los métodos y técnicas que orientan la ejecución del trabajo científico (Patel & Patel, 2019).

3.1 CONGRUENCIA METODOLÓGICA

Este capítulo constituye un principio esencial para garantizar la coherencia interna de la investigación, especialmente cuando se analiza los métodos de capacitación que influyen en la reducción de errores humanos en la pérdida de información sensible en Grupo Vesta, SPS 2026. Con el objetivo de que en la investigación exista una congruencia se presentan la matriz de congruencia metodológica en la que se integra el tema, problema de investigación y las variables del estudio.

3.1.1 MATRIZ METODOLÓGICA

McMeekin et al., (2020) define el marco metodológico como una guía estructurada para completar un proceso o procedimiento, por lo tanto, la matriz metodológica es una herramienta fundamental en la planificación de cualquier investigación, que permite organizar de manera clara los elementos claves del proceso investigativo.

Tabla 2. Matriz Metodológica

Título de la investigación	Objetivos de la investigación		Preguntas de Investigación	Variables	
	General	Específicos		Independiente	Dependiente
Métodos de capacitación que reducen errores humanos en pérdida de información sensible en grupo Vesta SPS, 2026	Evaluar métodos de capacitación que influyen en la reducción del error humano relacionado con la pérdida de información sensible en Grupo Vesta San Pedro Sula, 2026.	Enumerar métodos de capacitación en ciberseguridad implementados y los colaboradores por área que manejan información sensible en Grupo Vesta 2026. Identificar los errores humanos más relevantes que generan pérdida de información sensible en Grupo Vesta, San Pedro Sula, 2026.	¿En qué medida los métodos de capacitación del personal influyen en la reducción del error humano relacionado con la pérdida de información sensible en Grupo Vesta de San Pedro Sula en el año 2026? ¿Qué métodos de capacitación en ciberseguridad se implementan y cuántos colaboradores por área manejan información sensible en Grupo Vesta, SPS 2026? ¿Cuáles son los errores humanos más relevantes que generan pérdida de información sensible en Grupo Vesta, San Pedro Sula, en el 2026?	Métodos de Capacitación	Reducción de errores humanos en la pérdida de información sensible.

Fuente: Elaboración propia.

3.1.2 ESQUEMA DE VARIABLES DE ESTUDIO

Las variables son características, propiedades o condiciones que pueden ser medibles, observables y pueden variar según la situación, por lo tanto, son elementos que cambian y se miden para entender la relación entre ellas. Para este estudio se hace uso de dos variables una variable independiente y una dependiente.

Se comenzará definiendo la variable independiente como el factor que se manipula en un estudio para observar su efecto sobre otra variable, por lo que se dice que es una relación causal, dado que su variación es la que se espera que genere cambios en otra variable (Kaur & Mittal, 2021). Así mismo, determina que una variable dependiente es el resultado o efecto observado que cambia en función de una o más variables independientes dentro de un estudio.

Se detalla a continuación, las variables de estudio siendo la variable independiente los métodos de capacitación con sus dimensiones e indicadores y la variable dependiente la reducción de errores humanos en la pérdida de información sensible con sus dimensiones e indicadores.

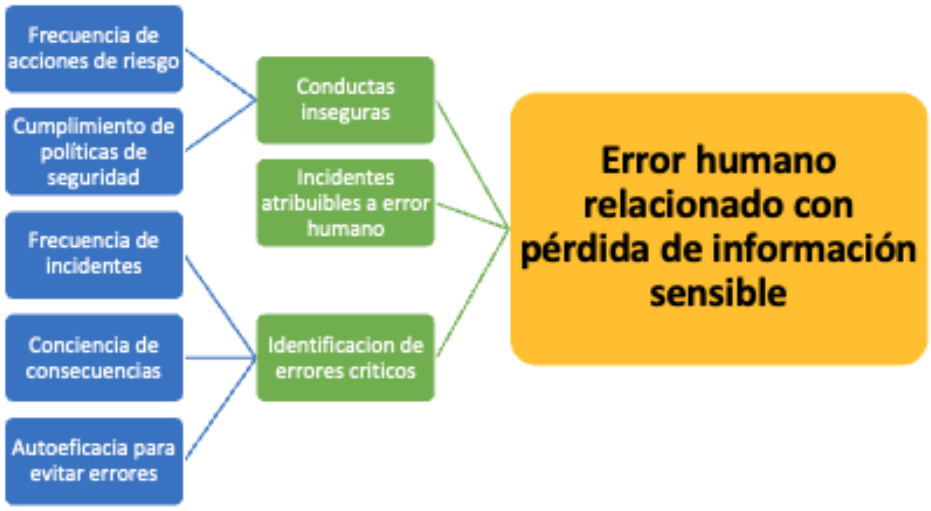


Figura 6.Variable dependiente con sus respectivas dimensiones e indicadores del estudio.
Fuente**:** Elaboración propia.

Figura 7.Variable independiente con sus dimensiones e indicadores del estudio.
Fuente**:** Elaboración propia.

En la figura 6 se encuentra plasmada la variable dependiente y en la figura 7 la variable independiente identificadas en esta investigación, siendo la variable independiente los métodos de capacitación la cual se pretende mediante esta investigación determinar si influye en la reducción de errores humanos en la pérdida de información sensible como variable dependiente que es la de interés principal en este estudio.

3.1.3 OPERACIONALIZACIÓN DE VARIABLES

Para la presente investigación se realizó la operacionalización de variables a fin de conocer cómo estos se convierten en elementos medibles que permitan estudiar la relación entre los métodos de capacitación del personal y la reducción del error humano asociado con la pérdida de información sensible en Grupo Vesta SPS. La variable independiente Métodos de capacitación del personal, se estructuró en las dimensiones contenido, modalidad, frecuencia y refuerzo, interactividad y evaluación. Estas dimensiones integran los indicadores de claridad del contenido,

adecuación del puesto, relevancia del contenido, modalidad predominante, adecuación de la modalidad, duración adecuada, cantidad de sesiones, materiales de refuerzo, actividades prácticas, aplicación de evaluación, nivel de interactividad y contenido comprendido. Estos indicadores se miden mediante escalas de tipo Likert y preguntas categóricas que permitieron obtener datos sobre los métodos de capacitación implementados en la organización.

Por otra parte, la variable dependiente, Error humano relacionado con la pérdida de información sensible, se operacionaliza mediante las dimensiones de conductas inseguras, incidentes atribuibles a error humano, conciencia y autoeficacia. Estas dimensiones tienen como indicadores; frecuencia de acciones de riesgo, cumplimiento de políticas de seguridad, frecuencia de incidentes, conciencia de consecuencias, autoeficacia para evitar errores. Estos indicadores fueron medidos mediante escalas Likert, con el fin de detectar los patrones de conducta de los empleados y los incidentes de seguridad que están relacionados al error humano. La operacionalización de ambas variables está relacionada con los objetivos de la investigación y el problema identificado, la incorporación de las dimensiones e indicadores facilitarán el análisis estadístico de la información sobre la relación entre los métodos de capacitación y el error humano.

Tabla 3. Operacionalización de variables

Variable	Definición		Dimensiones	Indicadores	Items	Unidades (Categorías)	Escala
	Conceptual	Operacional					
Métodos de capacitación del personal	Para Prümmer et al.,(2024) son los métodos o estrategias pedagógicas utilizadas por la organización para entrenar a sus colaboradores en buenas prácticas de seguridad. Puede incluir capacitación tradicional, e-learning, simulaciones de phishing, gamificación, talleres, etc. Una revisión sistemática reciente mapea estas metodologías y evalúa su eficacia en reducir riesgos humanos.	Los métodos de capacitación se definen como el conjunto de prácticas, actividades y estrategias formales que la organización utiliza para fortalecer los conocimientos y habilidades del personal en temas de seguridad de la información. Su medición se realiza a través de la percepción del empleado sobre la calidad, frecuencia, modalidad, interactividad y evaluación de las capacitaciones recibidas. Se cuantifica mediante un cuestionario estructurado con escalas tipo Likert que valoran dimensiones como el contenido, la modalidad de capacitación (presencial, virtual, mixta), interactividad y evaluación, así como la frecuencia y refuerzo de las capacitaciones recibidas	Contenido	Claridad del contenido	¿En qué medida considera que el contenido de las capacitaciones en seguridad de la información es claro y fácil de comprender?	Nada claro	1
						Poco claro	2
						Regular	3
						Claro	4
						Muy claro	5
				Adecuación al puesto	¿El contenido de las capacitaciones en seguridad de la información es relevante para mis actividades diarias dentro de la organización?	Totalmente en desacuerdo	1
						En desacuerdo	2
						Ni de acuerdo ni en desacuerdo	3
						De acuerdo	4
						Totalmente de acuerdo	5
				Relevancia del contenido	¿Qué tan relevantes considera los temas abordados durante las capacitaciones?	Nada relevante	1
						Poco relevante	2
						Medianamente relevante	3
						Relevante	4
						Muy relevante	5
					¿Las sesiones de capacitación incluyeron explicaciones sobre errores humanos comunes y cómo evitarlos?	Totalmente en desacuerdo	1
						En desacuerdo	2
						Neutral	3
						De acuerdo	4
						Totalmente de acuerdo	5
			Modalidad	Modalidad predominante	¿Ha recibido capacitaciones relacionados con buenas practicas de seguridad de la información?	No	0
						Si	1
					¿Qué modalidad predominó en las capacitaciones que recibió? (marque una)	Presencial	1
						E-learning (a distancia)	2
						Mixto	3
						Micro-learning (módulos breves)	4
						Boletines informativos	5
				Adecuación de la modalidad	¿La modalidad de capacitación (virtual, presencial o mixta) facilitó su aprendizaje?	Nada de acuerdo	1
						Poco de acuerdo	2
						Ni de acuerdo ni en desacuerdo	3
						De acuerdo	4
						Totalmente de acuerdo	5
				Duración adecuada	¿La duración de las sesiones fue adecuada para comprender la información presentada?	Totalmente en desacuerdo	1
						En desacuerdo	2
						Ni de acuerdo ni en desacuerdo	3
						De acuerdo	4
						Totalmente de acuerdo	5
			Frecuencia y Refuerzo	Cantidad de sesiones	¿Cuántas sesiones o módulos de capacitación en seguridad de la información recibió en los últimos 12 meses?	0 sesiones	1
						1 – 2 sesiones	2
						3 – 4 sesiones	3
						5 – 6 sesiones	4
						Más de 6 sesiones	5
				Materiales de refuerzo	¿Con qué frecuencia recibe recordatorios o materiales de refuerzo (tips, boletines, micro-learnings) sobre buenas prácticas de seguridad?	Nunca	1
						Annual	2
						Semestral	3
						Mensual	4
						Semanal	5
			Interactividad y evaluación	Actividades prácticas	En las capacitaciones, ¿Con qué frecuencia se incluyeron actividades prácticas tales como ser simulaciones, ejercicios, laboratorios, phishing simulado?	Nunca	1
						Rara vez	2
						A veces	3
						Frecuente	4
						Muy frecuente	5
				Aplicación de evaluación	¿En las capacitaciones recibidas se le aplicó una evaluación o prueba después de la capacitación? (p. ej. quiz, examen, post-test)	No	0
						Si	1
				Nivel de interactividad	¿Las capacitaciones incluyeron ejemplos o casos prácticos aplicables a su trabajo?	Nunca	1
						Rara vez	2
						A veces	3
						Frecuentemente	4
						Siempre	5
				Contenido comprendido	¿Qué tan satisfecho(a) está con la calidad general de las capacitaciones recibidas?	Muy insatisfecho(a)	1
						Insatisfecho (a)	2
						Ni satisfecho(a) ni insatisfecho(a	3
						Satisfecho(a)	4
						Muy satisfecho(a)	5

Continuación de la tabla 3.

Variable	Definición		Dimensiones	Indicadores	Items	Unidades (Categorías)	Escala
	Conceptual	Operacional					
Error humano relacionado con pérdida de información sensible	Según Khadka & Ullah (2025) el error humano se refiere a las acciones no maliciosas de empleados que pueden provocar incidentes de seguridad. Esto incluye descuidos, falta de conocimiento, errores cognitivos o decisiones incorrectas bajo presión. Estudios recientes destacan la relevancia de los factores humanos en la ciberseguridad y propone marcos centrados en el usuario para fortalecer la resiliencia organizacional.	En este estudio, el error humano relacionado con pérdida de información sensible se mide como el nivel de conductas de riesgo y la frecuencia/impacto de incidentes de pérdida de información atribuibles a personas dentro de la organización. Se operacionaliza a través de: (a) las conductas que provocan un incidente de seguridad(b) registros de incidentes donde la causa raíz se clasifica como error humano (por ejemplo, envío de información al destinatario equivocado, eliminación accidental, errores de configuración) y la conciencia del usuario una vez ha recibido la capacitación sobre seguridad. La variable se representa mediante un índice compuesto que combina puntuaciones de cuestionario tipo Likert y datos de incidentes registrados en los últimos 12 meses.	Conductas inseguras	Frecuencia de acciones de riesgo	¿Las capacitaciones modificaron mis hábitos o rutinas al manejar información sensible?	Totalmente en desacuerdo	1
						En desacuerdo	2
						Neutral	3
						De acuerdo	4
						Totalmente de acuerdo	5
					¿Con qué frecuencia deja visible información sensible en su computadora o documentos impresos al retirarse de su puesto de trabajo?	Nunca	1
						Rara vez	2
						A veces	3
						Frecuentemente	4
						Siempre	5
					¿Con qué frecuencia guarda, descarga o comparte información sensible en dispositivos o plataformas no autorizadas (USB personal, correo personal, apps no aprobadas)?	Nunca	1
						Rara vez	2
						A veces	3
						Frecuentemente	4
						Siempre	5
					¿Con qué frecuencia revisa cuidadosamente enlaces o archivos antes de hacer clic para evitar caer en intentos de phishing?	Nunca	1
						Rara vez	2
						A veces	3
						Casi siempre	4
						Siempre	5
					¿Con qué frecuencia utiliza contraseñas seguras (complejas, únicas y no compartidas) para acceder a sistemas o información sensible?	Nunca	1
						Rara vez	2
						A veces	3
						Casi siempre	4
						Siempre	5
				Cumplimiento de políticas de seguridad	En mi trabajo diario, ¿Sigo las políticas y procedimientos de seguridad al manejar información sensible?	Nunca	1
						Rara vez	2
						A veces	3
						Frecuentemente	4
						Siempre	5
					Antes de enviar información sensible, ¿Verifico cuidadosamente que el destinatario sea el correcto?	Nunca	1
						Rara vez	2
						A veces	3
						Frecuentemente	4
						Siempre	5
			Incidentes atribuibles a error humano	Frecuencia de incidentes	En los últimos 12 meses, ¿Con qué frecuencia ha ocurrido que, por un error suyo, se perdió, borró o quedó inaccesible información sensible?	Nunca	1
						Una vez	2
						2-3 veces	3
						4-5 veces	4
						mas 5 veces	5
					En los últimos 12 meses, ¿Con qué frecuencia ha ocurrido que, por un error suyo, se envió o expuso información sensible a personas no autorizadas?	Nunca	1
						Una vez	2
						2-3 veces	3
						4-5 veces	4
						mas 5 veces	5
			Conciencia y autoeficacia	Conciencia de consecuencia	¿Considero que un error mío en el manejo de información sensible podría generar consecuencias graves para la organización?	Totalmente en desacuerdo	1
						En desacuerdo	2
						Ni de acuerdo ni en desacuerdo	3
						De acuerdo	4
						Totalmente de acuerdo	5
					¿Tengo claro qué la información que manejo en mi trabajo se considera sensible?	No	0
						Si	1
				Autoeficacia para evitar errores	¿Me considero capaz de identificar situaciones en las que podría cometer un error que afecte información sensible?	Totalmente en desacuerdo	1
						En desacuerdo	2
						Ni de acuerdo ni en desacuerdo	3
						De acuerdo	4
						Totalmente de acuerdo	5
					¿Cuando tengo dudas sobre cómo manejar información sensible, sé a quién consultar o dónde buscar la información correcta para evitar errores?	Totalmente en desacuerdo	1
						En desacuerdo	2
						Ni de acuerdo ni en desacuerdo	3
						De acuerdo	4
						Totalmente de acuerdo	5
					¿Después de las capacitaciones, me siento más seguro(a) al manejar información sensible?	Totalmente en desacuerdo	1
						En desacuerdo	2
						Neutral	3
						De acuerdo	4
						Totalmente de acuerdo	5

Fuente: Elaboración propia

3.1.4 HIPÓTESIS

La información siendo un activo tan importante para las organizaciones, resulta imprescindible que el personal se encuentre capacitado para que los datos sean manejados de forma adecuada y segura. Sin embargo, uno de los factores que más influye en la pérdida de información es el error humano, que se puede presentar por varios motivos como ser desconocimiento, falta de preparación o ausencia de capacitación en temas de seguridad al personal. Ante este escenario, surge la necesidad de estudiar si las diferentes formas o métodos utilizados para capacitar al personal realmente tienen influencia en la disminución de errores humanos y por ende mejorar la seguridad de la información en Grupo Vesta SPS.

Es por ello por lo que en esta investigación se plantea evaluar la relación existente entre los métodos de capacitación y la reducción del error humano asociado a la pérdida de información sensible. Dicho esto, se plantea las siguientes hipótesis de investigación:

H_1: Los métodos de capacitación del personal influyen en gran medida con la reducción del error humano asociado con la pérdida de información sensible.

H_0: Los métodos de capacitación del personal no influyen con la reducción del error humano asociado con la pérdida de información sensible.

3.2 ENFOQUE Y MÉTODOS

En este apartado se detalla la metodología de investigación utilizada en el presente estudio de investigación, describiendo el tipo y enfoque utilizados, las variables de estudio, su operacionalización y las hipótesis que guían el análisis.

En este estudio se adopta un enfoque cuantitativo, ya que favorece la medición precisa de las variables y la obtención de resultados verificables, lo que contribuye a identificar patrones y establecer relaciones estadísticas en la investigación. A través del análisis estadístico, se busca establecer relaciones claras entre las variables definidas, proporcionando evidencia que facilite la toma de decisiones orientadas a robustecer la protección de la información sensible de la organización. Asimismo, se podrá profundizar sobre las dificultades que enfrenta el personal durante el proceso de capacitación y demás factores organizacionales que tienen relación con el problema de investigación lo que permitirá comprender de forma más detallada el entorno operativo, permitiendo identificar causas, percepciones y dinámicas internas en la organización.

Derivado del enfoque adoptado, el tipo de investigación para este estudio se clasifica como descriptivo y correlacional. Es descriptivo porque busca detallar las características actuales de los programas de capacitación utilizados por Grupo Vesta SPS, su frecuencia, metodologías, alcance y nivel de recepción del personal y los errores humanos más frecuentes a los que están expuestos. También es correlacional, ya que tiene como objetivo determinar si existe una relación entre los métodos de formación impartidos y la disminución de errores humanos que comprometen la información sensible. Este tipo de diseño permite analizar el comportamiento de ambas variables y evaluar su conexión sin manipularlas directamente.

"El término diseño se refiere al plan o estrategia concebida para obtener la información que se desea" (Sampieri et al., 2010, p. 162). El diseño seleccionado para esta investigación es no experimental, ya que el fin de la investigación es analizar la relación entre los métodos de capacitación implementados y la ocurrencia de errores humanos vinculados a la pérdida de información sensible sin manipular las variables identificadas, mediante este enfoque los resultados serán analizados en el entorno en el que se presentan en Grupo Vesta SPS, de modo que estos reflejen las técnicas de capacitación que utilizan actualmente y los errores humanos más frecuentes que ha experimentado la empresa. Así mismo el instrumento para la recolección de la información utilizado es el cuestionario, diseñado en escalas tipo Likert lo que servirá apoyo a obtener datos que permitan cuantificar, analizar la información obtenida.

Figura 8.Enfoque y métodos de investigación.
Fuente: Elaboración propia.

3.3 DISEÑO DE LA INVESTIGACIÓN

Constituye el plan estratégico que guía el desarrollo del estudio, una vez identificado el problema de investigación se delimitó el alcance del estudio y, con base a esta definición, se plantearon las hipótesis correspondientes, orientadas a dar respuesta a las preguntas de investigación y a lograr el cumplimiento de los objetivos establecidos. Para llevar a cabo el diseño de esta investigación es necesario tomar en cuenta la población, muestra, unidad de análisis y unidad de respuesta. El propósito es garantizar la validez, confiabilidad y coherencia metodológica asegurando que los resultados obtenidos respondan de manera precisa a los objetivos planteados. En síntesis, el diseño actúa como un esquema estructurado que orienta el proceso investigativo de manera sistemática y rigurosa.

3.3.1 POBLACIÓN

"Una población es el conjunto de todos los casos que concuerdan con una serie de especificaciones" (Hernández Sampieri & Fernández-Collado, 2014). Es decir, el conjunto total de individuos u objetos que comparten características relevantes para el estudio. La función principal es definir el alcance del estudio ya que establece a quiénes o a qué se dirigen los resultados de la investigación. Además, es la base para la selección de la muestra. El propósito principal es garantizar que el estudio se enfoque en un grupo claramente delimitado, coherente con el problema, y los objetivos de la investigación, así mismo, busca asegurar que las conclusiones derivadas del análisis respondan a las variables estudiadas y aporten conocimiento válido y útil para la toma de decisiones, formulación de estrategias o el desarrollo de futuras investigaciones.

Para este estudio se cuenta con una población finita de 112 empleados, en Grupo Vesta ubicada en San Pedro Sula, quienes se distribuyen en las diferentes áreas, tal como se describe en la tabla 3.

Tabla 4.Distribución de áreas de colaboradores en Grupo Vesta SPS.

Megamall	Área	Área Crítica
Total 112	Torre de control OB	
	Torre de Control IB	
	Opex	X
	Comercial	
	IT	X
	Créditos y cobros	X
	Facturación	X
	Recursos humanos	X
	Trading	
	Administración	X
	Marítimo	
	SIIA	
	PUMA	
	Permisos	

Fuente: Grupo Vesta SPS.

3.3.2 MUESTRA

"La muestra es un subgrupo de la población de interés sobre el cual se recolectarán datos, y que tiene que definirse y delimitarse de antemano con precisión, además de que debe ser representativo de la población" (Hernández Sampieri & Fernández-Collado, 2014). Esta surge a

partir de la imposibilidad práctica de estudiar poblaciones completas. Así mismo, como optimizar recursos, tiempo y costos, sin comprometer la precisión y confiabilidad de los resultados, permitiendo la recolección, el análisis y la interpretación de datos de forma eficiente.

Para el cálculo de la muestra de este estudio se desarrolla la siguiente fórmula para poblaciones finitas:

$$n = \frac{(Z^2 * N * p * q)}{e^2 * (N-1) + Z^2 * p * q}$$

n: Tamaño de la muestra que se quiere calcular

N: Tamaño de la población finita

Z: Nivel de confianza

p: Probabilidad a favor de que ocurra un evento

q: Probabilidad en contra o de que no ocurra un evento

e: Margen de error máximo aceptado

Nivel de confianza de: 95%

N= 112

Z= 1.95

p= 50%

q= 50%

$e \leq 0.05$

$$n = \frac{1.95^2 * 0.5 * 0.5 * 112}{0.05^2 * (112-1) + 1.95^2 * 0.5 * 0.5}$$

$$n = \frac{106.47}{1.2281}$$

n= 87.00

La población seleccionada es de 112 colaboradores y el total de la muestra es de 87 unidades de muestreo.

Cobertura de la investigación = muestra/población
87/112 = 0.776

La cobertura de la investigación es de 78 %.

3.3.3 TÉCNICAS DE MUESTREO

La función principal de las técnicas de muestreo es garantizar la selección adecuada de la muestra, de modo que ésta refleje las características relevantes de la población, por lo tanto, asegura la representatividad y pertinencia de la muestra contribuyendo a que los resultados sean confiables.

El tipo de muestra utilizado en esta investigación es el probabilístico aleatorio simple, ya que todos los colaboradores tienen la misma probabilidad de ser elegidos, la muestra fue obtenida utilizando la fórmula para poblaciones finitas.

3.4 TÉCNICAS, INSTRUMENTOS Y PROCEDIMIENTOS APLICADOS

El objeto de estudio está definido para el personal de las áreas consideradas como críticas dentro de Grupo Vesta SPS, quienes participan en los procesos de capacitación y que manejan información sensible en sus operaciones diarias. Este grupo de colaboradores será de gran relevancia para la investigación, ya que sus percepciones y experiencias permitirán evaluar de forma más precisa la efectividad de los métodos de capacitación implementados y su influencia en la ocurrencia de errores humanos asociados a la pérdida de información sensible. Así mismo se consideró el personal encargado de gestionar los incidentes de seguridad que se presentan en la organización ya que su conocimiento técnico y su participación en la atención de eventos de riesgo y los contenidos de las capacitaciones que se imparten aportan una perspectiva complementaria, para comprender las causas de dichos incidentes relacionados con el error humano.

3.4.1 TÉCNICAS

En base al enfoque establecido, los objetivos y las variables de investigación, las técnicas utilizadas en la presente investigación se enfocan en la aplicación de encuestas. La encuesta apoyará en la recolección de información ordenada de la población definida consultando de forma individual la misma información al objeto de estudio que como anteriormente se mencionó son los empleados de áreas críticas en Grupo Vesta SPS. Esta técnica nos brindará datos cuantitativos que apoyaran a realizar un análisis estadístico sobre información relevante enmarcado en las variables de métodos de capacitación y errores humanos relacionados con la pérdida de información.

Complementando lo anterior, la aplicación del instrumento será en base a las capacitaciones que se imparten y los incidentes de seguridad que estén específicamente relacionados a errores humanos que han expuesto información sensible de la organización. La aplicación de esta técnica permitirá abordar desde varias perspectivas el problema de investigación y mediante el análisis de los resultados determinar si los métodos de capacitación aplicados al personal influyen verdaderamente en la reducción del error humano.

3.4.2 INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Conforme a la técnica seleccionada, se aplicará mediante un cuestionario estructurado el cual está conformado por un conjunto de preguntas elaboradas a partir de las dimensiones e indicadores obtenidos en el proceso de operacionalización de las variables, lo que asegura su alineamiento con los objetivos de investigación. Para el cuestionario se utilizó el método de medición de escala Likert de cinco puntos que mediante una lista de opciones el colaborador podrá seleccionar la respuesta que mejor se adapte a su experiencia y percepción relacionadas a las variables métodos de capacitación de los empleados y los errores humanos que provocan la fuga de información sensible. Este instrumento de recolección de datos fue seleccionado debido a que se pretende obtener datos cuantificables que permitan realizar un análisis, comparación y estadísticas de las respuestas brindadas por los colaboradores de Grupo Vesta SPS. Esto resulta fundamental para comprobar las hipótesis planteadas, su estructura clara y secuencial garantiza que los colaboradores puedan responder de forma fácil y rápida, disminuyendo posibles sesgos y aumentando la fiabilidad de los datos obtenidos. El diseño del instrumento seleccionado se fundamentó en la necesidad de recopilar información precisa que facilite la detección de patrones, tendencias y asociaciones entre las variables previamente definidas.

3.4.3 PROCEDIMIENTOS

Para la aplicación del instrumento de recolección de datos Encuesta, se notificará al encargado del departamento de TI para definir el día en que se aplicará el cuestionario a los colaboradores seleccionados según el departamento al que pertenecen. Se informará a los colaboradores de Grupo Vesta SPS sobre los objetivos del estudio y la naturaleza confidencial de su participación en la encuesta a aplicar. Posteriormente, el cuestionario estructurado será aplicado de manera digital, según la disponibilidad del personal, proporcionando instrucciones claras para responder cada pregunta planteada. Una vez completados los cuestionarios será validado la

cantidad de respuestas recibidas conforme a la muestra seleccionada verificando que todos los colaboradores seleccionados hayan respondido el cuestionario. Posteriormente los resultados obtenidos de los cuestionarios aplicados serán revisados, organizados, preparados, analizados y trabajados de forma cuantitativa. Finalmente serán integrados para fortalecer la comprensión del fenómeno estudiado y aportar evidencia que permita validar las hipótesis planteadas.

3.5 FUENTES DE INFORMACIÓN

Según la Universidad de Minnesota (2025), las fuentes de información son los documentos, registros o recursos que contienen datos, evidencias o conocimientos utilizados como soporte para construir, analizar y comunicar el conocimiento científico dentro de una investigación. Estas fuentes se clasifican según el grado de originalidad y proximidad al fenómeno estudiado, lo que permite seleccionar material adecuado para responder a las preguntas de investigación y garantizar la validez y fiabilidad de los resultados.

3.5.1 FUENTES PRIMARIAS

Para la Universidad de Nueva Gales del Sur (2025), las fuentes primarias son aquellas que presentan información original y directa sobre las variables o fenómenos estudiados, generada por los propios investigadores en el momento que ocurre la investigación. Por lo tanto, constituyen la información de primera mano, es decir, que contiene datos y resultados originales, incluye metodología detallada, datos, análisis y conclusiones de primera mano.

En este estudio se recopilaron datos a través de las encuestas digitales aplicadas a los colaboradores de Grupo Vesta SPS con el fin de determinar los métodos de capacitación que influyen en la reducción de errores humanos en la pérdida de información sensible.

3.5.2 ÉTICA DE LA INVESTIGACIÓN

“La ética de la investigación tiene el fin de proteger los derechos, la integridad y la confidencialidad de los participantes en investigaciones. La integridad científica se refiere a la conducta responsable en la investigación” (Espinoza & Alger, 2020). Básicamente es el conjunto de principios, normas y valores que orientan la conducta del investigador durante las etapas de

proceso investigativo, con el fin de garantizar el respeto, la integridad y la dignidad de las personas, organizaciones o unidad de análisis involucradas. En el desarrollo de esta investigación, la ética implica el uso honesto de la información brindada, la protección de datos obtenidos, el respeto a la confidencialidad y el consentimiento informado de los colaboradores, evitando cualquier forma de daño, manipulación o uso indebido de la información. Por ende, se ha reconocido adecuadamente las fuentes consultadas y se ha evitado el plagio, para mantener la objetividad en el análisis e interpretación de los datos.

3.5.3 LIMITACIONES

Algunas limitaciones para el estudio que deben ser consideradas al momento de interpretar resultados, son: En primer lugar, la investigación se circunscribe al análisis de los métodos de capacitación aplicado a Grupo Vesta San Pedro Sula, lo cual puede restringir la generalización de los hallazgos en otra organización con características, políticas de seguridad y niveles de madurez en ciberseguridad diferente. Asimismo, el uso de instrumentos de recolección de datos basado en la encuesta puede influir en la objetividad de la respuesta en temas relacionados con errores humanos y manejo de información sensible.

Otra limitación relevante se relaciona con factores externos como la cultura organizacional, el nivel previo de conocimientos en seguridad de la información y el grado de cumplimiento de políticas internas, pueden influir en los resultados y no ser totalmente controlados dentro del alcance del estudio. El reconocimiento de estas limitaciones permite delimitar el alcance de la investigación, al mismo tiempo que permite abrir la posibilidad a futuras investigaciones que profundicen en la comparativa de métodos de capacitación en la reducción de errores humanos asociados a la pérdida de información sensible.

CAPÍTULO IV: RESULTADOS Y ANÁLISIS

En el presente capítulo se detallan los resultados obtenidos a partir de la aplicación del instrumento de recolección de datos (encuesta), diseñado específicamente para evaluar la influencia de los métodos de capacitación del personal en la reducción del error humano y la pérdida de información sensible en Grupo Vesta SPS, 2026. En este apartado también se presentan, los resultados y hallazgos derivados del análisis de las variables, independiente, correspondiente a los métodos de capacitación implementados en Grupo Vesta SPS y la variable dependiente, relacionada a la ocurrencia de errores humanos asociados a la pérdida de información sensible.

Los resultados se presentan en función de las variables de estudio definidas, así también se detallan las tablas y representaciones gráficas que apoyan al entendimiento e interpretación de los resultados obtenidos, permitiendo exponer la información con claridad, precisión y transparencia. Seguidamente, se realiza un análisis detallado donde se identificarán tendencias, patrones, y asociaciones con el fin de determinar si los métodos de capacitación aplicados por Grupo Vesta SPS inciden de forma significativa en la disminución de incidentes atribuibles a error humano que permite la exposición de la información sensible de la organización, de esta forma contrastar las hipótesis definidas.

4.1 INFORME DE PROCESO DE RECOLECCIÓN DE DATOS.

El proceso de recolección de datos se desarrolla en relación con el enfoque metodológico cuantitativo adoptado para esta investigación, para ello se elaboró un instrumento tipo cuestionario en relación con las variables de estudio y sus dimensiones operacionales donde se incluyeron diferentes preguntas utilizando preguntas cerrada y de escala Likert diseñadas para recolectar información valiosa y de relevancia para la investigación.

La población estuvo conformada por colaboradores de diferentes áreas de la empresa Grupo Vesta en San Pedro Sula que tienen acceso a información institucional. El instrumento se aplicó a 87 colaboradores de la empresa, mediante un cuestionario en línea del cual se obtuvo 100% de respuesta según la muestra definida, lo que permitió la recolección, procesamiento y análisis de la información mediante diferentes técnicas que permitieron medir el comportamiento de las variables de la investigación y determinar si existe relación entre ellas.

4.2 RESULTADOS Y ANÁLISIS DE LAS TÉCNICAS APLICADAS.

En el siguiente apartado se presentan y analizan los resultados obtenidos a partir de la aplicación del instrumento de investigación a los colaboradores de Grupo Vesta SPS, esta sección tiene como fin interpretar y analizar la información recopilada. El análisis se efectúa bajo un enfoque cuantitativo, apoyado en herramientas estadísticas que permitirán detectar patrones y relaciones entre las variables de investigación, con la finalidad de determinar si existe relación entre los métodos de capacitación implementados en la organización y la reducción del error humano asociado con la pérdida de información sensible.

Tabla 5. Estadística de Fiabilidad

Alfa de Cronbach	N de elementos
,813	38

Fuente: Datos obtenidos de la aplicación de instrumento mediante SPSS.

En la tabla anterior se observa la prueba de fiabilidad aplicada al instrumento de investigación, realizada mediante la estadística de fiabilidad de Alfa de Cronbach, el resultado muestra un valor de 0.813 para un total de 38 ítems. Este resultado indica que el instrumento posee alta fiabilidad, lo que se traduce a que las preguntas presentan coherencia y miden correctamente el tema de investigación sobre si los métodos de capacitación y su influencia en la reducción del error humano asociado con la pérdida de información sensible. De acuerdo con Sampieri et al., la confiabilidad se refiere al grado en que un instrumento produce resultados consistentes (Pág. 2024). Para escalas tipo Likert, el coeficiente Alfa de Cronbach es uno de los indicadores más utilizados para medir la fiabilidad de un cuestionario para este estudio se consideró valores aceptables superiores a 0.70.

ESTADÍSTICAS DESCRIPTIVAS

Figura 9.Género
Fuente: Elaboración propia.

El gráfico muestra la distribución de los encuestados según el género dentro de la muestra obtenida. Se observa que el 57% corresponde al género femenino, mientras que el 42% pertenece al género masculino. Estos resultados indican una mayor participación de colaboradores mujeres en el estudio, aspecto de relevancia para la interpretación de los resultados relacionados con la percepción de los métodos de capacitación y las conductas asociadas al manejo de información sensible. Sheng et al., (2010) en su estudio para estudiar tanto la relación entre demografía y susceptibilidad al phishing, los resultados sugieren que las mujeres son más susceptibles que los hombres al phishing (Pág. 1). Estas diferencias no deben atribuirse exclusivamente al género, si no a factores contextuales como el tipo de funciones desempeñadas.

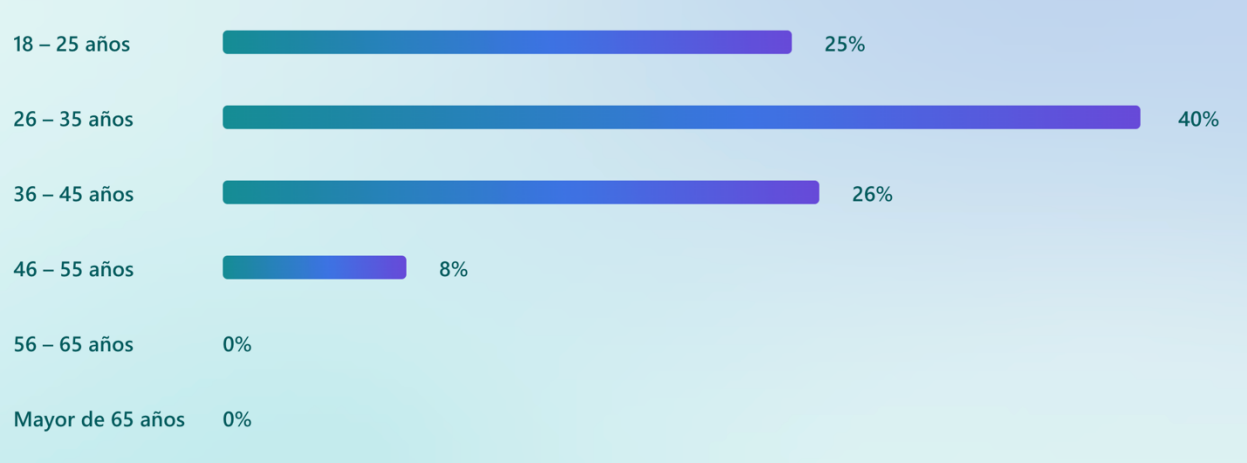


Figura 10.Edad
Fuente: Elaboración propia.

El gráfico presenta la distribución de los encuestados según el rango de edad. Se observa que el 40% de los encuestados se encuentra en un rango de 26 a 35 años, seguido por un 26% en el rango de 36 a 45 años y un 25% entre 18 y 25 años. Por su parte el 8% corresponde al grupo de 46 a 55 años, mientras que no se registraron participantes en los rangos de 56 a 65 ni mayores a 65 años. Estos resultados evidencian que la mayor concentración de la muestra se encuentra en edades comprendidas entre los 26 y 35 años, lo que indica una población predominantemente joven.

Los resultados obtenidos reflejan la percepción y comportamiento de colaboradores en etapas joven-adulta. En este sentido, estudios previos han demostrado que el error humano es más asociado a factores como condiciones de trabajo y el entorno organizacional (Báez et al., 2013, p. 1), por lo tanto, aunque la predominancia de una población joven podría influir en aspectos como la familiaridad con herramientas digitales, no se puede afirmar que la edad sea un factor determinante en la reducción o incremento del error humano.

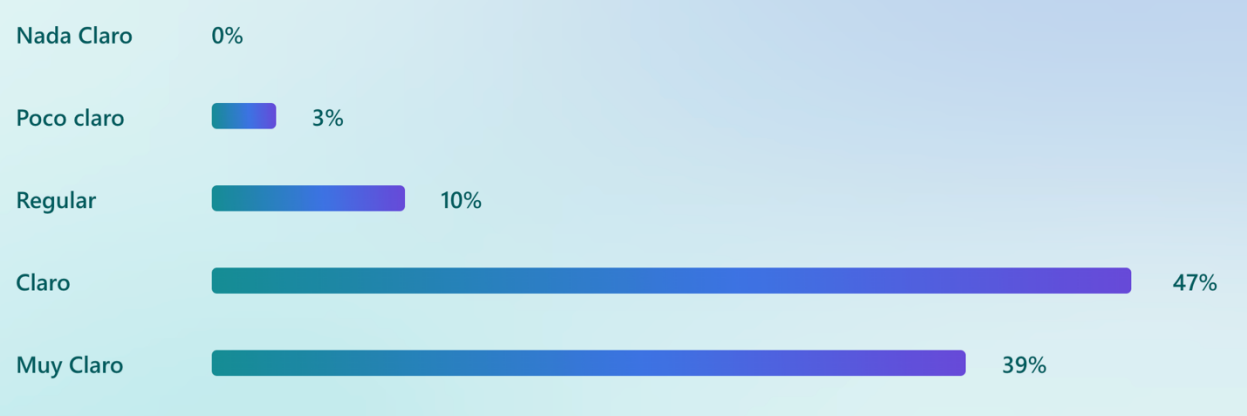


Figura 11. ¿En qué medida considera que el contenido de las capacitaciones en seguridad de la información es claro y fácil de comprender?
Fuente: Elaboración propia.

El gráfico presenta la percepción de los colaboradores respecto a la claridad y comprensión del contenido de las capacitaciones en seguridad de la información. El 47% indicó que el contenido es claro, el 39% muy claro evidenciando que el 86% de los encuestados percibe de forma positiva la claridad del material impartido.

Estos resultados evidencian una percepción favorable con relación a la claridad del contenido impartido, lo que permite inferir que el material de capacitación es comprensible para la mayoría de los colaboradores. Diversos estudios han demostrado que la calidad y claridad de la

información en los procesos informativos influyen en la retención del conocimiento y la reducción de errores operativos. (Kruger & Kearney, 2016, p. 1). En este sentido, los resultados son coherentes con la literatura, ya que una alta percepción de claridad en las capacitaciones puede favorecer la modificación de hábitos.

Asimismo, es importante considerar que la claridad del contenido no solo facilita la comprensión inmediata, sino que también incide en la capacidad de los colaboradores para aplicar correctamente los conocimientos adquiridos en situaciones reales de trabajo, especialmente en el manejo de información sensible.

De igual manera, un contenido claro reduce la ambigüedad en la interpretación de las políticas de seguridad, lo cual disminuye la probabilidad de cometer errores involuntarios, como la divulgación inadecuada de información o el incumplimiento de protocolos establecidos.

En relación con el objetivo general del estudio, estos resultados sugieren que los métodos de capacitación implementados presentan condiciones favorables para influir en la reducción del error humano; sin embargo, esta relación debe analizarse en conjunto con otros factores como la frecuencia de capacitación y los métodos utilizados.

Finalmente, aunque los resultados son positivos, la presencia de un 13% de colaboradores que perciben el contenido como regular o poco claro evidencia oportunidades de mejora en el diseño instruccional, lo que implica la necesidad de reforzar estrategias pedagógicas que aseguren la comprensión total del contenido por parte de todos los participantes.

Figura 12. ¿El contenido de las capacitaciones en seguridad de la información es relevante para mis actividades diarias dentro de la organización?
Fuente: Elaboración propia.

El gráfico presenta la percepción de los colaboradores respecto a la relevancia del contenido de las capacitaciones en seguridad de la información para sus actividades diarias dentro de la organización. Los resultados muestran que un 48% de los encuestados está de acuerdo y otro

48% totalmente de acuerdo, lo que representa un 96% de valoración positiva sobre la pertinencia del contenido formativo. Por su parte, el 2% manifestó una población neutral y únicamente el 1% indicó estar totalmente en desacuerdo. Estos datos evidencian que la gran mayoría de los participantes considera que las capacitaciones están alineadas con sus funciones laborales.

En relación con la investigación, la relevancia del contenido constituye un elemento clave en la efectividad de los métodos de capacitación, ya que facilita la transferencia del conocimiento al contexto laboral. Un estudio destaca que los programas de concienciación deben estar alineados con las tareas reales de los empleados para influir en su comportamiento y cumplimiento de políticas de seguridad (T. Siponen, 2000, p.1). En este sentido, la literatura indica que la capacitación en seguridad de la información es más efectiva cuando el contenido es percibido como relevante y aplicable por los usuarios, lo que incrementa la conciencia y reduce los errores

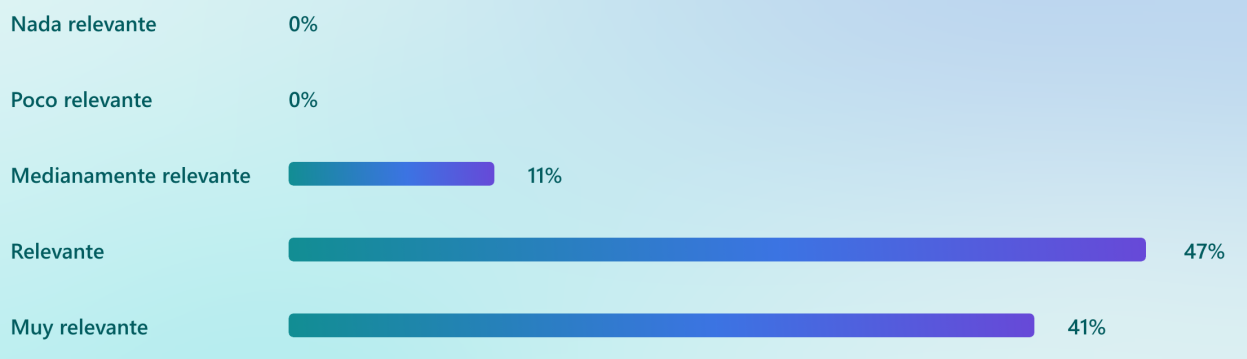


Figura 13.¿Qué tan relevantes considera los temas abordados durante las capacitaciones?
Fuente: Elaboración propia.

El gráfico muestra la percepción de los colaboradores respecto al nivel de relevancia de los temas abordados durante las capacitaciones en seguridad de la información. Se observa que el 47% considera los temas relevantes y el 41% muy relevantes, lo que representa un 88% de valoración positiva. Asimismo, el 11% indicó que los contenidos son medianamente relevantes, mientras que no se registraron respuestas en las categorías nada relevante ni poco relevante. Estos resultados evidencian que los temas impartidos responden de forma adecuada a las necesidades del personal y que esta se encuentra alineada con las responsabilidades de la organización. En este sentido, la literatura señala que la efectividad de los programas de capacitación en seguridad depende en gran medida de que los usuarios perciban el contenido como útil y aplicable a sus funciones, pero también aclara que la capacitación por sí sola no elimina los errores humanos, siendo necesario complementar con controles organizacionales y técnicos (Wilson & Hash, 2003). No obstante, a

pesar de que el contenido es percibido como relevante, esto no garantiza por sí mismo la reducción del error humano.

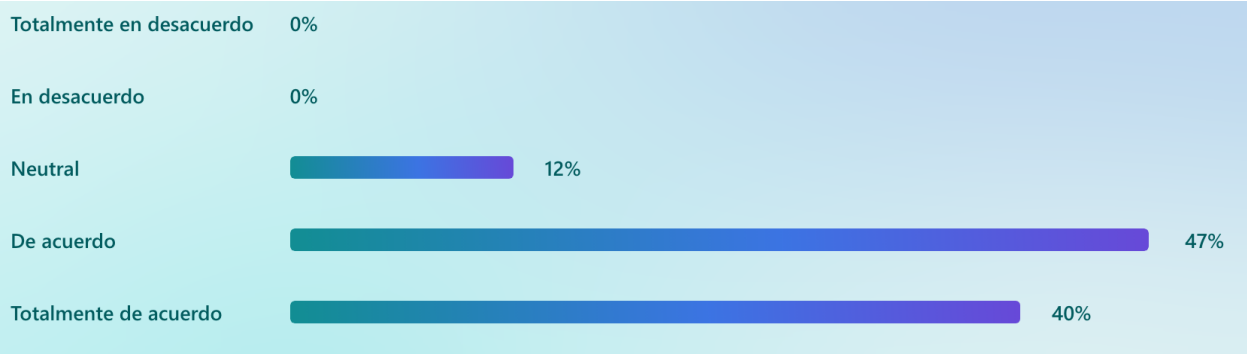


Figura 14.¿Las sesiones de capacitación incluyeron explicaciones sobre errores humanos comunes y cómo evitarlos?
Fuente: Elaboración propia

En el gráfico se presenta la percepción de los colaboradores respecto a si las sesiones de capacitación incluyeron explicaciones sobre errores humanos comunes y cómo evitarlos. Los resultados evidencian que el 47% de los encuestados están de acuerdo y el 40% totalmente de acuerdo, lo que representa un 87% de valoración positiva. Por su parte el 12% manifestó una posición neutral y no se registraron respuestas en las categorías de desacuerdo y totalmente en desacuerdo. Por lo tanto, los resultados demuestran que los programas formativos incorporan contenidos orientados a la prevención de errores humanos.

Estos resultados se vinculan con los objetivos de la investigación ya que la inclusión de este tipo de contenidos constituye una estrategia preventiva dentro del proceso de capacitación. En este sentido Parsons et al., (2014) destacan que la formación es más efectiva cuando no sólo transmite conocimiento, sino que también influye en la actitud y el comportamiento del usuario (pág. 1).

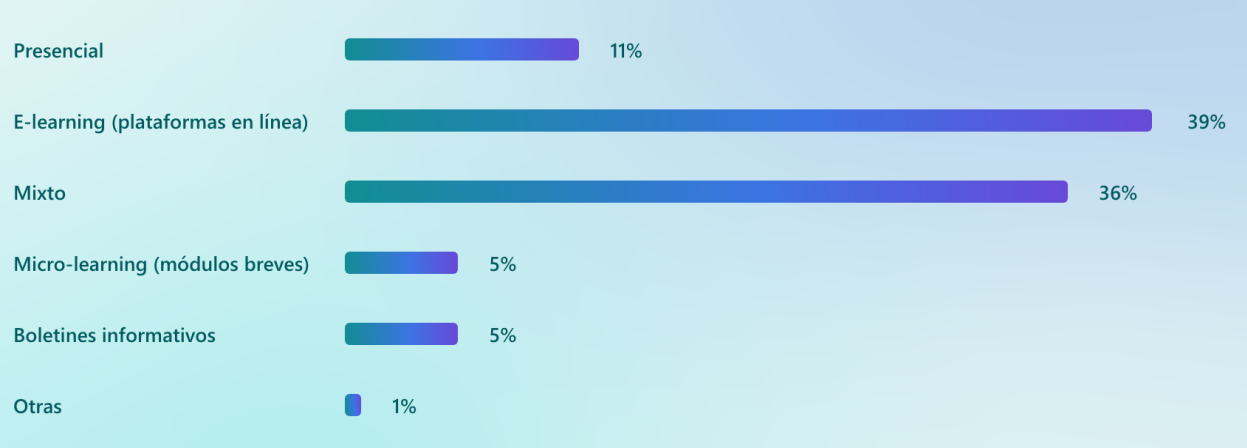


Figura 15. ¿Qué modalidad predominó en las capacitaciones que recibió?
Fuente: Elaboración propia.

El gráfico presenta la modalidad predominante de capacitación recibida por los colaboradores en materia de seguridad de la información. Se observa que el 39% indicó que la modalidad principal fue e-learning (Plataforma en línea), seguido por un 36% que señaló modalidad mixta y un 11% capacitación presencial. Por su parte el 5% manifestó haber recibido micro-learning y otro 5% boletines informativos, mientras que únicamente el 1% seleccionó otras modalidades. Estos resultados evidencian que las estrategias formativas implementadas se orientan principalmente hacia otros entornos digitales y combinados, priorizando metodologías flexibles y apoyadas en tecnología.

En relación con los objetivos de investigación, estos resultados responden directamente al objetivo de enumerar los métodos de capacitación implementados, constituyendo un insumo clave ya que permite analizar posteriormente si estos métodos influyen en la reducción del error humano asociado a la pérdida de información sensible. Investigaciones como Ghahramani et al., (2024) señalan que las modalidades de capacitación basadas en entornos digitales facilitan la difusión del conocimiento (pág. 1), sin embargo, su efectividad depende mucho del nivel de interacción, su diseño y sobre todo el refuerzo continuo.

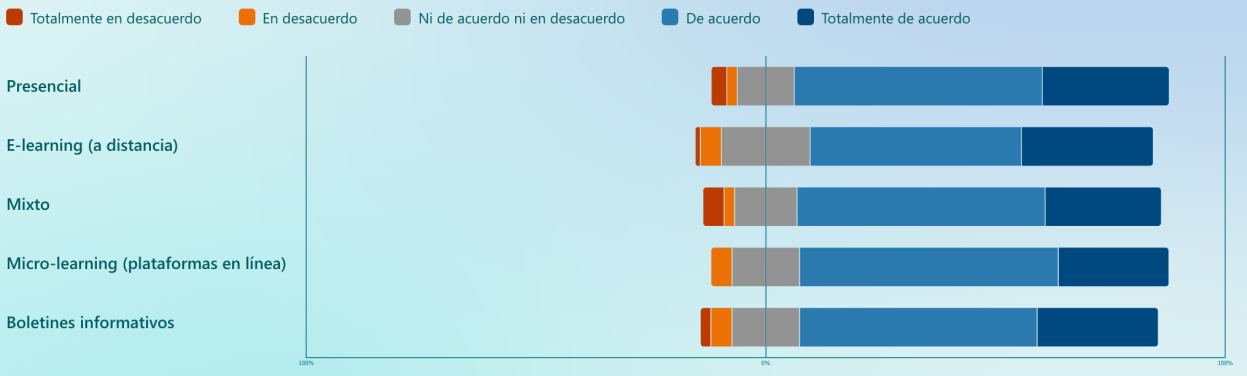


Figura 16. ¿Para cada una de las siguientes modalidades de capacitación, indique su nivel de acuerdo según el grado en que está facilitó su aprendizaje?
Fuente: Elaboración propia

El gráfico presenta el nivel de acuerdo de los colaboradores respecto al grado en que cada modalidad de capacitación facilitó su aprendizaje en materia de seguridad de la información. En todas las modalidades evaluadas, presencial, e-learning, mixta, micro-learning y boletines informativos, predomina la valoración positiva concentrándose principalmente en las categorías de acuerdo y totalmente de acuerdo. Las modalidades e-learning y mixta evidencian altos niveles de aceptación al igual que micro-learning y boletines informativos, mientras que las respuestas en desacuerdo representan una proporción mínima en cada caso.

Los resultados indican que las modalidades presentadas contribuyen a su proceso de aprendizaje, lo que lo vincula con el objetivo general de evaluar los métodos de capacitación, ya que evidencia que las modalidades implementadas son percibidas como facilitadoras del aprendizaje, estos resultados evidencian que estos métodos de capacitación son útiles para el aprendizaje de los colaboradores.

Asimismo, la predominancia de valoraciones positivas en modalidades digitales y combinadas sugiere una transición hacia entornos de aprendizaje más flexible y adaptativos, donde los colaboradores pueden gestionar su propio ritmo de aprendizaje y acceder a los contenidos en función de las necesidades laborales. Esto es especialmente relevante en el contexto de la seguridad de la información, donde la actualización constante del conocimiento es fundamental debido a la evolución continua de las amenazas.

En este sentido, diversos estudios señalan que el aprendizaje es más efectivo cuando se emplean múltiples modalidades y se promueve la interacción activa de los usuarios con el contenido, lo cual mejora tanto la comprensión como la retención del conocimiento (Towards an Innovative Model for Cybersecurity Awareness Training, 2024).

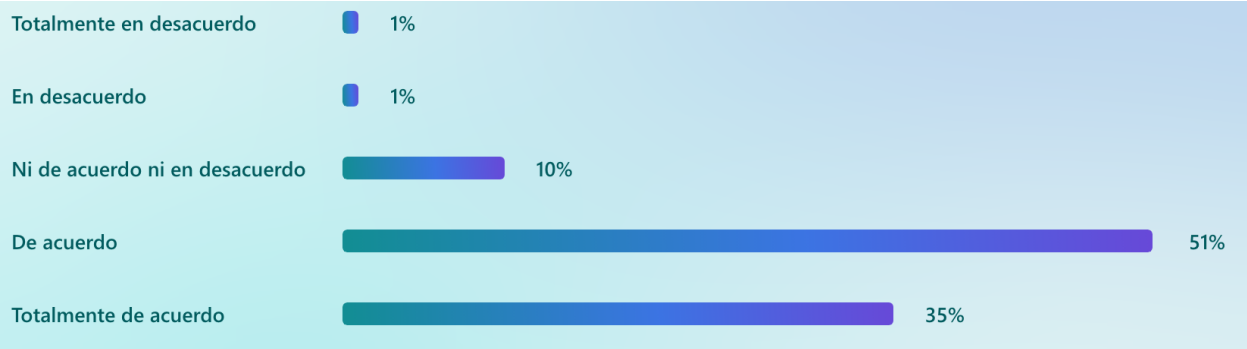


Figura 17.¿La duración de las sesiones fue adecuada para comprender la información presentada?
Fuente: Elaboración propia.

El gráfico muestra la percepción de los colaboradores respecto a si la duración de las sesiones de capacitación fue adecuada para comprender la información presentada. Los resultados indican que el 51% está de acuerdo y el 35% totalmente de acuerdo, lo que representa un 86% de valoración positiva sobre el tiempo asignado a las capacitaciones. Por su parte el 10% manifestó una posición neutral, mientras que únicamente el 1% indicó en desacuerdo y otro 1% totalmente en desacuerdo. En términos generales la extensión de las sesiones resulta suficiente para facilitar la comprensión del contenido relacionado con la seguridad de la información.

Estos resultados se vinculan con los objetivos de investigación, ya que la duración de las sesiones constituye un elemento clave dentro del diseño metodológico de la formación. Paas & . van Merriënboer4 (2020) indica que la duración de las sesiones de capacitación influye en la atención, la retención del conocimiento y la carga cognitiva del usuario, ya que un diseño inadecuado puede generar sobrecarga en la memoria de trabajo y afectar el aprendizaje (pág. 3).

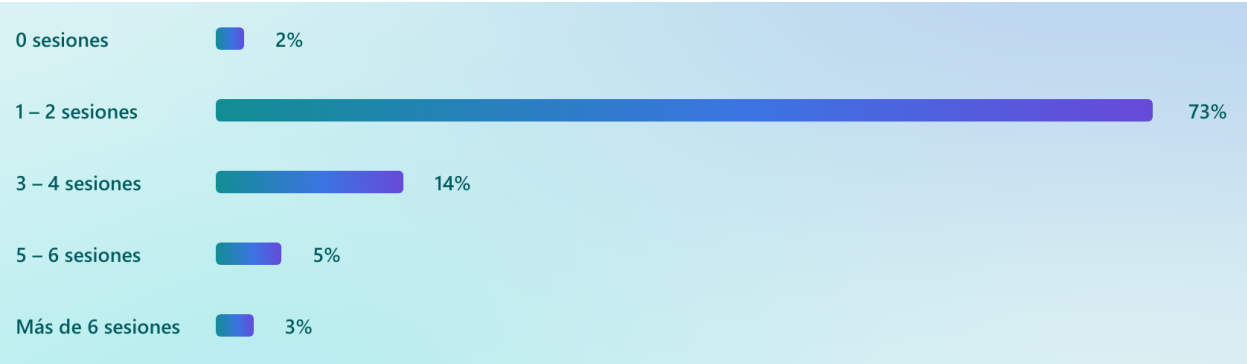


Figura 18. ¿Cuántas sesiones o módulos de capacitación en seguridad de la información recibió en los últimos 12 meses?
Fuente: Elaboración propia.

El gráfico presenta la cantidad de sesiones o módulos de capacitación en seguridad de la información recibidos por los colaboradores durante los últimos 12 meses. Se observa que el 73% indicó haber recibido entre 1 y 2 sesiones, seguido por un 14% que reportó entre 3 y 4 sesiones. Por su parte, el 5% manifestó haber recibido entre 5 y 6 sesiones y el 3% más de 6 sesiones, mientras que un 2% señaló no haber recibido ninguna capacitación en el periodo evaluado. Estos resultados evidencian que la mayor parte del personal ha participado en al menos una capacitación anual.

La concentración de la mayoría de los colaboradores en el rango de 1 a 2 sesiones anuales sugiere que la capacitación podría no ser suficiente para generar cambios sostenidos en el comportamiento del usuario, este resultado, aunque descriptivo aporta un elemento relevante para el análisis de la hipótesis, ya que indica que aun cuando existen programas de capacitación, su frecuencia podría ser insuficiente para influir significativamente en la reducción del error humano.

En este sentido, la frecuencia de las capacitaciones constituye un factor crítico dentro de la efectividad de los programas de formación en seguridad de la información, ya que el aprendizaje y la modificación de conductas requieren procesos continuos de refuerzo y actualización.

Diversos estudios han señalado que las intervenciones esporádicas tienden a tener un impacto limitado en el comportamiento de los usuarios, mientras que los programas de capacitación recurrentes y sistemáticos favorecen la interiorización de buenas prácticas y la reducción de incidentes de seguridad.

De acuerdo con el Instituto Nacional de Estándares y Tecnología (Haney & Lutters, 2020), los programas de concienciación en ciberseguridad deben desarrollarse de manera continua y periódica para garantizar su efectividad, promoviendo cambios sostenibles en el comportamiento del personal.

En relación con el objetivo general de la investigación, estos hallazgos sugieren que, aunque los métodos de capacitación están presentes en la organización, su baja frecuencia podría limitar su impacto en la reducción del error humano asociado a la pérdida de información sensible.

Finalmente, la existencia de un porcentaje, aunque reducido, de colaboradores sin capacitación el 2%, representa un riesgo significativo para grupo Vesta SPS, ya que estos empleados pueden convertirse en un punto vulnerable dentro de la gestión de la seguridad de la información.

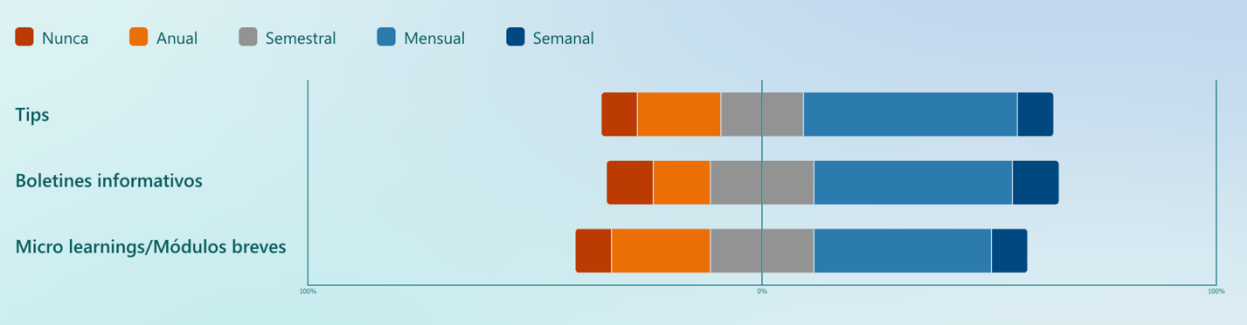


Figura 19. ¿Con qué frecuencia recibe recordatorios o materiales de refuerzo sobre buenas prácticas de seguridad?
Fuente: Elaboración propia.

El gráfico muestra la frecuencia con la que los colaboradores reciben recordatorios o materiales de refuerzo sobre buenas prácticas de seguridad, a través de tips, boletines informativos y micro-learnings o módulos breves. Se observa que en las tres modalidades predomina la frecuencia mensual, seguida en menor proporción por la frecuencia semanal y semestral, mientras que las opciones anuales y nunca presentan porcentajes reducidos. Estos resultados evidencian que la organización mantiene una formación continua de refuerzo, utilizando distintos canales para fortalecer el aprendizaje.

No obstante, aunque la frecuencia mensual representa un esfuerzo sostenido por parte de Grupo Vesta SPS, diversos enfoques en seguridad de la información sugieren que los recordatorios más frecuentes, como los semanales, tienden a generar una mayor retención del conocimiento y una respuesta más automática ante riesgos, especialmente en entornos donde las amenazas evolucionan constantemente.

Estos resultados se vinculan con los objetivos planteados ya que permiten analizar no solo qué métodos se utilizan, sino también con qué frecuencia se aplican, asimismo este resultado aporta evidencia relevante para el análisis de la hipótesis, ya que indica que, aunque existen estrategias de capacitación recurrentes, su intensidad podría no ser suficiente para generar cambios sostenidos en el comportamiento de los colaboradores.

En relación con el objetivo general de la investigación, la frecuencia de los recordatorios constituye un componente clave dentro de la efectividad de los métodos de capacitación, ya que el esfuerzo periódico facilita la internalización de hábitos seguros y disminuye la probabilidad de errores humanos asociados al manejo de información.

El NIST señala que la capacitación en seguridad debe mantenerse de forma constante para fortalecer las prácticas seguras en el tiempo, lo que sugiere la necesidad de fortalecer la continuidad y frecuencia de estas actividades para lograr un mayor impacto en la reducción del error humano.

De acuerdo con el Instituto Nacional de Estándares y Tecnología Haney & Lutters (2020),destacan que los programas de concienciación en seguridad deben ir más allá de sesiones aisladas, incorporando mecanismos continuos de refuerzo como recordatorios, campañas y micro capacitaciones, los cuales contribuyen a mantener la atención del usuario y a consolidar comportamientos seguros a largo plazo.

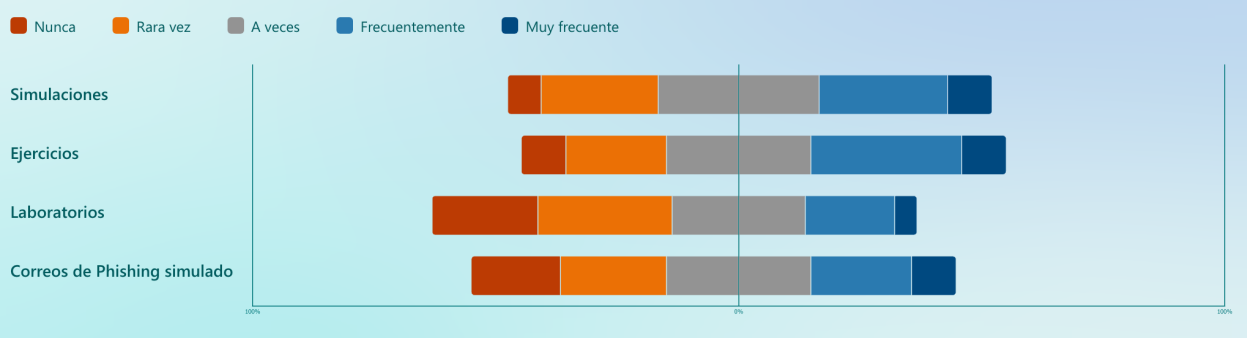


Figura 20. En las capacitaciones recibidas, ¿con qué frecuencia se incluyeron actividades prácticas?
Fuente: Elaboración propia.

El gráfico presenta la frecuencia con la que incluyeron actividades prácticas en las capacitaciones recibidas, tales como simulaciones, ejercicios, laboratorios y correos de phishing simulado. Se observa que las actividades de simulación y ejercicios muestran una mayor concentración en las categorías frecuentemente y muy frecuente, en contraste, los laboratorios y correos de phishing simulado presentan mayores porcentajes en las categorías Nunca y Rara vez, indicando una menor recurrencia de estas metodologías. Por lo tanto, la empresa prioriza las simulaciones y ejercicios como estrategias prácticas de aprendizaje, mientras que las demás se aplican con menos frecuencia.

La limitada implementación de laboratorios y simulaciones representa una debilidad significativa, considerando que estas metodologías permiten recrear escenarios reales de riesgo, este resultado permite realizar el análisis de la hipótesis, ya que, aunque existen refuerzos formativos, la falta de prácticas más especializadas podría limitar el impacto de la capacitación en la reducción del error humano. Estudios sobre concienciación en seguridad de la información

evidencian que las intervenciones educativas, incluyendo simulaciones de phishing, permiten reducir la susceptibilidad de los usuarios frente a ataques reales, al mejorar su capacidad de detección y respuesta (Sheng et al., 2010, p. 1). La literatura destaca que las metodologías prácticas, son altamente efectivas para reducir errores humanos ya que permiten a los usuarios experimentar situaciones reales y mejorar su capacidad de respuesta.

Figura 21. ¿En las capacitaciones recibidas se le aplicó una evaluación o prueba después de la capacitación? (p. ej. quiz, examen, post-test)
Fuente: Elaboración propia.

Los resultados en el gráfico presentado sobre evaluaciones después de capacitación indican que el 50% de los colaboradores afirmó que sí se aplicó una evaluación, mientras que el 49% señaló que no. Estos datos indican que las evaluaciones no constituyen una práctica estandarizada en todas las capacitaciones impartidas al personal de la organización. Estos resultados se vinculan con el objetivo general, ya que la aplicación de evaluaciones constituye un componente fundamental para medir la efectividad del aprendizaje, así mismo con el objetivo de identificar factores asociados al error humano, puesto que la ausencia de evaluación impide verificar si los colaboradores han comprendido correctamente los contenidos y si están en capacidad de aplicarlos en su entorno laboral.

Este resultado aporta evidencia relevante para el análisis de la hipótesis, ya que sugiere que, aunque se implementan programas de capacitación la falta de mecanismos sistemáticos de evaluación podría reducir su impacto en la disminución de error humano. En este sentido, el modelo de evaluación de la formación El Modelo Kirkpatrick (2024), establece que la medición de resultados es necesaria para determinar si la capacitación genera cambios en el comportamiento del individuo. Por lo tanto, los resultados evidencian que la falta de evaluación sistemática en las capacitaciones podría estar limitando la capacidad de la organización para verificar la efectividad de sus programas formativos.

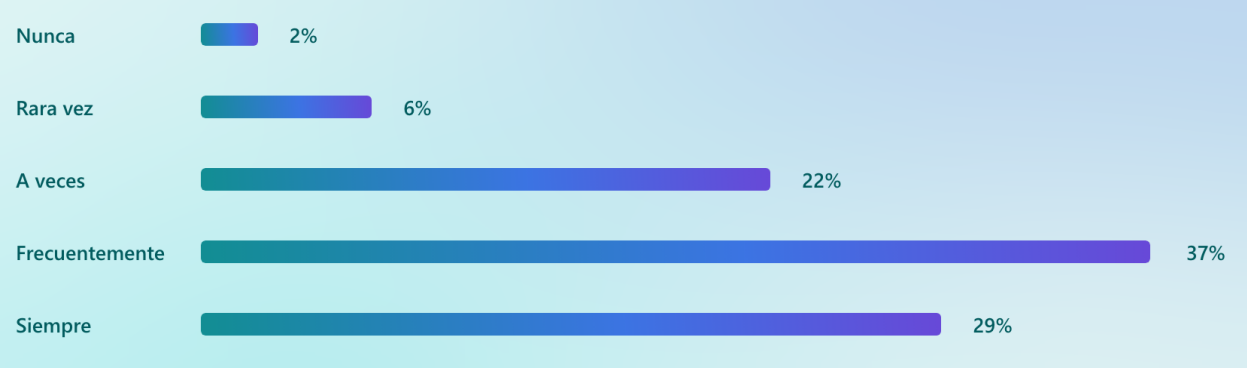


Figura 22. ¿Las capacitaciones incluyeron ejemplos o casos prácticos aplicables a su trabajo?
Fuente: Elaboración propia.

Se observa en el gráfico que el 37% indicó que estos se incluyeron frecuentemente y el 29% manifestó que siempre, lo que representa un 66% de valoración positiva en cuanto a la aplicación de casos prácticos, mientras que el 6% indicó rara vez y el 2% nunca. Estos resultados muestran que las capacitaciones del personal integran elementos prácticos orientados a la realidad laboral del personal. La inclusión de casos prácticos constituye un componente clave en la efectividad del aprendizaje, asimismo, el aprendizaje basado en situaciones reales facilita la comprensión de riesgos y la correcta toma de decisiones en el manejo de información sensible, por lo tanto tiene relación directa con los objetivos establecidos en la investigación así como también con la hipótesis planteada ya que si bien, existen refuerzos por integrar metodologías prácticas, estos no se aplican de manera uniforme ni sistemática, lo que podría limitar su impacto en la reducción del error humano. Diversos estudios han demostrado que las metodologías prácticas permiten anclar el aprendizaje y mejorar la transmisión del conocimiento (Meijer, 2019, p. 1).

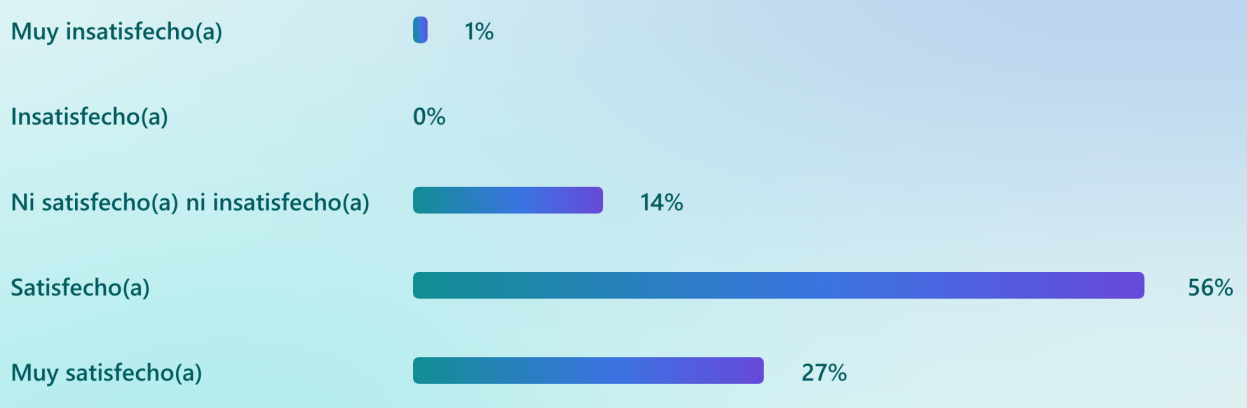


Figura 23. ¿Qué tan satisfecho(a) está con la calidad general de las capacitaciones recibidas?
Fuente: Elaboración propia.

El gráfico presenta el nivel de satisfacción de los colaboradores respecto a la calidad general de las capacitaciones recibidas en seguridad de la información. Se observa que el 56% manifestó estar satisfecho y el 27% muy satisfecho, lo que representa un 83% de valoración positiva. Asimismo, el 14% indicó una posición neutral, mientras que solo el 1% expresó estar muy insatisfecho y no se registraron respuestas en la categoría de insatisfecho.

En este contexto, el gráfico muestra que la mayoría de los colaboradores valora favorablemente las capacitaciones; sin embargo, este indicador corresponde a una evaluación de tipo reactiva, centrada en la experiencia del colaborador y no necesariamente en los resultados del aprendizaje o en cambios conductuales medibles.

En relación con el objetivo general de la investigación, enfocado en evaluar la influencia de los métodos de capacitación en la reducción del error humano, este resultado aporta información relevante sobre la aceptación del programa, pero resulta insuficiente para determinar su efectividad real sino se contrasta con indicadores de desempeño o incidencia de errores.

Asimismo, el 14% que contesto respuestas neutrales sugiere que existe un segmento de colaboradores que no percibe claramente la calidad o utilidad de las capacitaciones, lo que podría estar asociado a una desconexión entre los contenidos impartidos y las funciones específicas que desempeñan dentro de la organización.

Por otra parte, el hecho de que no exista valoraciones negativas significativas podría interpretarse como una fortaleza del programa de capacitación. Finalmente, estos resultados refuerzan la necesidad de complementar la evaluación de las capacitaciones con otros indicadores objetivos, como la frecuencia de participación, la claridad del contenido y la reducción de errores

humanos, con el fin de establecer una relación más precisa entre la formación recibida y su impacto en la seguridad de la información.

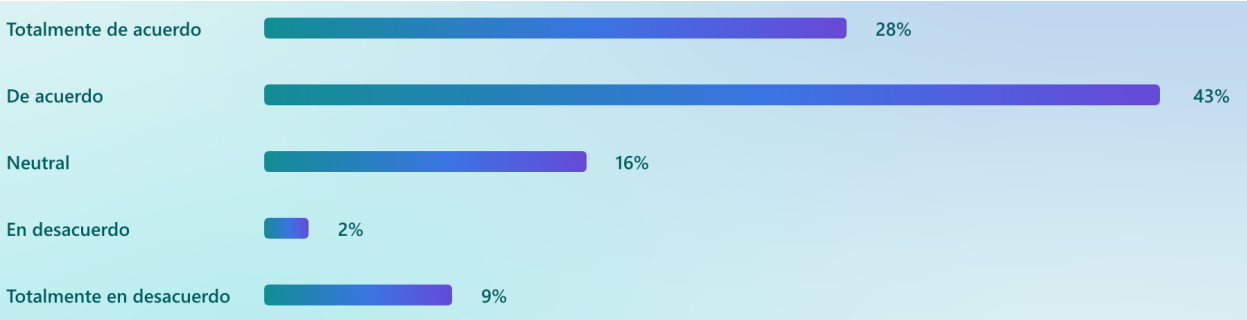


Figura 24. ¿Las capacitaciones modificaron mis hábitos o rutinas al manejar información sensible?
Fuente: Elaboración propia.

El gráfico presenta la percepción de los colaboradores respecto a si las capacitaciones recibidas modificaron sus hábitos o rutinas al manejar información sensible. Los resultados indican que el 43% está de acuerdo y el 28% totalmente de acuerdo, lo que representa un 71% de valoración positiva en cuanto al impacto conductual de la capacitación. Por su parte, el 16% manifestó una posición neutral, mientras que el 2% indicó estar en desacuerdo y el 9% totalmente en desacuerdo. Estos resultados indican que, para la mayoría del personal, las capacitaciones han generado cambios en sus prácticas relacionadas con la gestión de la información sensible. Estos resultados evidencian un posible impacto en el comportamiento del personal por lo que están estrechamente ligados con los objetivos e hipótesis planteadas en la investigación ya que un gran porcentaje de encuestados sugiere un impacto favorable en su comportamiento.

Parsons et al. (2014) establece en los resultados de su investigación que la concientización en seguridad se compone de conocimiento, actitud y comportamiento (Pág. 1). En este sentido, los resultados sugieren que las capacitaciones han logrado influir en el comportamiento de una parte importante del personal, no obstante, la presencia de un porcentaje considerable de colaboradores que no perciben cambios evidencia la necesidad de fortalecer las estrategias formativas con el fin de lograr una transformación conductual más uniforme.

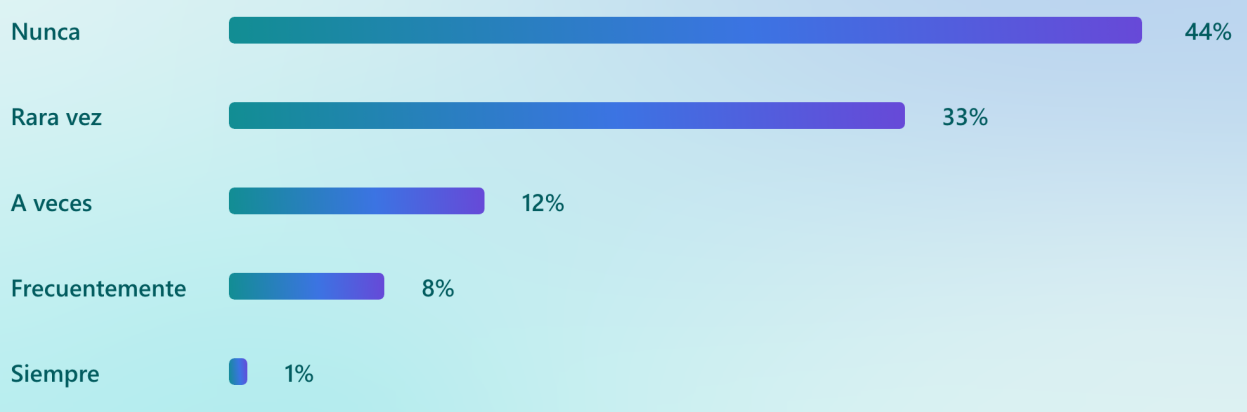


Figura 25. ¿Con qué frecuencia deja visible información sensible en su computadora o documentos impresos al retirarse de su puesto de trabajo?
Fuente: Elaboración propia.

El gráfico presenta la frecuencia con la que los colaboradores dejan visible información sensible en sus computadoras o en documentos impresos al retirarse de su puesto de trabajo. Se observa que el 44% indicó que nunca incurre en esta práctica y el 33% manifestó que rara vez lo hace, lo que representa un 77% de conductas seguras. No obstante, el 12% señaló que a veces deja información visible, el 8% frecuentemente y el 1% siempre. Evidenciando que aún existe un grupo que mantiene prácticas de riesgo. Estos resultados indican que, aunque la mayoría del personal adopta medidas adecuadas de protección de la información, aún existen conductas que pueden generar pérdida de información.

Estos resultados se relacionan directamente con el objetivo específico de identificar los errores humanos más relevantes que generan pérdida de información, ya que la exposición de información en el puesto de trabajo constituye un riesgo. Resultados similares indican que existe una relación significativa entre el comportamiento humano y las brechas de seguridad en las organizaciones (Hughes et al., 2021, p. 1).

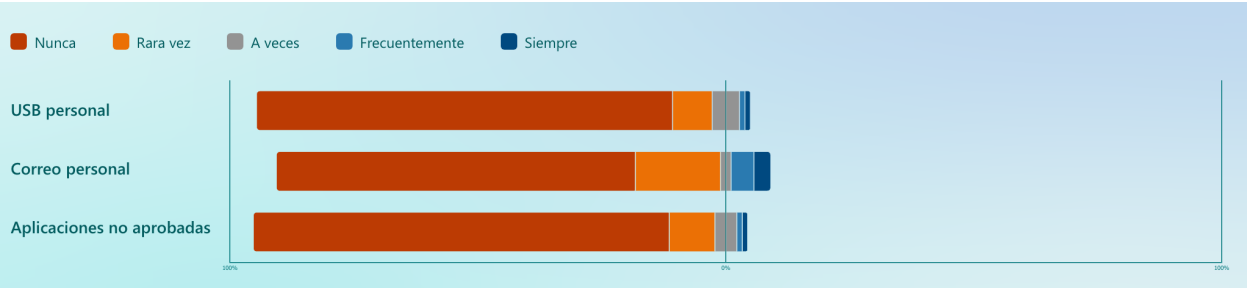


Figura 26. ¿Con qué frecuencia guarda, descarga o comparte información sensible o plataformas no autorizadas?
Fuente: Elaboración propia.

El gráfico presenta la frecuencia con la que los colaboradores guardan, descargan o comparten información sensible mediante medios no autorizados, tales como USB personal, correo personal y aplicaciones no aprobadas. Se observa que en las tres categorías predomina ampliamente la opción Nunca, seguida en menor proporción por Rara vez, mientras que las categorías frecuentemente y Siempre presentan porcentajes mínimos. Sin embargo, se observa en menor porcentaje que aún existen prácticas que podrían generar la pérdida de información sensible. El uso de dispositivos o canales no autorizados representa una vulnerabilidad crítica lo que lo vincula con el objetivo específico de identificar errores humanos más relevantes que generan pérdida de información sensible.

Desde otra perspectiva, aunque los resultados reflejan una alta adopción de conductas seguras, la presencia de un grupo reducido indica que el riesgo no ha sido completamente mitigado, este dato es relevante para el análisis de la hipótesis, ya que sugiere que la capacitación ha contribuido a disminuir estas conductas, pero no ha logrado eliminarlas en su totalidad.

En particular, se reconoce que los usuarios tienden a recurrir a medios no autorizados por razones como la conveniencia, la rapidez o la falta de percepción del riesgo, lo que mantiene latente la posibilidad de incidentes de seguridad. La persistencia de estas prácticas, aunque en baja proporción evidencia que la capacitación debe ser complementada con controles técnicos, monitoreo continuo y políticas más estrictas, ya que la concientización por sí sola no garantiza el cumplimiento total de las normas de seguridad. En este sentido, los programas efectivos combinan educación, controles organizacionales y mecanismos de supervisión para reducir de manera integral el riesgo asociado al factor humano.

Estos resultados coinciden con lo planteado por ENISA (2024) en su informe Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity, señala que el comportamiento del usuario sigue siendo un punto crítico en la seguridad de la información y que las organizaciones deben implementar enfoques integrales que incluyan formación continua y medidas de control para mitigar riesgos asociados al uso de canales no autorizados (Cybersecurity Culture Guidelines, 2024).

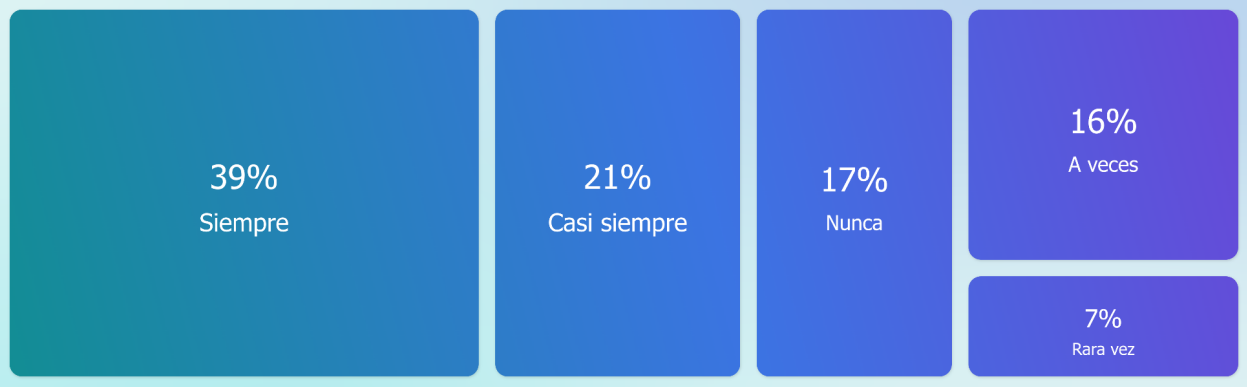


Figura 27. ¿Con qué frecuencia revisa cuidadosamente enlaces o archivos antes de hacer clic para evitar caer en intentos de phishing?
Fuente: Elaboración propia.

El gráfico presenta la frecuencia con la que los colaboradores revisan cuidadosamente enlaces o archivos antes de hacer clic, con el fin de evitar caer en intentos de phishing. Los resultados indican que el 39% manifestó que siempre realiza esta verificación y el 20% casi siempre, sumando un 59% de conductas preventivas constantes. Sin embargo, el 16% señaló que solo a veces adopta esta práctica, el 6% rara vez y el 17% nunca revisa cuidadosamente los enlaces o archivos antes de interactuar con ellos. Estos datos evidencian que, aunque más de la mitad del personal mantiene hábitos seguros frente a amenazas de ingeniería social, existe un porcentaje significativo que aún presenta conductas de riesgo.

Este resultado está sumamente relacionado con el objetivo de identificar errores humanos más relevantes, dado que el phishing constituye una de las principales causas de compromiso de información en entornos empresariales. Desde otra perspectiva, aunque el 60% de conductas refleja un impacto positivo de las capacitaciones, el 40% de colaboradores no realiza una verificación evidencia que las capacitaciones no han sido completamente efectivas, en contraste de estos datos con las hipótesis sugiere que las capacitaciones pueden influir en la reducción del error humano, pero no garantizan la adopción uniforme de comportamientos seguros.

Figura 28. ¿Con qué frecuencia utiliza contraseñas seguras (complejas, únicas, y no compartidas) para acceder a sistemas o información sensible?
Fuente: Elaboración propia.

El gráfico presenta la frecuencia con la que los colaboradores utilizan contraseñas seguras, complejas, únicas y no compartidas para acceder a sistemas o información sensible. Los resultados indican que el 38% manifestó que siempre utiliza contraseñas seguras y el 31% casi siempre, lo que representa un 68% de conductas alineadas con buenas prácticas de seguridad. No obstante, el 21% señaló que solo a veces adopta esta medida, mientras que el 5% rara vez y el 6% nunca emplean contraseñas seguras de forma frecuente. Estos datos indican que, aunque la mayoría del personal mantiene hábitos adecuados en la gestión de credenciales, aún existe un porcentaje relevante que podría representar un riesgo potencial de acceso no autorizado, dado que el uso inadecuado de contraseñas constituye una de las principales vulnerabilidades en la seguridad de la información, la presencia de un porcentaje considerable de colaboradores que no aplica estas prácticas evidencia que el cambio conductual no es uniforme, esto evidencia la necesidad de fortalecer estrategias de capacitación, así como implementar controles adicionales como políticas de contraseñas robustas etc.

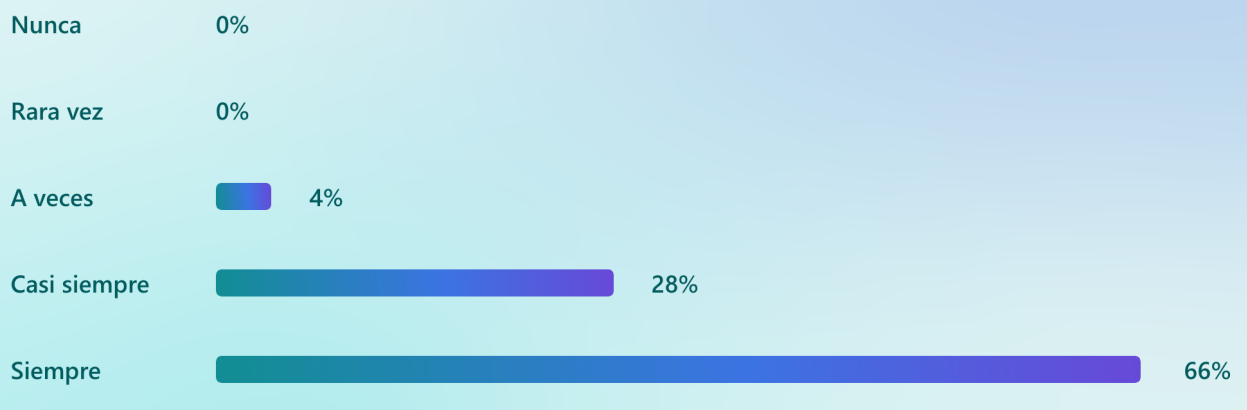


Figura 29. ¿En mi trabajo diario, sigo las políticas y procedimientos de seguridad al manejar información sensible?
Fuente: Elaboración propia.

El gráfico presenta la frecuencia con la que los colaboradores siguen las políticas y procedimientos de seguridad al manejar información sensible en su trabajo diario. Los resultados evidencian que el 66% manifestó que siempre cumple con las políticas establecidas y el 28% casi siempre, lo que representa un 94% de conductas alineadas con las normas institucionales. Asimismo, el 4% indicó que solo a veces sigue los procedimientos, mientras que no se registraron respuestas en las categorías nunca o rara vez, lo que refleja un alto compromiso con el cumplimiento de las políticas internas de seguridad de la organización.

Este resultado se vincula con el objetivo de esta investigación, ya que la evidencia de las estrategias formativas implementadas ha contribuido significativamente a la adopción de comportamientos alineados con la seguridad de la información. Este resultado aporta evidencia sólida a favor de la hipótesis planteada indicando que los métodos de capacitación influyen en la reducción del error humano. Los programas de capacitación efectivos fortalecen la cultura de seguridad y aumentan el cumplimiento de normas internas.

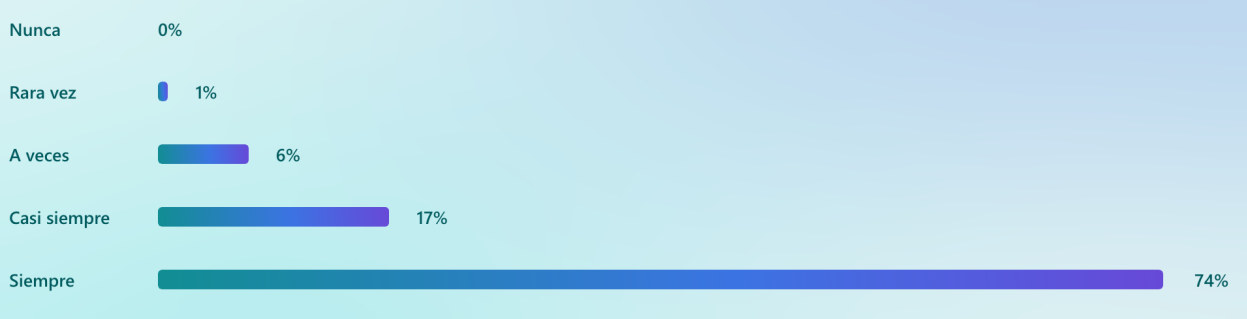


Figura 30. ¿Antes de enviar información sensible, verificó cuidadosamente que el destinatario sea el correcto?
Fuente: Elaboración propia.

El gráfico presenta la frecuencia con la que los colaboradores verifican cuidadosamente que el destinatario sea el correcto antes de enviar información sensible. Los resultados evidencian que el 74% manifestó que siempre realiza esta verificación y el 17% casi siempre, lo que representa un 91% de conductas preventivas consistentes. Asimismo, el 6% indicó que solo a veces válida el destinatario y el 1% rara vez lo hace, mientras que no se registraron respuestas en la categoría de nunca. Esto evidencia que existe un alto nivel de conciencia respecto al envío incorrecto de información, uno de los errores más comunes en la pérdida de información. Desde una perspectiva analítica el alto porcentaje de 91% sugiere que las capacitaciones han tenido un impacto positivo y consciente en la adopción de prácticas seguras por parte del personal lo que proporciona evidencia a la hipótesis alternativa.

No obstante, la existencia de un porcentaje, aunque reducido de colaboradores que no realizan esta verificación de forma constante representa un punto crítico, ya que el envío incorrecto de información suele estar asociado a errores humanos involuntarios que pueden tener consecuencias significativas en términos de confidencialidad. Esto implica que incluso niveles altos de cumplimiento no eliminan completamente el riesgo, sino que lo reducen parcialmente.

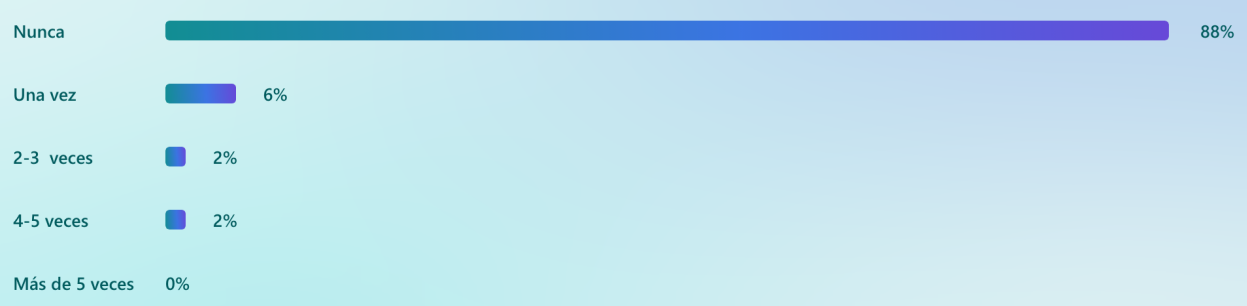


Figura 31. En los últimos 12 meses, ¿con qué frecuencia ha ocurrido que, por error suyo, se perdió, borró o quedó inaccesible información sensible?
Fuente: Elaboración propia.

El gráfico presenta la frecuencia con la que, en los últimos 12 meses, ha ocurrido que por un error del colaborador se perdió, borró información sensible. Los resultados indican que el 88% manifestó que nunca ha experimentado este tipo de incidente, mientras que el 6% señaló que ocurrió una vez. Asimismo, el 2% reportó haber enfrentado esta situación entre 2 y 3 veces y otro 2% entre 4 y 5 veces, sin registrarse casos superiores a cinco eventos. Estos datos indican que la ocurrencia de incidentes generados por error humano es baja dentro de la empresa. El alto porcentaje de colaboradores que no ha experimentado incidentes 88%, sugiere que las estrategias de capacitación han contribuido de forma significativa en la reducción del error humano, este resultado aporta evidencia a favor de la hipótesis alternativa indicando que los métodos de capacitación influyen en la disminución de incidentes. La baja incidencia de eventos de pérdida de información evidencia la afectividad de los métodos de capacitación, sin embargo, la presencia de incidentes en una menor proporción confirma que el error humano no puede ser eliminado completamente.

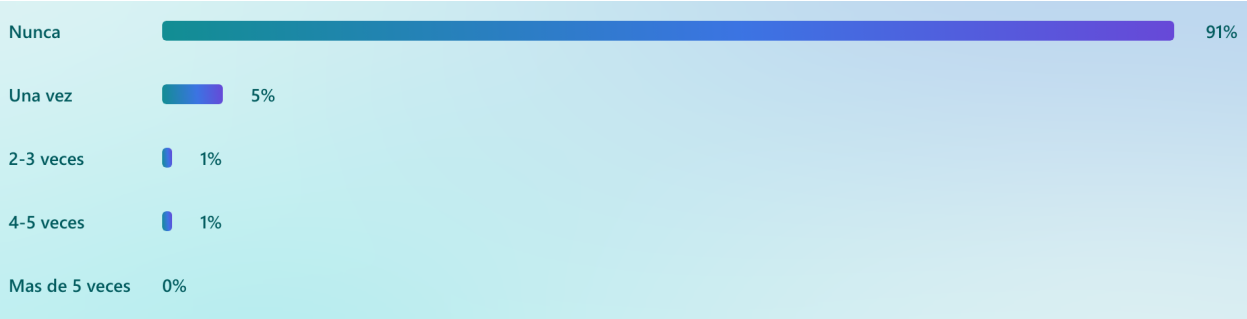


Figura 32 . En los últimos 12 meses, ¿con qué frecuencia ha ocurrido que, por un error suyo, se envió o expuso información sensible a personas no autorizadas?
Fuente: Elaboración propia.

El gráfico presenta la frecuencia con la que en los últimos 12 meses por error del colaborador se envió o expuso información sensible a personas no autorizadas. Los resultados muestran que el 91% indicó que nunca ha ocurrido este tipo de incidente, mientras que el 5% manifestó que sucedió una vez, asimismo, el 1% señaló que ocurrió entre 2 y 3 veces y otro 1% entre 4 y 5 veces, sin registrarse casos superiores a cinco eventos. Estos resultados indican que la exposición accidental de información es un evento poco común en la empresa. En relación con los objetivos de la investigación, este hallazgo se vincula directamente con el objetivo de identificar los errores humanos que generan pérdida de información sensible, dado que este tipo de incidente representa un riesgo en términos de seguridad de la información. La baja incidencia de eventos de exposición de información sensible evidencia la afectividad de los métodos de capacitación.

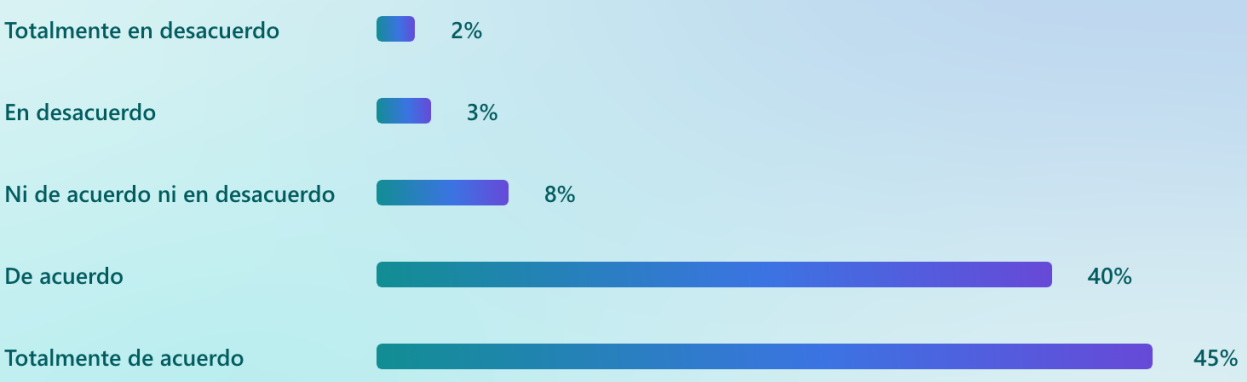


Figura 33. ¿Considero que un error mío en el manejo de información sensible podría generar consecuencias graves para la organización?
Fuente: Elaboración propia.

El gráfico presenta la percepción de los colaboradores respecto a si un error propio en el manejo de información sensible podría generar graves consecuencias para la organización. Los resultados indican que el 45% está totalmente de acuerdo y el 40% de acuerdo, lo que representa un 85% de sensibilidad respecto al impacto de sus acciones. Por su parte, el 8% manifestó una posición neutral, mientras que el 3% está en desacuerdo y el 2% totalmente en desacuerdo. Estos datos evidencian un alto nivel de conciencia sobre la responsabilidad individual en la protección de información sensible, la concienciación del riesgo es un componente esencial para la adopción de comportamientos seguros.

Sin embargo, más allá de evidenciar un alto nivel de concientización, estos resultados permiten analizar la homogeneidad de la cultura de seguridad dentro de la empresa. En este sentido, aunque la mayoría reconoce las consecuencias del error humano, la existencia de un grupo

pequeño sugiere que la cultura de seguridad no se encuentra completamente consolidada. Desde la perspectiva de los objetivos de investigación, resulta relevante comprender por qué a pesar de recibir capacitación y el observar otros resultados que indican un alto nivel de capacitación y cumplimiento, existen colaboradores que no están conscientes de las consecuencias de la ocurrencia de un error humano.

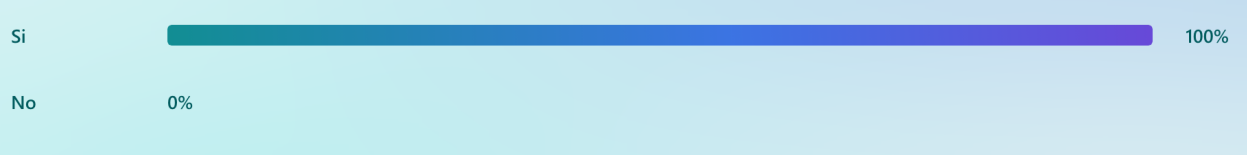


Figura 34¿Tengo claro que la información que manejo en mi trabajo se considera sensible?
Fuente: Elaboración propia.

El gráfico presenta el nivel de claridad que poseen los colaboradores respecto a si la información que manejan en su trabajo es considerada sensible. Los resultados indican que el 100% de los encuestados respondió afirmativamente, mientras que no se registraron respuestas negativas. Este resultado evidencia que los colaboradores poseen pleno conocimiento sobre el tipo de información que se maneja en sus puestos de trabajo, no obstante, este conocimiento no garantiza la correcta aplicación de prácticas seguras, así mismo desde la perspectiva de la hipótesis planteada, este resultado no permite por sí mismo validar la influencia de los métodos de capacitación en la reducción del error humano. En este sentido, estos resultados sugieren que la organización ha logrado establecer un nivel básico de conocimiento homogéneo respecto a la información sensible, sin embargo, la efectividad de los métodos de capacitación debe evaluarse en función de su capacidad para transformar este conocimiento en prácticas seguras conscientes.

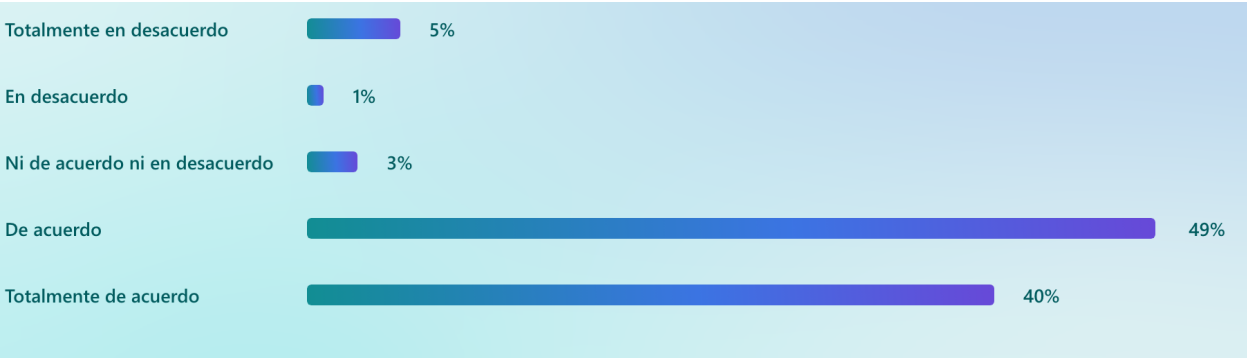


Figura 35¿Me considero capaz de identificar situaciones en las que podría cometer un error que exponga información sensible?
Fuente: Elaboración propia.

El gráfico presenta la percepción de los colaboradores respecto a su capacidad para identificar situaciones en las que podrían cometer un error que exponga información sensible. Los resultados muestran que el 49% está de acuerdo y el 40% totalmente de acuerdo, lo que representa un 89%de percepción positiva sobre su capacidad para identificar riesgos. Por su parte el 3% manifestó una posición neutral, mientras que el 1% está en desacuerdo y el 5% totalmente en desacuerdo. Estos datos evidencian un alto nivel de autoconciencia frente a posibles escenarios que pueden resultar en pérdida de información por un error humano. No obstante, al contrastar este resultado con los demás de este estudio, donde aún se registran errores y exposiciones de información, se evidencia una posible brecha entre la percepción de capacidad y el comportamiento efectivo.

Figura 36. ¿Cuándo tengo dudas sobre cómo manejar información sensible, sé a quién consultar o dónde buscar la información correcta para evitar errores?
Fuente: Elaboración propia.

El gráfico presenta la percepción de los colaboradores respecto a si, cuando tienen dudas sobre cómo manejar información sensible, saben a quién consultar o donde buscar la información correcta para evitar errores. Los resultados indican que el 47% está totalmente de acuerdo y el 42% de acuerdo, lo que representa un 89% de respuestas positivas. Por su parte el 5% manifestó una posición neutral, mientras que el 1% está en desacuerdo y el 3% totalmente en desacuerdo. Los datos muestran que la mayoría del personal cuenta con claridad sobre los canales de consulta en materia de seguridad de la información, lo cual es un factor importante para la prevención de errores operativos.

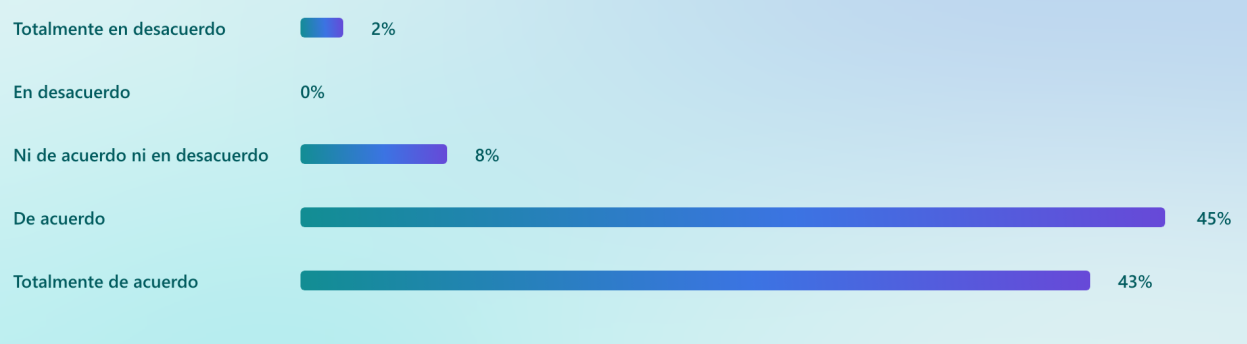


Figura 37¿Después de las capacitaciones, me siento más seguro(a) al manejar información sensible?
Fuente: Elaboración propia.

El gráfico muestra la percepción de los colaboradores respecto a si después de las capacitaciones se sienten más seguros al manejar información sensible. Los resultados reflejan que el 45% está de acuerdo y el 43% totalmente de acuerdo, acumulando un 88% de valoración positiva. Un 8% se mantiene en una postura neutral, mientras que únicamente el 2% manifestó estar totalmente en desacuerdo y el 0% en desacuerdo. En conclusión, los resultados demuestran que los métodos de capacitación implementados han generado un impacto favorable en la autoconfianza del personal para gestionar información sensible. Desde otra perspectiva, el alto nivel de confianza 88% podría interpretarse como un indicador positivo del proceso formativo, no obstante, también plantea un elemento crítico, la confianza elevada no siempre se traduce en comportamientos seguros, así mismo no constituye evidencia para afirmar una reducción efectiva del error humano relacionada con las hipótesis planteadas. La organización ha logrado fortalecer la confianza del personal, ahora el reto es asegurar que dicha confianza esté alineada con prácticas seguras.

Con el propósito de realizar un análisis comparativo en base a los objetivos de investigación, se realizó un cruce de variables en SPSS, las gráficas presentadas a continuación presentan visualmente los resultados en base al objetivo de enumerar los métodos de capacitación en ciberseguridad implementados y los colaboradores por área, que manejan información sensible en Grupo Vesta SPS, 2026.

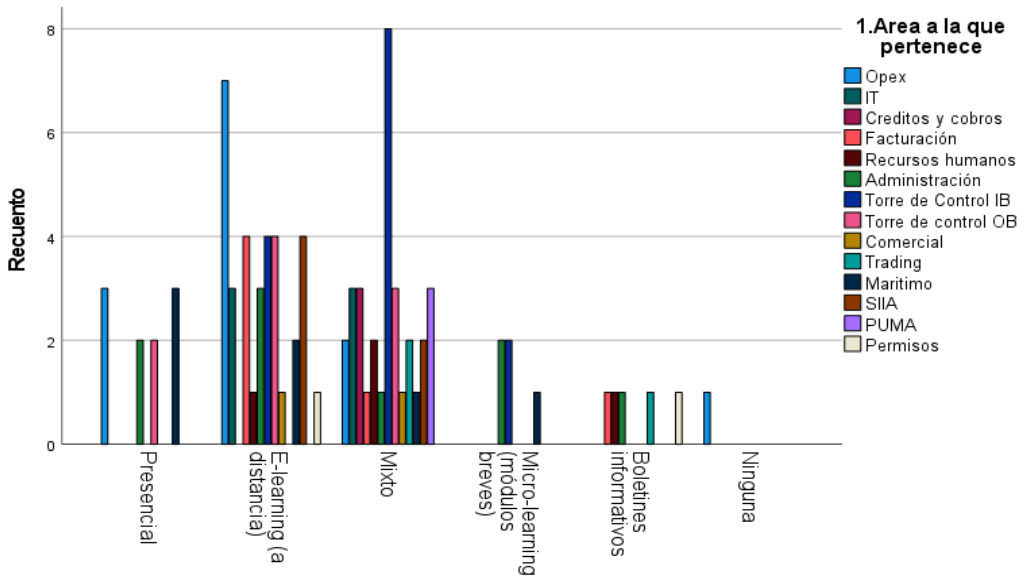


Figura 38.Métodos de capacitación por área
Fuente: Elaboración propia.

Se observa en la gráfica anterior que el método mixto es uno de los métodos de capacitación más utilizados para las distintas áreas, seguido por el e-learning, el cual evidencia una tendencia hacia modelos de capacitación digitales, asimismo, se observa que las modalidades micro-learning y boletines informativos presentan menor frecuencia. Estos resultados demuestran que Grupo Vesta SPS prioriza métodos de capacitación combinados lo que contribuye a fortalecer la reducción de error humano. En el gráfico anterior se identifica cuáles son los enfoques predominantes en el contexto organizacional lo que está relacionado al objetivo de enumerar los métodos de capacitación implementados, dicho esto es importante señalar que este gráfico no permite por sí solo determinar la efectividad de dichos métodos en la reducción del error humano, por tanto, puede ser considerado como un insumo descriptivo en cuanto a la hipótesis planteada.

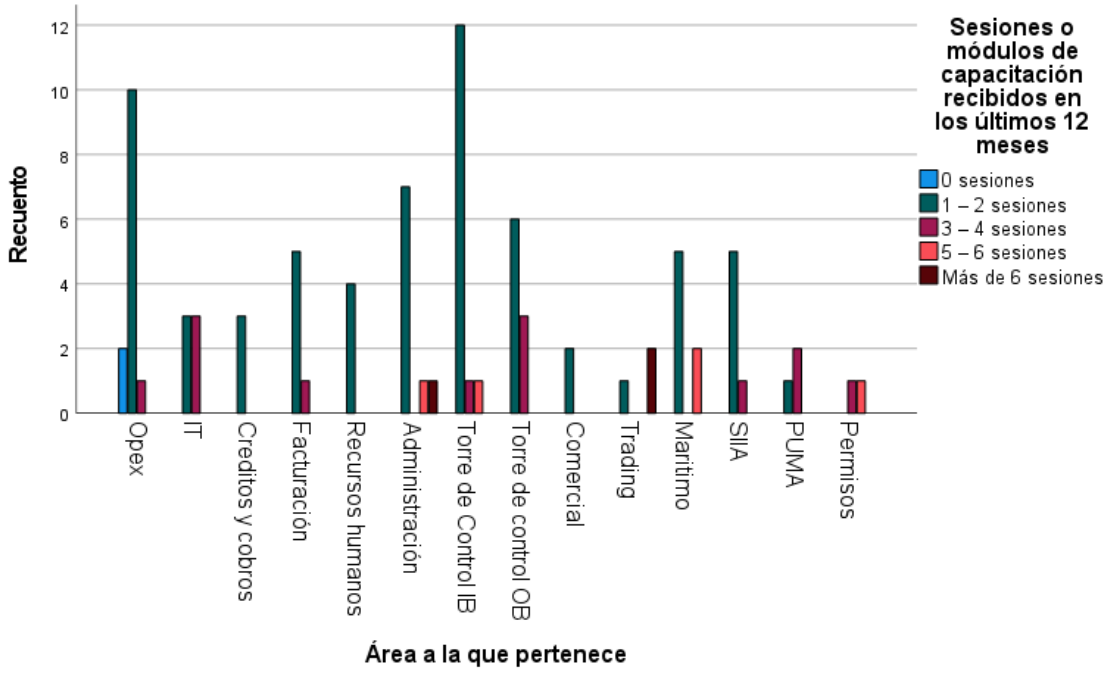


Figura 39.Intensidad de capacitación por área
Fuente: Elaboración propia

En la gráfica anterior se observa que la categoría predominante es la de 1-2 sesiones de capacitación recibida en los últimos 12 meses lo que indica una intensidad básica, en contraste con esto las áreas con mayor intensidad formativa se observa Torre de control IB con rangos de 1-2 sesiones, 3-4 y 5-6 lo que evidencian, mayor número de sesiones de formación, Opex, y con menos intensidad Trading, permisos y PUMA. La variabilidad de las sesiones recibidas por área sugiere que no existe una estandarización en las capacitaciones impartidas al personal. Más allá de la frecuencia de las sesiones, estos resultados permiten analizar la lógica de distribución de la capacitación dentro de la organización. En este sentido, la variabilidad observada sugiere que la capacitación no sigue un modelo homogéneo, sino que podría estar definida por criterios estratégicos, esto puede ocasionar brechas de conocimiento y comportamiento entre las áreas. Si bien la capacitación podría influir en la reducción del error humano, su efectividad depende no solo de la existencia de programas formativos, si no de su cobertura y frecuencia adecuada.

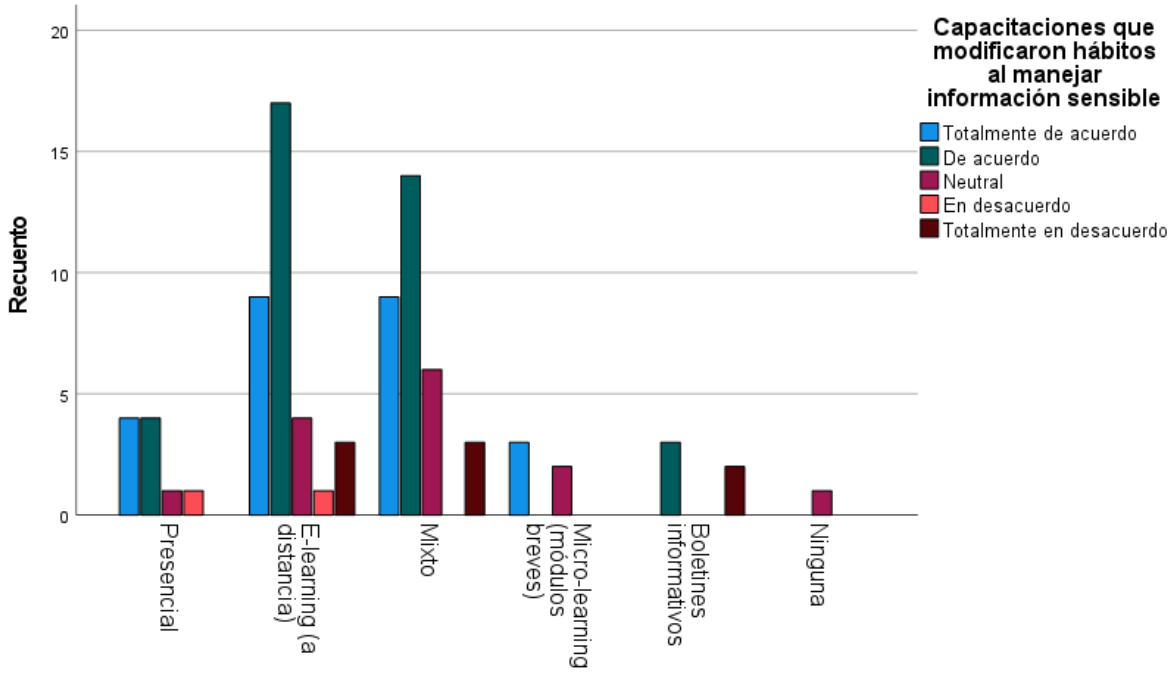


Figura 40. Evaluar qué método genera mayor cambio conductual.
Fuente: Elaboración propia.

Según la gráfica anterior los métodos que causaron un mayor impacto en la conducta de los colaboradores, donde el método con mayor concentración en de acuerdo y totalmente de acuerdo es e-learning, lo que indica que los colaboradores perciben esta modalidad como un medio positivo que les ha permitido modificar sus conductas y prácticas en el manejo de información. Asimismo, se observa el método mixto. Esto sugiere que una combinación de modalidad presencial y virtual puede fortalecer la conciencia sobre adoptar buenas prácticas de seguridad. En relación con los objetivos de investigación, este resultado se vincula directamente con el objetivo general, ya que evidencia cuáles estrategias formativas tienen mayor capacidad para generar cambios en las prácticas del personal, asimismo, aporta al análisis del error humano, considerando que la modificación de hábitos es un elemento clave para su prevención.

También este gráfico constituye una de las evidencias más directas a favor de la hipótesis alternativa, ya que demuestra que ciertos métodos de capacitación influyen en la modificación de comportamientos. Estudios muestran resultados similares tal como un estudio que, adoptando un enfoque de educación abierta en ingeniería, se ha iniciado una enseñanza mixta impulsada por proyectos centrada en el "constructivismo", constituyendo un modelo que combina la instrucción online y presencial, tareas dentro y fuera de clase, actividades dentro y fuera del laboratorio, trabajos académicos y concursos. Este modo de aprendizaje combinado ha tenido un resultado

beneficioso en mejorar las capacidades de autoaprendizaje de los estudiantes (Sui & Yang, 2023, p. 1).

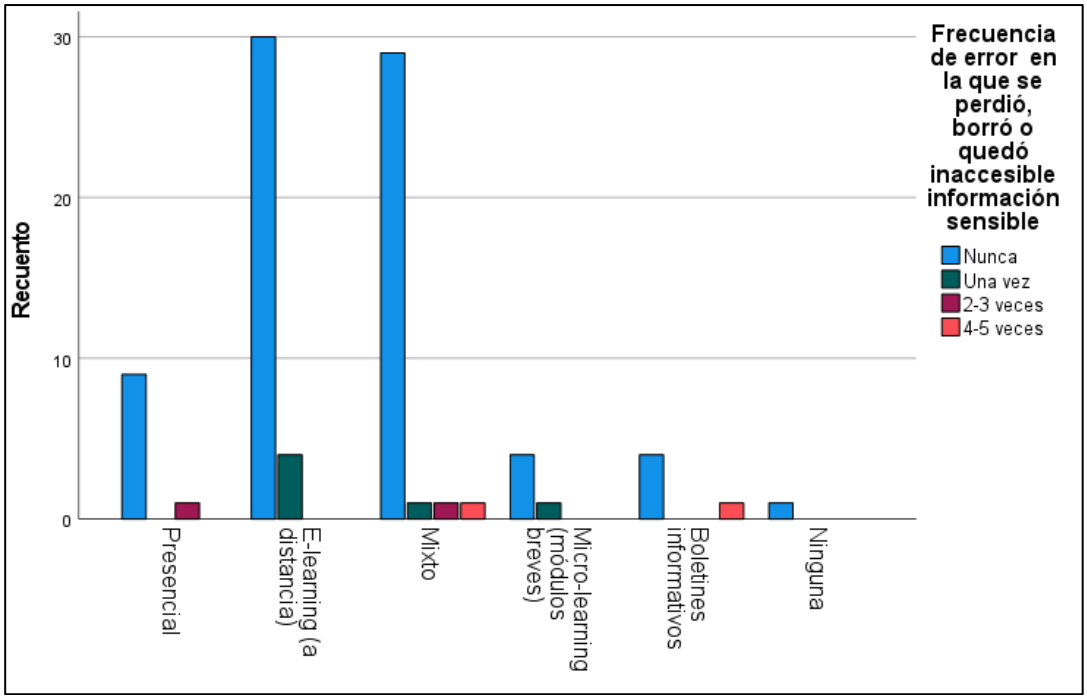


Figura 41. Relación entre método y reducción de incidentes.
Fuente: Elaboración propia.

Se observa en la gráfica anterior que los métodos e-learning y mixto presentan mayor número de respuesta en la categoría de nunca, esto indica que los colaboradores que recibieron estos métodos reportan un menor número de incidentes relacionados con errores humanos y la pérdida de información, a diferencia de los demás métodos que presentan menor asociación con la reducción de incidentes. Este resultado permite identificar una asociación directa entre el tipo de capacitación y la ocurrencia de errores humanos, evidenciando que no todas las estrategias formativas tienen el mismo impacto en la reducción de incidentes. Tal como lo plantea Oroni et al., (2025) en un estudio para estudiantes con menor conciencia en ciberseguridad, la participación activa en el aprendizaje en línea junto con el estricto cumplimiento de las políticas de seguridad también mejora significativamente la ciberseguridad.

Estos datos demuestran que ningún factor garantiza la ciberseguridad; más bien, múltiples combinaciones de condiciones pueden lograr resultados positivos (pág. 1). En este contexto, los resultados obtenidos son consistentes con la literatura, al evidenciar que los métodos de capacitación basados en entornos digitales y combinados presentan una mayor asociación con la

reducción de incidentes, no obstante, la presencia de algunos casos de error incluso en estos métodos indica que, aunque efectivos no eliminan completamente el riesgo, lo que refuerza la necesidad de complementar la capacitación con controles adicionales.

Tal como se expuso en el apartado anterior, se realizó el mismo procedimiento estadístico para graficar los resultados de los cruces de variables en base al objetivo de identificar los errores humanos más relevantes que generan pérdida de información sensible en Grupo Vesta, San Pedro Sula, 2026.

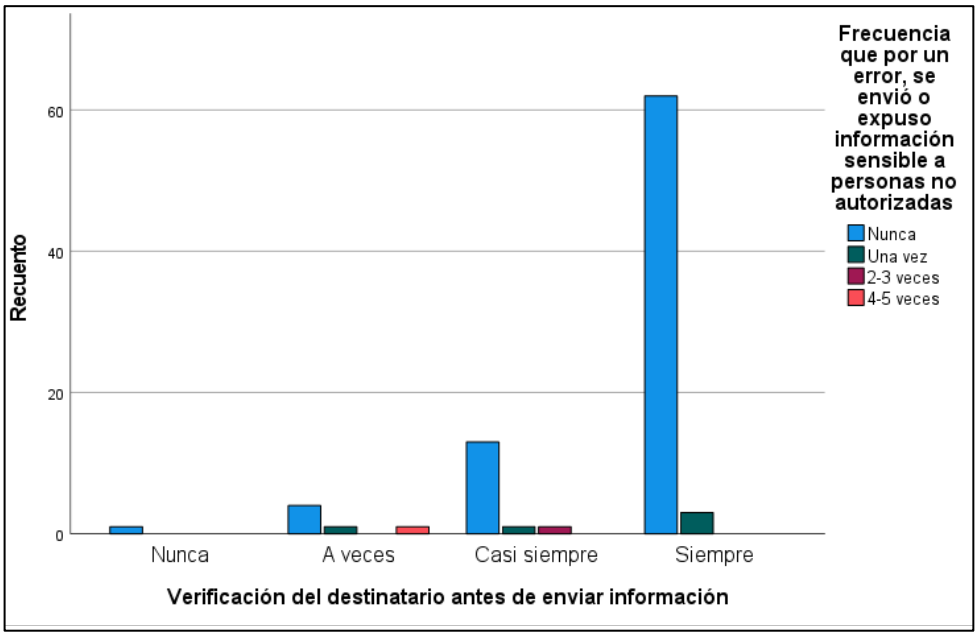


Figura 42. Frecuencia de verificación de destinatario antes de enviar información relacionada con la frecuencia de error humano
Fuente: Elaboración propia.

En la gráfica se observa que en la categoría siempre verifica el destinatario, concentra mayor cantidad de respuestas en la opción nunca ha expuesto información sensible, lo que refuerza que una conducta con buenas de prácticas de seguridad influye en la reducción de incidentes. También en la categoría casi siempre, aunque predomina también la opción nunca se observan algunos casos de error en categorías como una vez y 2-3 veces, esta tendencia se observa en la categoría a veces donde aumenta la presencia de incidentes, y la categoría de nunca verifica presenta menos registros de error, con un número muy pequeño de participantes. Este resultado permite identificar que la verificación del destinatario es un factor crítico operativo en la

prevención de errores, asimismo se verifica como una conducta específica influye en la ocurrencia de este tipo de incidentes lo que se relaciona al objetivo de identificar errores humanos.

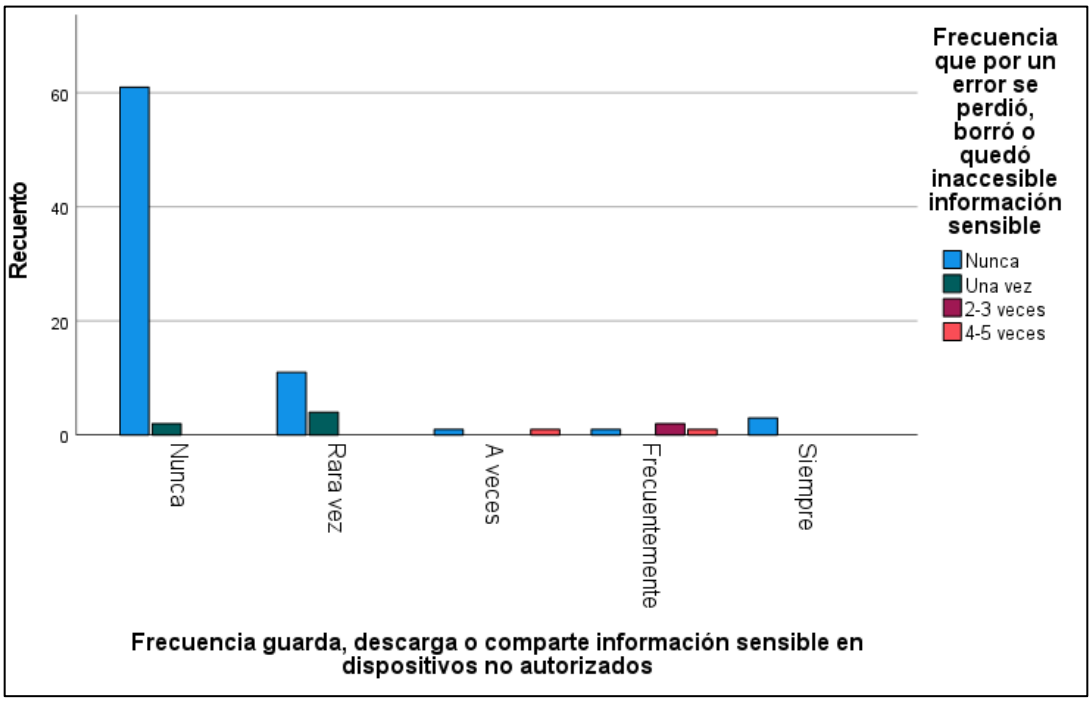


Figura 43. Identificar si el uso de plataformas no autorizadas está vinculado a pérdida de información.
Fuente: Elaboración propia.

Se observa que en la categoría nunca guarda o comparte información en dispositivos no autorizados, concentrándose un alto número de respuestas en la opción nunca de frecuencia de errores, lo que expone una asociación entre el cumplimiento de buenas prácticas y la reducción de errores. Dicho lo anterior se observa en las categorías Rara vez, A veces, y frecuentemente que se incrementan las respuestas de errores cometidos por los empleados en los rangos de 2-3 veces, 4-5 veces, esto indica que la no adopción de buenas prácticas de seguridad aumenta el riesgo de incidentes generados por error humano. Los resultados evidencian que la reducción del error humano no depende únicamente del conocimiento adquirido, sino del grado en que los colaboradores eviten prácticas que incrementan la exposición al riesgo, como el uso de dispositivos no autorizados

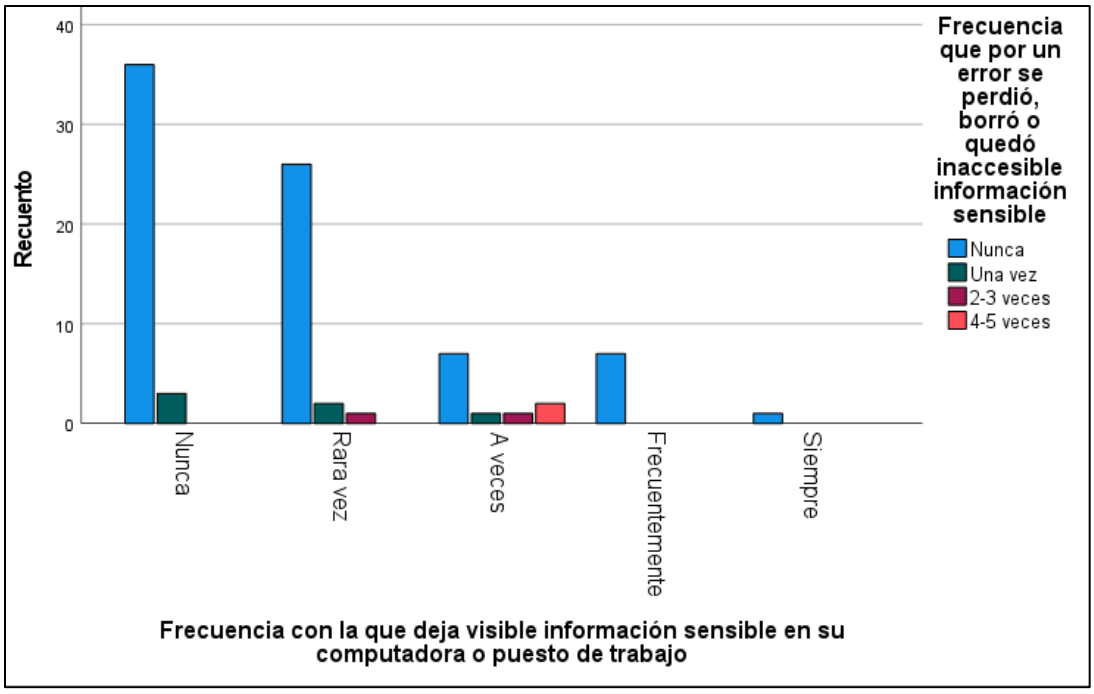


Figura 44.Determinar si el descuido físico está asociado a incidentes reales.
Fuente: Elaboración propia.

Según los resultados plasmados en la gráfica anterior detallan que la mayoría quienes indican que Nunca dejan información expuesta reportan también no haber sufrido incidentes: sin embargo, a medida que la conducta pasa a Rara vez y especialmente A veces, se observa un incremento en los casos donde la información se perdió una o más veces. Aunque la categoría de Frecuentemente y Siempre presentan menor cantidad de personas, mantienen presencia de incidentes, lo que refuerza el patrón presentado. El gráfico sugiere una relación entre la exposición de información sensible y la materialización de incidentes debido a errores humanos. La presencia de incidentes en categorías como rara vez sugiere que incluso desviaciones mínimas en el comportamiento pueden generar consecuencias, lo que evidencia una baja tolerancia al error en el manejo de información sensible.

Tabla 6. Cantidad de colaboradores por área que manejan información sensible.

Área a la que pertenece	¿Tengo claro qué la información que manejo en mi trabajo se considera sensible?
	Si
Opex	13
IT	6
Créditos y cobros	3
Facturación	6
Recursos humanos	4
Administración	9
Torre de Control IB	14
Torre de control OB	9
Comercial	2
Trading	3
Marítimo	7
SIIA	6
PUMA	3
Permisos	2
Total	**87**

Fuente: Elaboración propia

La tabla presenta la distribución de los colaboradores por área en la empresa Grupo Vesta SPS que reconocen que la información que manejan en su trabajo es considerada sensible, evidenciando un total de 87 colaboradores distribuidos en diferentes áreas. Al contrastar estos resultados con la identificación previa de áreas críticas que tiene definida la empresa, se observa que existe una discrepancia en las áreas que manejan información sensible y que son catalogadas

como críticas. En relación con los objetivos planteados, este resultado permite no solo enumerar las áreas donde se implementan métodos de capacitación en ciberseguridad, sino también identificar la distribución del personal expuesto al manejo de información sensible, lo que constituye un insumo para el diseño de estrategias formativas dentro de la empresa. En este contexto, los resultados evidencian que la organización cuenta con una base clara para estructurar sus programas de capacitación, sin embargo, también resalta la necesidad de priorizar aquellas áreas que combinan alta criticidad en base al tipo de información que manejan.

ESTADÍSTICAS INFERENCIALES

El propósito de esta sección es interpretar los datos obtenidos de la muestra y generalizarse a toda la población objeto de estudio. Aquí se va a comprobar las hipótesis y determinar las relaciones significativas que hay entre las variables de estudio. Se establece el nivel de significancia, los criterios de decisión y la interpretación de los resultados, con el fin de garantizar el rigor científico y validez en las conclusiones obtenidas.

PRUEBA DE HIPÓTESIS

A continuación, se procede a realizar la comprobación de la hipótesis planteada en el capítulo anterior, se empleó la prueba estadística no paramétricas, la prueba de Chi-cuadrado para 38 ítems, y así evaluar si la distribución de las respuestas difiere de una distribución esperada uniforme y determinar si se rechaza o acepta la hipótesis nula. Se emplearon variables categóricas ordinales y determinar si las diferencias encontradas se deben al azar o si son estadísticamente significativas.

A continuación, se presenta la tabla de los resultados obtenidos, utilizando la herramienta SPSS V.27.

Tabla 7. Estadísticos de prueba

	4. ¿En qué medida considera que el contenido de las capacitaciones en seguridad de la información es claro y fácil de comprender?	5.¿El contenido de las capacitaciones en seguridad de la información es relevante para mis actividades diarias dentro de la organización?	6.¿Qué tan relevantes considera los temas abordados durante las capacitaciones?	7.¿Las sesiones de capacitación incluyeron explicaciones sobre errores humanos comunes y cómo evitarlos?	9.¿La modalidad presencial facilitó su aprendizaje?	10.¿La modalidad E-learning (a distancia) facilitó su aprendizaje?	28.¿Con qué frecuencia guarda, descarga o comparte información sensible en dispositivos o plataformas no autorizadas como USB personal?	29.¿Con qué frecuencia guarda, descarga o comparte información sensible en dispositivos o plataformas no autorizadas como correo personal?	30.¿Con qué frecuencia guarda, descarga o comparte información sensible en dispositivos o plataformas no autorizadas como aplicaciones no aprobadas?	31.¿Con qué frecuencia revisa cuidadosamente enlaces o archivos antes de hacer clic para evitar caer en intentos de phishing?	32.¿Con qué frecuencia utiliza contraseñas seguras (complejas, únicas y no compartidas) para acceder a sistemas o información sensible?
N	87	87	87	87	87	87	87	87	87	87	87
Mediana	4,00	4,00	4,00	4,00	4,00	4,00	1,00	1,00	1,00	4,00	4,00
Chi-cuadrado	4,062[b]	1,894[c]	4,385[d]	2,352[e]	2,311[f]	8,588[g]	5,917[q]	1,936[f]	13,255[q]	,691[b]	1,476[r]
gl	5	5	5	5	5	5	5	5	5	5	5
Sig. asin.	,541	,864	,495	,799	,805	,127	,314	,858	,021	,983	,916

Fuente: Datos obtenidos de la aplicación de instrumento mediante SPSS.

La tabla muestra, para cada ítem del cuestionario, una muestra de 87, así mismo la mediana, chi-cuadrado, gl y Sig. Asintótica. Esta última que permitirá contrastar hipótesis, donde si $p < 0.05$ => Se rechaza H_0, ya que existe diferencia significativa y si $p \geq 0.05$ => No se rechaza H_0, no hay evidencia suficiente. Al revisar la fila Sig. asint., se observa que, la gran mayoría de los ítems presentan $p > 0.05$, sin embargo, se identifica que en el ítem 30, $p = 0.021$ por lo tanto, la significancia estadística, se determina entonces que hay evidencia de relación entre capacitación y manejo de información. Se rechaza la hipótesis nula., H_0: "Los métodos de capacitación del personal no influyen en la reducción del error humano asociado con la pérdida de información sensible."

Los resultados evidencian que los métodos de capacitación implementados influyen significativamente en variables relacionadas con la reducción del error humano y la protección de información sensible, es decir, influye de manera significativa en la disminución de prácticas inseguras, como compartir o almacenar información sensible en plataformas no autorizadas evidenciando que la capacitación es un factor clave para reducir errores humanos en la seguridad de la información. Por tanto, se concluye que existe evidencia estadística suficiente para afirmar que la capacitación del personal contribuye a la disminución del riesgo asociado a la pérdida de información sensible.

4.3 RESULTADOS Y ANÁLISIS DE LOS DATOS ENCONTRADOS.

En el presente apartado se interpretan los resultados obtenidos en la investigación en contraste con resultados de investigaciones anteriores realizadas de temas relacionados a capacitación y concientización del personal, a partir de esta comparativa se pretende realizar un análisis crítico y de reflexión en base al tema de investigación y la interpretación de resultados similares y su impacto en la reducción del error humano. También se presentan nuevas recomendaciones o ideas para investigaciones futuras que servirán de referencia para analizar distintos programas de capacitación en seguridad de la información.

DISCUSIÓN DE LOS RESULTADOS

De acuerdo con (Becerril, 2019), además de los riesgos de ciberseguridad por ataques, las empresas, gobiernos e instituciones deben preocuparse por las vulnerabilidades asociadas al desconocimiento por incumplimiento de políticas de seguridad o demandas relacionadas con la violación de datos (data breach). Si no se tienen adecuados procesos, capacitación e

innovación tecnológica en materia de ciberseguridad, estos actores pueden verse inmersos en varios problemas, pues además de la pérdida de la información (pág. 11).

Como se menciona anteriormente el tema de capacitación al personal en temas relacionados con la seguridad de la información debe ser tomada como un asunto importante en las organizaciones, como se presentaron anteriormente los resultados demuestran que las capacitaciones redujeron significativamente los incidentes de seguridad, este patrón se ha observado en distintas investigaciones donde se resalta la capacitación como una estrategia para evitar vulnerabilidades e incidentes de seguridad.

Un estudio realizado en México donde el objetivo de la investigación era el de analizar los programas de capacitación como herramienta para fortalecer la ciberseguridad en una empresa de tal país. Los resultados de este estudio demostraron lo siguiente:

> La mayoría de los empleados (52.1%) consideran que tienen el conocimiento necesario sobre las amenazas cibernéticas que pueden enfrentar, pero el resto no consideran que conozcan dichas amenazas. Además, a pesar de que el tema de ciberseguridad es prioritario para la organización, los colaboradores no cuentan con la suficiente capacitación que les ayude a reducir las amenazas a las que están expuestos (Piñón et al., 2023, p.1) .

Estos resultados se asemejan mucho a los del presente estudio donde, se observó que la frecuencia de capacitación para las distintas áreas de la empresa es de 1-2 veces al año lo que se consideraría una frecuencia básica baja, asimismo el método utilizado en Grupo Vesta SPS no es aplicado de forma general, por lo que existen colaboradores que no poseen suficientes conocimientos para evitar un error que dé como resultado la fuga de información.

Otro estudio evaluó la efectividad de planes de concienciación para reducir la vulnerabilidad de los empleados ante ataques cibernéticos en una pequeña empresa. Donde se obtuvieron los siguientes resultados.

> El análisis reveló que la edad, experiencia laboral y acceso a información sensible impactaron la capacidad de respuesta, con mejores resultados en empleados jóvenes y tecnológicamente experimentados. Aunque la concienciación redujo la vulnerabilidad, persistieron riesgos asociados al comportamiento humano, sugiriendo la necesidad de formación continua y soluciones tecnológicas automatizadas (Cabezas & Fiallos, 2024, p. 1).

Los resultados presentados anteriormente para este estudio detallan que las edades promedio de los encuestados son de 26-35 años lo que puede ser aprovechado por la organización para afianzar los conocimientos en seguridad de la información, así mismo los colaboradores están conscientes que manejan información sensible, y aunque se ha observado una reducción en incidentes de seguridad debido al error humano, aún persiste el riesgo de que estos se puedan materializar.

El artículo, Errores humanos: una preocupación en ciberseguridad y el eslabón más débil de las pequeñas empresas, dice que los resultados revelaron que los errores humanos repetidos comprometen los principios de seguridad de la información y convierten a los empleados en el eslabón más débil. El estudio explicó los riesgos que los empleados pueden causar debido a la ignorancia o la mala toma de decisiones, errores técnicos y errores de habilidades y políticas (Ncubukezi, s. f., p. 1).

Estos resultados se asocian a esta investigación porque se demostró que los errores humanos no siempre son intencionales sino productos de descuidos, malas prácticas o desconocimientos de políticas internas, y que mediante estrategias formativas como capacitaciones mediante métodos mixtos y e-learning, puede transformar ese eslabón más débil en un elemento fortalecido dentro de la organización.

Así también el artículo cuyo objetivo era el investigar la conciencia del usuario y los comportamientos vulnerables, la capacitación efectiva para los usuarios y la investigación de enfoques de vanguardia para medir o evaluar la postura de ciberseguridad de la organización en comparación con marcos de la industria como el marco NIST. “Demuestra que las políticas de ciberseguridad formuladas y aplicadas, junto con la educación, capacitación y concienciación en seguridad dirigidas, son fundamentales para disminuir los errores de los usuarios, reduciendo así la probabilidad de un ciberataque” (Amorosa & Yankson, 2023, p.1).

Los resultados de este estudio se relacionan de manera directa y complementaria, con los resultados de Grupo Vesta SPS, ya que ambos coinciden en que la capacitación estratégica y adaptada al contexto organizacional, reduce significativamente los errores humanos, y por ende, los incidentes en seguridad de la información (Olushola et al., s. f., p. 1).

En relación a los resultados del presente estudio y con referencia de estudios similares se recomienda para futuras investigaciones, se realice una ampliación del alcance del estudio, ampliando y abordando distintas empresas del sector privado o público en Honduras, con el objetivo de realizar una comparativa de los resultados teniendo en cuenta diferentes contextos organizacionales, también, se recomienda enfocar el estudio en simulaciones prácticas, donde se realicen investigaciones experimentales con ejercicios de evaluación post capacitación como por ejemplo pruebas de phishing con el fin de determinar si la metodología seleccionada genera un impacto en la conducta de los colaboradores y la cultura de seguridad de la información que reduzcan el error humano y por ende la fuga de información sensible en las empresas.

CONSIDERACIONES ÉTICAS

La presente investigación se realizó bajo criterios éticos de integridad, honestidad y responsabilidad, en la que se garantiza que la recolección, el análisis e interpretación de los datos obtenidos se realizaron sin manipulación de estos, realizando el proceso de forma transparente y objetivo. La información obtenida a través de los instrumentos de investigación se utilizó para fines meramente académicos, garantizando confidencialidad y el uso adecuado de la información recopilada. Los colaboradores de la organización fueron previamente informados sobre el cuestionario a aplicar, su propósito y el tratamiento de la información anónima en la presentación de los resultados. No se expuso información de ningún colaborador ya que la encuesta no guardó registros como nombres, cuentas de correo o algún identificativo que mostrará la identidad del encuestado, de esta forma se cumplieron criterios éticos, esto por tratarse de percepciones y experiencias internas y posibles vulnerabilidades asociadas al error humano.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

El presente capítulo detalla las conclusiones como resultado de los análisis realizados mediante la aplicación de los instrumentos de recolección de datos, con relación a los objetivos definidos en la organización. También, se mencionan algunas recomendaciones orientadas a reforzar los programas de capacitación en seguridad de la información en Grupo Vesta SPS, con el fin de mejorar la cultura de seguridad y reducir la probabilidad de incidentes que se puedan presentar por errores humanos.

5.1 CONCLUSIONES

En base a los resultados y su respectivo análisis en función de los objetivos, hipótesis y variables de la investigación se presentan las conclusiones que sintetizan los principales hallazgos relacionados con los métodos de capacitación y su influencia en la reducción del error humano en el manejo de información sensible.

1. Los resultados obtenidos demuestran que existe relación entre la frecuencia y el método de capacitación en seguridad de la información y la reducción de prácticas de riesgo que pueden provocar la pérdida de información sensible en Grupo Vesta, San Pedro Sula. Mediante el cumplimiento del objetivo general, se logró evaluar la influencia de dichos métodos identificando que una adecuada planificación, frecuencia y contenido de las capacitaciones contribuyen significativamente a disminuir prácticas inseguras en los colaboradores. A nivel estadístico, el análisis permitió rechazar la hipótesis nula, confirmando que existe una relación entre la capacitación y la mejora en el manejo de la información, afirmando así que los métodos de capacitación sí influyen en la reducción del error humano. Por tanto, se concluye que la implementación de programas de capacitación efectivos es un factor clave para reducir riesgos, prevenir errores humanos y fortalecer la cultura de seguridad de la información dentro de la organización.

2. La distribución de capacitaciones por área evidencia que no existe uniformidad en la participación del personal, teniendo mayor énfasis en áreas operativas y menor participación en áreas estratégicas. Esto demuestra que, aunque las capacitaciones se lleven a cabo, no se aplican según el nivel de riesgo asociado a cada área. Determinando así que

la modalidad principal implementada fue e-learning (Plataforma en línea), seguido de la modalidad mixta y en un tercer lugar la capacitación presencial. Las áreas a quienes se les ha impartido más capacitaciones presentan menor incidencia de prácticas inseguras, como dejar información visible o reportar pérdida de información por error. Asimismo, la frecuencia de capacitaciones de 1-2 sesiones anuales, sugiere que, aunque la organización ha implementado un plan de capacitación, estas podrían no ser suficientes para reforzar una cultura de seguridad de la información.

Las áreas que actualmente están identificadas como áreas críticas, son OPEX, IT, Créditos y cobros, Facturación, Recursos Humanos y Administración, sin embargo, los resultados demuestran que las 14 áreas identificadas en la recolección de los datos indican que manejan información sensible.

3. Los resultados permiten identificar que los errores humanos más relevantes asociados a la pérdida de información sensible se centran en la exposición de la información en las estaciones de trabajo y en los descuidos por falta de revisión previa. Estas situaciones derivan en consecuencia como en la pérdida, borrado o inaccesibilidad de la información afectando directamente la integridad y disponibilidad de los datos. Asimismo, se evidenció una tendencia significativa en la frecuencia de incidentes en aquellos colaboradores que realizan prácticas inseguras, lo que confirma que acciones como dejar información visible, no verificar antes de enviar o manipular datos sin los debidos controles incrementan el riesgo organizacional. En este sentido, se determina que las malas prácticas del personal influyen directamente en la materialización de incidentes de seguridad, por tanto, el factor humano se consolida como un elemento crítico en la gestión de la seguridad de la información.

5.2 RECOMENDACIONES

En función de los hallazgos obtenidos en la investigación, se plantean las siguientes recomendaciones con el fin de fortalecer los métodos de capacitación en seguridad de la información y contribuir a la reducción del error humano en la organización.

1. Se recomienda fortalecer el programa de capacitación en seguridad de la información o implementar un nuevo programa de capacitación del personal que sea de forma continua con periodicidad trimestral, combinando metodologías teóricas y prácticas e incorporando ejercicios que apoyen a una comprensión más clara y profunda, como por ejemplo ejercicios de phishing, simulaciones y casos reales. Es importante actualizar continuamente los contenidos según las amenazas actuales y evaluar el aprendizaje de los colaboradores para asegurar su efectividad. Asimismo, se sugiere establecer campañas de concientización permanentes, y promover una cultura organizacional orientada a la prevención, donde cada colaborador asuma responsabilidad en la protección de la información sensible.

2. Implementar un programa de capacitación integral y equitativo que abarque todas las áreas de la organización, priorizando aquellas que manejan información sensible. Es necesario combinar modalidades e-learning, presencial y mixta, para mejorar su efectividad. Asimismo, se sugiere realizar un análisis de riesgos por área que permita identificar, evaluar y clasificar el nivel de exposición de cada unidad organizativa frente a posibles amenazas relacionadas con la seguridad de la información. Este análisis debe considerar factores como el tipo de información que se maneja, la frecuencia de uso de datos sensibles y los antecedentes a incidentes. A partir de estos resultados se podrá diseñar un programa de capacitación que permita asignar capacitaciones según su nivel de exposición. Finalmente se debe garantizar la participación obligatoria del personal, implementar registros de asistencia y evaluaciones de aprendizaje y reforzamiento del conocimiento, para monitorear el cumplimiento con el fin de fortalecer una cultura organizacional sólida en la seguridad de la información.

3. Reforzar los controles operativos y las buenas prácticas en el manejo de la información, enfocándose en la prevención del error humano. Es fundamental implementar capacitaciones específicas sobre el manejo seguro de los datos, enfatizando en la revisión previa antes de enviar información, reforzar campañas internas y establecer políticas claras sobre escritorio limpio, bloqueo de equipos y controles de acceso adecuados. También es importante promover auditorías internas y monitoreo constante para detectar prácticas inseguras en el entorno de trabajo.

CAPÍTULO VI: APLICABILIDAD

En este capítulo se presenta de forma breve como los resultados de la investigación pueden implementarse en la práctica. Su propósito es trasladar los hallazgos teóricos a acciones concretas dentro de la organización.

En este apartado se incluye un plan de capacitación orientado a reducir los errores humanos en el manejo de información sensible, así como una matriz de áreas críticas que permite identificar los puntos de mayor riesgo dentro de Grupo Vesta SPS.

En conjunto este capítulo detalla las acciones, recursos y estrategias necesarias para aplicar de forma efectiva los métodos de capacitación demostrando la utilidad del estudio en la mejora de la seguridad de la información en la empresa.

6.1 NOMBRE DE LA PROPUESTA

"Plan de capacitación de seguridad de la información y matriz de identificación de áreas críticas en la empresa Grupo Vesta SPS".

6.2 JUSTIFICACIÓN DE LA PROPUESTA

La presente propuesta se fundamenta en los resultados obtenidos en la investigación, los cuales evidencian que existe relación entre la frecuencia y los métodos de capacitación en seguridad de la información y la reducción de prácticas inseguras por parte de los colaboradores. Las áreas que reciben mayor número de capacitaciones presentan menor incidencia de conductas que pueden provocar la pérdida de información sensible.

Asimismo, se identificó que la frecuencia actual de capacitaciones, que oscila entre una y dos sesiones anuales, podría no ser suficiente para fortalecer una cultura sólida de seguridad de la información dentro de la organización. De igual manera se observó una distribución desigual de las capacitaciones entre las distintas áreas de la empresa, lo que puede generar vulnerabilidades en las áreas que tienen menor participación en estos procesos formativos.

Por otra parte, los resultados permitieron identificar que los errores humanos más frecuentes están relacionados con la exposición de información en estaciones de trabajo y descuidos por falta de revisión previa, lo que puede ocasionar pérdida, eliminación o inaccesibilidad de la información. Ante esta situación, se considera necesario implementar estrategias que permitan reducir estos riesgos.

En este sentido, la implementación de un plan de capacitación continuo y una matriz de identificación de áreas críticas, permitirá identificar las vulnerabilidades, fortalecer las buenas prácticas en el manejo de la información y prevenir incidentes de seguridad derivados del error humano, contribuyendo así a una gestión más eficiente y segura de los activos de información dentro de la empresa.

6.3 ALCANCE DE LA PROPUESTA

La propuesta se enfoca en el diseño de un Plan de capacitación en seguridad de la información y una matriz de identificación de áreas críticas para la empresa Grupo Vesta SPS, con el objetivo de fortalecer el conocimiento de colaboradores sobre el manejo adecuado de la información y prevenir incidentes relacionados con el error humano.

El plan de capacitación está dirigido a las diferentes áreas de la organización, promoviendo buenas prácticas y una mayor conciencia sobre la importancia de la seguridad de la información. Por su parte, la matriz de identificación de áreas críticas permitirá identificar las áreas que presentan mayor nivel de exposición a los riesgos asociados al manejo de la información dentro de la empresa.

Esta propuesta se limita al diseño de estrategias de capacitación y a la elaboración de una herramienta de identificación de áreas críticas que manejan información sensible, las cuales servirán como base para mejorar la gestión de la seguridad de la información en la organización.

6.4 DESCRIPCIÓN Y DESARROLLO A DETALLE DE LA PROPUESTA

La propuesta tiene como fin la implementación de un proceso de evaluación que permita identificar las áreas críticas que manejan información sensible en Grupo Vesta SPS y mediante esta evaluación elaborar un programa de capacitación enfocado en las áreas críticas identificadas que contribuya a disminuir la pérdida de información sensible.

Los resultados obtenidos de la investigación mostraron que existe relación entre los métodos de capacitación y la reducción de errores humanos que producen pérdida de información, los análisis realizados mostraron que las áreas que reciben mayor cantidad de capacitaciones presentan menor incidencia de prácticas que pueden provocar pérdida de información sensible. De igual manera los resultados reflejaron que las capacitaciones se imparten con una frecuencia de una a dos sesiones anuales, y estas no son impartidas de manera uniforme entre las áreas de la organización.

En función de estos resultados, se propone un proceso que permita a la organización identificar áreas con mayor exposición a los errores identificados más frecuentes y determinar los métodos de capacitación adecuados para su mitigación.

ETAPA 1: IDENTIFICACIÓN DE ÁREAS QUE MANEJAN INFORMACIÓN SENSIBLE

En esta etapa se realizará un análisis de las áreas de la organización que manejan información sensible dentro de sus procesos operativos. Para ello se llevará a cabo una revisión de la estructura organizativa de la empresa y de las funciones de cada área, con el fin de identificar aquellas que tienen acceso, manipulación o responsabilidad sobre la información crítica de la organización, estas áreas serán clasificadas según el manejo de información sensible que estas manejen, considerando tres niveles: alto, medio y bajo.

Esta clasificación permitirá identificar las áreas donde un error humano podría generar mayores impactos en términos de pérdida financiera, reputacional o exposición de información. El resultado de esta etapa permitirá determinar qué áreas requieren más sesiones de capacitación en seguridad de la información.

OBJETIVO

Identificar las áreas organizacionales que presentan mayor nivel de exposición al riesgo asociado al error humano por el manejo de información sensible dentro de Grupo Vesta SPS.

METODOLOGÍA

La evaluación de las áreas críticas se llevará a cabo mediante el uso de una matriz de evaluación de criticidad, la cual permitirá analizar cada área de la empresa en base a tres criterios principales basados en los resultados de la aplicación del instrumento de investigación, así mismo se clasificaron en tres niveles de criticidad:

Nivel Alto: Corresponde a áreas que presentan un alto nivel de acceso a información sensible, prácticas inseguras frecuentes o un bajo nivel de capacitación en seguridad de la información. Estas áreas requieren mayor capacitación y concientización.

Nivel Medio: incluye áreas que manejan información sensible de forma ocasional o presentan algunas prácticas que pueden representar riesgo para la seguridad de la información. Estas áreas requieren acciones periódicas de capacitación para fortalecer los conocimientos del personal.

Nivel Bajo: Comprende áreas con acceso limitado a información sensible y que presentan un adecuado cumplimiento de buenas prácticas de seguridad de la información. En este caso las acciones de capacitación estarán orientadas a reforzar la cultura de seguridad en la organización.

CRITERIOS

1. NIVEL DE ACCESO Y MANEJO DE INFORMACIÓN SENSIBLE

Este criterio evalúa el grado en que cada área tiene acceso, manipulación o responsabilidad sobre información sensible dentro de la organización. Es importante mencionar que para esta evaluación se considera como información sensible aquellos datos cuya pérdida, exposición o modificación podría afectar la operación, la confidencialidad o la integridad de la información de la empresa.

Tabla 8. Criterios de evaluación

Nivel	Descripción
Alto	Manejo frecuente de información confidencial, financiera o estratégica.
Medio	Manejo ocasional de información sensible dentro de los procesos del área.
Bajo	Acceso limitado o nula a la información sensible.

Fuente: Elaboración propia

2. PRÁCTICAS DE MANEJO DE INFORMACIÓN

En este criterio evalúa las prácticas cotidianas del personal relacionadas con el manejo de información en su entorno de trabajo, en los resultados de la investigación se identificaron prácticas que pueden incrementar el riesgo de pérdida de información sensible como, por ejemplo:

- Información visible en estaciones de trabajo

- Falta de bloqueo de equipos al ausentarse del puesto
- Manejo inadecuado de documentos confidenciales
- Eliminación accidental de información

Las áreas serán evaluadas considerando la frecuencia con la que estas prácticas se presentan

Tabla 9. Frecuencia de prácticas inseguras

Nivel	Descripción
Alto	Se identifican frecuentemente prácticas inseguras en el manejo de información.
Medio	Se presentan prácticas inseguras de forma ocasional
Bajo	Se observa cumplimiento de buenas prácticas de manejo de información.

Fuente: Elaboración propia

3. NIVEL DE CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Este criterio evalúa el nivel de formación que poseen los colaboradores en temas relacionados con seguridad de la información. Los resultados de este estudio evidenciaron que la frecuencia de capacitación en la empresa se encuentra entre una o dos veces al año, por esta razón, se evaluará el nivel de capacitación considerando la participación del personal en actividades formativas relacionadas con seguridad de la información:

Tabla 10. Nivel de capacitaciones recibidas

Nivel	Descripción
Alto	El área participa regularmente en capacitaciones de seguridad de la información
Medio	El área ha recibido capacitaciones de forma ocasional
Bajo	El área presenta escasa o nula participación en capacitaciones

Fuente: Elaboración propia

Según lo detallado anteriormente para determinar el nivel de criticidad de cada área se utilizará una matriz de evaluación que permitirá analizar los tres criterios y niveles definidos en base a los siguiente:

Tabla 11. Escala de medición

Color	Descripción	Puntaje
Rojo	Criticidad alta	3
Naranja	Criticidad media	2
Verde	Criticidad Baja	1

Fuente: Elaboración propia

Tabla 12. Nivel de criticidad

Puntaje Total	Nivel de criticidad
7-9	Alto
4-6	Medio
< 3	Bajo

Fuente: Elaboración propia

A partir de los valores obtenidos se tendrá como resultado un mapa de calor, en el cual se podrá visualizar el nivel de criticidad de cada área mediante una escala de colores.

Tabla 13. Ejemplo tabla de identificación de áreas críticas

Área	Acceso a información	Prácticas inseguras	Nivel de capacitación	Puntaje Total	Nivel de criticidad
Área 1	3	3	2	8	Alto
Área 2	2	1	2	5	Medio
Área 3	1	1	1	3	Bajo

Fuente: Elaboración propia

ETAPA II: ELABORACIÓN DEL PROGRAMA DE CAPACITACIÓN.

En base a la identificación de las áreas, se elaborará el programa de capacitación teniendo en cuenta las modalidades que mostraron un mayor porcentaje de aprendizaje, este programa detalla las actividades a realizar de forma anual incluyendo sesiones formativas sobre seguridad de la información, ejercicios prácticos, simulaciones y campañas de concientización sobre buenas prácticas de manejo de información. Este programa apoyará a fortalecer el conocimiento del personal y promover la adopción de buenas prácticas seguras en el manejo de la información, contribuyendo a una cultura de seguridad de la información.

OBJETIVO

Implementar un programa anual de capacitación en seguridad de la información, orientado a fortalecer los conocimientos de los colaboradores en mejores prácticas de seguridad y reducir el error humano relacionado con la pérdida de información.

ALCANCE

El programa está dirigido a todos los colaboradores de la organización, sin embargo, se prioriza la participación de aquellas áreas clasificadas como alto y medio riesgo, debido a su mayor exposición a errores humanos por el tipo de información que manejan.

METODOLOGÍA

El programa combinará diferentes métodos de aprendizaje con el fin de facilitar la comprensión de los contenidos por parte de los colaboradores. Entre los métodos de capacitación se utilizarán los siguientes:

- Capacitaciones de forma virtual y presencial
- Ejercicios prácticos
- Simulaciones de phishing
- Campañas de concientización

Las áreas identificadas con un nivel alto de riesgo recibirán un enfoque prioritario dentro del programa de capacitación, este enfoque permitirá orientar los esfuerzos de capacitación hacia áreas donde existe mayor probabilidad de error humano relacionado con la pérdida de información.

La evaluación para medir la efectividad del programa se realizará de forma breve posterior a cada una de las capacitaciones, así mismo se llevará un registro de la asistencia del personal.

Las etapas anteriormente detalladas se fundamentan en los resultados obtenidos de la investigación, así mismo el enfoque metodológico adoptado responde a la naturaleza aplicada del

estudio, ya que busca proporcionar una solución práctica al problema identificado. La propuesta se basa en un enfoque de diagnóstico, que permitirá identificar las áreas críticas antes de definir el plan de capacitación. Este enfoque resulta adecuado, ya que permite orientar estrategias de capacitación hacia las áreas donde existe mayor exposición de riesgo, lo que ayudará a optimizar los recursos destinados a la formación del personal y aumentando la efectividad de las acciones implementadas.

En resumen, la propuesta contribuye directamente al cumplimiento de los objetivos definidos y los resultados de la aplicación del instrumento de investigación, este enfoque permitirá orientar las actividades de capacitación en seguridad de la información, lo que facilitará el conocimiento de los colaboradores con relación al manejo adecuado de información sensible, promoviendo la adopción de buenas prácticas que contribuyan a la reducción de riesgos relacionado con el error humano. Asimismo, la propuesta brinda a la organización una guía práctica que permite planificar y desarrollar las actividades de capacitación a lo largo del año.

6.5 MEDIDAS DE CONTROL

Con el propósito de reducir los errores humanos asociados a la pérdida de información sensible en Grupo Vesta SPS, se establecen las siguientes medidas de control, orientadas a fortalecer la seguridad de la información y garantizar la correcta implementación del plan de capacitación:

Tabla 14 . Medidas de control

Control	Descripción	Indicador	Frecuencia de Medición	Herramienta	Límites aceptables	
					Mínimo	Máximo
Controles de capacitación	Implementar un programa de capacitación, priorizando las áreas de alto riesgo.	Número de capacitaciones implementadas al año.	Semestral	Cronograma de capacitación	6 capacitaciones al año	12 capacitaciones al año
	Establecer evaluaciones posteriores a cada capacitación para medir el nivel de compresión de los colaboradores.	Promedio de calificación obtenida por colaborador %	Después de cada capacitación.	Formularios digitales o pruebas escritas.	70% de aprobación	100% de aprobación
	Llevar un registro de asistencia y participación del personal en todas las actividades formativas.	Porcentaje (%) de asistencia	Por cada sesión	Lista de asistencia	85%	100%
Controles sobre el manejo de información	Establecer políticas para el manejo adecuado de documentos físicos y digitales.	Nivel de cumplimiento de políticas (%)	Trimestral	Auditorías internas, checklist de cumplimiento	80%	100%
	Promover el uso de pantallas de bloqueo al abandonar el puesto de trabajo.	Porcentaje de cumplimiento en bloqueo en equipos	Mensual	Observación directa o auditorías de TI	90%	100%
	Implementar procedimientos seguros para la eliminación de información	Número de incidentes por eliminación adecuada.	Trimestral	Reporte de incidentes	0	2
Controles de monitoreo y seguimiento	Realizar evaluaciones periódicas utilizando la matriz	Nivel de riesgo identificado	Trimestral	Matriz de áreas críticas	reducción del riesgo alto en un 20%	0% incremento en riesgos

Continuación tabla 14

Control	Descripción	Indicador	Frecuencia de Medición	Herramienta	Límites aceptables	
					Mínimo	Máximo
	de áreas críticas para identificar cambios en los niveles de riesgo.					
	Monitorear las prácticas del personal en el manejo de la información.	Número de incumplimientos detectados	Mensual	Auditorías	0 incumplimientos	5 incumplimientos
	Aplicar simulaciones para evaluar el comportamiento de los colaboradores.	Tasa de error en simulaciones %	Semestral	Software de simulación	≤10% de error	25%
Controles de concientización	Desarrollar campañas internas de sensibilización sobre seguridad de la información.	Número de campañas ejecutadas	Trimestral	Correos	4 campañas al año	8 campañas al año
	Fomentar una cultura organizacional orientada a la protección de la información.	Nivel de percepción de seguridad	Semestral	Encuestas de clima organizacional	75% percepción positiva	100%
Controles correctivos	Establecer acciones correctivas ante incidentes de seguridad causados por error humano	Tiempo de respuesta ante incidentes	Por evento	Bitácoras	Menor a 24 horas	72 horas
	Retroalimentar a los colaboradores sobre las fallas detectadas	Porcentaje de colaboradores retroalimentados	Mensual	Reportes, reuniones o correos	90%	100%

Fuente: Elaboración propia.

6.6 CRONOGRAMA DE IMPLEMENTACIÓN

El presente cronograma de implementación tiene como propósito organizar de manera estructurada las actividades necesarias para la ejecución de la propuesta planteada. A través de este instrumento se establecen los tiempos, responsables y secuencia lógica de cada una de las actividades, con el fin de asegurar un desarrollo ordenado y eficiente. Asimismo, el cronograma permite dar seguimiento al avance del proyecto, facilitando la identificación de posibles desviaciones y la toma oportuna de decisiones correctivas. Su aplicación contribuye a optimizar los recursos disponibles y garantizar el cumplimiento de los resultados esperados dentro de los plazos establecidos.

Tabla 15. Cronograma de identificación de áreas críticas

No	Actividad	Descripción	semana1	semana2	semana3	semana4	semana5	semana6	Responsable	Entregable
1	Recolección de información	Identificación de áreas que manejan información							Jefes de áreas TH TI	Listado de áreas
2	Aplicación de matriz de identificación de áreas críticas	Visita a las áreas identificadas y evaluación de criterios según matriz, tabulación de datos y asignación de valores númericos							TH TI	Matriz de identificación de áreas críticas
3	Clasificación de áreas, según nivel de criticidad	Determinación del nivel de criticidad (alto, medio, bajo).							TH TI	Matriz de identificación de áreas críticas
4	Elaboración de mapa de calor de áreas críticas	Presentación visual de resultados							TI Jefes de áreas	Mapa de calor

Fuente: Elaboración propia

Tabla 16. Cronograma de capacitación sobre seguridad de la información

N	Nombre de la Capacitación	Modalidad	Dirigido a	Mes												Ejecución		
				Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	Duración Horas	Fecha	Instructor/ Encargado
1	Introducción a la seguridad de la información	Presencial	Todos los colaboradores													1 hr	29/1/27	Personal de TI asignado
2	Boletín - campaña de concientización sobre escritorio limpio	Correo institucional	Todos los colaboradores													N/A	17/2/27	Personal de TI asignado
3	Taller práctico sobre manejo seguro de información	Presencial	Áreas de riesgo medio y alto													1 hr	29/3/27	Personal de TI asignado
4	Clasificación de la información	Virtual	Todos los colaboradores													1 hr	30/4/27	Personal de TI asignado
5	Ejercicio de simulación de phishing	Correo institucional	Áreas de riesgo medio y alto													N/A	24/5/27	Personal de TI asignado
6	Boletín - seguridad en el puesto de trabajo	Correo institucional	Todos los colaboradores													N/A	28/6/27	Personal de TI asignado
7	Gestión segura de documentos digitales	Virtual	Todos los colaboradores													1 hr	26/7/27	Personal de TI asignado
8	Uso seguro de correo electrónico e identificación de correos sospechosos	Presencial	Todos los colaboradores													1 hr	30/8/27	Personal de TI asignado
9	Gestión de incidentes (Cómo reportar?, qué puedo reportar?)	Virtual	Todos los colaboradores													1 hr	30/9/27	Personal de TI asignado
10	Boletín - uso apropiado de internet	Correo institucional	Todos los colaboradores													N/A	25/10/27	Personal de TI asignado
11	Ingeniería Social	Virtual	Áreas de riesgo medio y alto													1 hr	22/11/27	Personal de TI asignado
12	Boletín - prevención de fuga de información	Correo institucional	Todos los colaboradores													N/A	15/12/27	Personal de TI asignado

Fuente: Elaboración propia

6.7 PRESUPUESTO E IMPACTO DEL PRESUPUESTO

El presupuesto es una herramienta esencial para la planificación y gestión eficiente de los recursos, permitiendo establecer prioridades. En este contexto, la asignación presupuestaria se considera un mecanismo estratégico que permite orientar los recursos hacia iniciativas que generen valor, tal como la capacitación del personal. En consecuencia, el presente análisis aborda el presupuesto como un elemento clave, cuyo impacto trasciende el ámbito financiero para convertirse en un factor determinante en la reducción de riesgos y el fortalecimiento de la cultura de seguridad dentro de la organización.

Tabla 17. Presupuesto

Concepto	Descripción	Cantidad	Costo estimado
Materiales	Diapositivas, imágenes, videos.	Según cada capacitación	L. 0.00
Software	Canvas	1	L, 1360.00
	Teams	112	L. 0.00
	Correo	112	L. 0.00
Tecnología	Computadora	112	L. 0.00
	Data Show	1	L. 2,500.00
	Sonido	1	L. 12,000.00
Recurso Humano	Personal interno involucrado	112	L. 67,200.00
Coffee Break (capacitaciones presenciales)	Café y galletas	112	L. 15,000.00
Mobiliario	Sillas, mesas para capacitaciones presenciales	112 sillas y 18 mesas	L. 8,000.00
Total			**L. 106, 060.00**

Fuente: Elaboración propia

"El ROI es la tradicional fórmula de calcular el retorno de la inversión: beneficio menos inversión, dividido por la inversión. Se puede encontrar en números absolutos o expresado en porcentaje." (Castelló, s. f., p. 4). En pocas palabras el ROI es un indicador que muestra cuánto se gana o se pierde en relación con lo invertido y si esta vale la pena para la empresa. En el contexto de seguridad de la información, el ROI no se mide únicamente en término de ganancias, sino principalmente en función de las pérdidas evitadas derivadas de errores humanos que ocasionen pérdida de información. Con relación a esto en la presente investigación este cálculo se realiza en base a la siguiente fórmula:

$$ROI = \frac{Beneficio - Costo}{Costo} \times 100$$

Donde:

- El costo es la inversión en el programa de capacitación.
- El beneficio es el ahorro generado por la reducción de incidentes provocados por errores humanos.
-

Teniendo en cuenta esto, se presentan dos escenarios basados en supuestos:

En un escenario sin capacitación

No existe un programa de capacitación, por ende, existe mayor probabilidad de que se presente un incidente ocasionado por error humano lo que puede aumentar la tasa de incidentes presentados al año. Teniendo en cuenta esas características se considera el siguiente escenario:
Costo promedio por incidente: **L 100,000**
3 incidentes por año
3×100,000=300,000 **Costo anual de incidentes**

En un escenario con capacitación

Este es el escenario posterior para implementar el programa, lo que ayuda a la reducción de errores humanos y por ende la cantidad de incidentes en la empresa.

Reducción = 50%

300,000×50%=150,000 **Beneficio**

Teniendo en cuenta este escenario y el costo por la implementación del programa de capacitación el cálculo del ROI para Grupo Vesta en base al programa de capacitación implementado es el siguiente:

$$\frac{150,000 - 106,060}{106,060} \times 100 \approx 41.4\%$$

El resultado del ROI permite evaluar para este caso la viabilidad económica del programa de capacitación el ROI >0% indica que la implementación del programa de capacitación no solo contribuye a reducir el error humano, sino que también genera un impacto económico positivo para la empresa. Es importante mencionar que para esta investigación este cálculo adquiere un enfoque preventivo, donde el beneficio se refleja en la disminución de riesgos por la cultura de seguridad que se fomentará por medio de la capacitación y sobre todo la prevención de pérdidas económicas.

6.8 CONCORDANCIA DE LOS SEGMENTOS DE LA TESIS CON LA PROPUESTA

La presente tabla de concordancia tiene como finalidad establecer la relación directa entre los distintos segmentos desarrollados en la tesis y la propuesta planteada. Este instrumento permite evidenciar la coherencia interna del estudio, demostrando como los resultados, conclusiones y hallazgos obtenidos sustentan cada uno de los componentes de la propuesta.

Tabla 18. Concordancia de los segmentos de la tesis con la propuesta de investigación

Capítulo I			Capítulo II	Capítulo III			Capítulo V	Capítulo VI	
Título investigación	**Objetivo General**	**Objetivos específicos**	**teoría/Metodologías de sustento**	**Variables**	**Poblaciones**	**Técnicas**	**Conclusiones**	**Nombre de la propuesta**	**Objetivos propuesta**
Métodos de capacitación que reducen errores humanos en pérdida de información sensible en Grupo Vesta SPS 2026	Evaluar métodos de capacitación que influyen en la reducción del error humano relacionado con la pérdida de Información sensible en Grupo Vesta San Pedro Sula, 2026.	Enumerar métodos de capacitación en ciberseguridad implementados y los colaboradores por área que manejan información sensible.	La ISO/IEC 27001, establece la educación de seguridad de la información en una organización y así mismo ha establecido un sistema para gestionar sus riesgos asociados con la seguridad de la información.	Métodos de Capacitación	Población finita de 112 colaboradores	La encuesta	Se determinó que la modalidad principal fue e-learning (Plataforma en línea), seguido de la modalidad mixta,	Plan de capacitación y Matriz de áreas críticas	Identificar las áreas organizacionales que presentan mayor nivel de exposición al riesgo asociado al error humano por el manejo de información sensible dentro de Grupo Vesta SPS.
		Identificar los errores humanos más relevantes que generan pérdida de información sensible.	Establece una tipología del error humano, derivado de la clasificación de los niveles de ejecución humana en actividades complejas: errores basados en habilidades, errores basados en reglas y errores basados en	Reducción de errores humanos en la pérdida de información sensible.			Los resultados permiten determinar los errores humanos más relevantes: información expuesta en la estación de trabajo, y descuidos por falta de		

Capítulo I			Capítulo II	Capítulo III			Capítulo V	Capítulo VI	
Título investigación	**Objetivo General**	**Objetivos específicos**	**teoría/Metodologías de sustento**	**Variables**	**Poblaciones**	**Técnicas**	**Conclusiones**	**Nombre de la propuesta**	**Objetivos propuesta**
			conocimientos, siendo los últimos los que alcanzan mayor frecuencia de ocurrencia. Enfoque ergonómico: los estudios ergonómicos vinculados a la seguridad se concentran, fundamentalmente, en estudios sobre la carga de trabajo. Se basan en el análisis de la interrelación entre las exigencias de la tarea y los recursos físicos y mentales movilizados por el trabajador para cumplir con estos requerimientos de manera exitosa. Enfoque sistémico: El enfoque sistémico asume que en el ámbito laboral el individuo comete errores que deben ser considerados como consecuencias y no como causas. En este sentido, aporta una serie de postulados que son útiles para la gestión de riesgos:				revisión previa que incurre en la pérdida, borrado o inaccesibilidad de la información.		

Continuación tabla 18.

Capítulo I			Capítulo II	Capítulo III			Capítulo V	Capítulo VI	
Título investigación	**Objetivo General**	**Objetivos específicos**	**teoría/Metodologías de sustento**	**Variables**	**Poblaciones**	**Técnicas**	**Conclusiones**	**Nombre de la propuesta**	**Objetivos propuesta**
			El error es inherente a la condición humana. No es posible cambiar la condición humana, pero sí optimizarla. Las condiciones en las que el trabajador realiza sus funciones sí se pueden modificar, con lo cual se contribuye a optimizar la condición humana. Introducir barreras y defensas permitirá minimizar el error humano en todos los niveles, así como sus consecuencias.						

Fuente: elaboración propia

REFERENCIAS BIBLIOGRÁFICAS

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, *2*, 100031. https://doi.org/10.1016/j.csa.2023.100031

AESA-EY. (2022, noviembre). *Cibersecurity sector in central america*.

Aguilar Antonio, J. M. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. *Estudios internacionales (Santiago)*, *53*(198), 169-197. https://doi.org/10.5354/0719-3769.2021.57067

Aldulaimi, S., Saeed, M., & Yousif, M. (2023). *FORMULATING THE CYBER SECURITY CULTURE IN ORGANIZATIONS: PROPOSING AND ARGUING INSIGHTS*. https://doi.org/10.26668/businessreview/2023.v8i5.1660

Alqahtani, K. S., Albalawi, A. M., & Frikha, M. (2023). REVIEWING OF CYBERSECURITY THREATS, ATTACKS, AND MITIGATION TECHNIQUES IN CLOUD COMPUTING ENVIRONMENT. . . *Vol.*, (6).

Álvarez, A. L., Cruz, J. A., Cruz, S. B., Gallardo, J. de C., López, I. M., & Garcia, R. E. (2024). *El phishing como amenaza en la ciberseguridad corporativa de grandes empresas*. 8. https://doi.org/10.51378/ilia.vi1.8496

Alzahrani, L., & Seth, K. P. (2021). The Impact of Organizational Practices on the Information Security Management Performance. *Information*, *12*(10), 398. https://doi.org/10.3390/info12100398

Báez, Y., Rodríguez, M., De la Vega, E., & Tlapa, D. (2013). *Factores que Influyen en el Error Humano de los Trabajadores en Líneas de Montaje Manual*. https://doi.org/10.4067/S0718-07642013000600001

Becerril, A. (2019). *La ciberseguridad en los Tratados de Libre Comercio*. 28. https://doi.org/DOI%252010.5354/0719-2584.2019.53447

Cabezas, E., & Fiallos, H. (2024). *Simulación de ataques phishing y Planes de Concienciación aplicables al ámbito empresarial – Un enfoque práctico para mejorar la resiliencia organizacional*. 16. https://doi.org/10.33890/innova.v9.n4.2024.2678

Cadenas, S. (2025). *FORMACIÓN PROFESIONAL Y CIBERSEGURIDAD*. 28. https://doi.org/10.31009/IUSLabor.2025.i02.01

Castelló, A. (s. f.). *EL ESTUDIO DEL RETORNO DE LA INVERSIÓN Y EL IMPACTO EN LA RELACIÓN DE LA COMUNICACIÓN EMPRESARIAL Y PUBLICITARIA EN PLATAFORMAS SOCIALES: HERRAMIENTAS DISPONIBLES EN EL MERCADO*.

Centeno, C. M. R. (2017). La brecha existente en la ciberseguridad en Honduras. *Innovare: Revista de ciencia y tecnología*, *6*(2), 58-73. https://doi.org/10.5377/innovare.v6i2.5571

Chaudhary, S. (2024). Driving behaviour change with cybersecurity awareness. *by Elsevier Ltd.*, 15. https://doi.org/10.1016/j.cose.2024.103852

Comisión Nacional de Banca y Seguros. (2022, diciembre 19). *NORMAS PARA LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN, CIBERSEGURIDAD Y CONTINUIDAD DEL NEGOCIO*. https://circulares.cnbs.gob.hn/Archivo/Viewer/2520/025-2022%20NORMAS%20GESTION%20TECNOLOGIAS%20INFORMACION.pdf

da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, *49*, 162-176. https://doi.org/10.1016/j.cose.2014.12.006

El Modelo Kirkpatrick. (2024). https://www.kirkpatrickpartners.com/the-kirkpatrick-model/

Espinoza, E., & Alger, J. (2020). Ética y conducta responsable en investigación: Una mirada a través de la Revista Médica Hondureña. *Revista Médica Hondureña*, *88*(1), 33-37. https://doi.org/10.5377/rmh.v88i1.11597

Fueres, E., Andrade, R., & Yamba, M. (2024). *Protección contra ataques de ingeniería social: Análisis cualitativo de estrategias, tecnologías y patrones específicos*. 16. https://doi.org/10.46652/rgn.v10i44.1310

García, F., Barraza, Í., Flores, A., Soto, C., Fonseca, V., & Martínez, R. (2024). *Examinando la cultura de ciberseguridad en lasorganizaciones de la ciudad de León.* 16.

Ghahramani, M., Shams, G., Zareisaroukolaei, M., & RezaeiZadeh, M. (2024). *Indicadores de evaluación de la eficacia de los cursos de e-learning organizacional*.

HBL Reporte de Ciberseguridad. (2024). *Fundamentos del futuro*. 19.

Hernández Sampieri, R., & Fernandez-Collado, C. F. (2014). *Metodología de la investigación* (P. Baptista Lucio, Ed.; Sexta edición). McGraw-Hill Education.

Hoong, Y., & Rezania, D. (2024). *Navigating Cybersecurity Governance: The influence of opportunity structures in socio-technical transitions for small and medium enterprises*. 15. https://doi.org/10.1016/j.cose.2024.103852

Hughes, K., Meng, L., & Botchey, F. (2021). *Factor humano, un punto débil crítico en la seguridad de la información del Internet de las cosas de una organización*. https://www.cell.com/heliyon/fulltext/S2405-8440(21)00625-

3?_returnURL=https%3A%2F%2Flinkinghub.elsevier.com%2Fretrieve%2Fpii%2FS2405844021006253%3Fshowall%3Dtrue

Jabareen, Y. (2009). Building a Conceptual Framework: Philosophy, Definitions, and Procedure. *International Journal of Qualitative Methods*, *8*(4), 49-62. https://doi.org/10.1177/160940690900800406

Kaur, L., & Mittal, R. (2021). *Variables in Social Science Research*.

Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. *International Journal of Information Security*, *24*(3), 119. https://doi.org/10.1007/s10207-025-01032-0

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, *106*, 102267. https://doi.org/10.1016/j.cose.2021.102267

Kruger, H. A., & Kearney, W. D. (2016). *Un prototipo para evaluar la conciencia sobre la seguridad de la información*. https://doi.org/10.1016/j.cose.2006.02.008

LabCIBE-UNA. (2024, julio 3). *Estado de la Ciberseguridad en Costa Rica*. https://www.unacomunica.una.ac.cr/index.php/julio-2024/5452-concientizacion-y-vulnerabilidad-destacan-en-encuesta-de-ciberseguridad

León, J. (2022). «Sensitive» vs. «Non-Sensitive» Data. En *ResearchGate*. https://www.researchgate.net/publication/367991237_Sensitive_vs_Non-Sensitive_Data

Lundgren, B., & Möller, N. (2019). Defining Information Security. *Science and Engineering Ethics*, *25*(2), 419-441. https://doi.org/10.1007/s11948-017-9992-1

Marousis, A. (2021, abril 6). La formación en ciberseguridad va rezagada, mientras que los hackers aprovechan la COVID-19. *TalentLMS*. https://www.talentlms.com/blog/cybersecurity-statistics-survey/

Marreos, J., Acosta, D., & Mendoza, A. (2023). *Mecanismos de seguridad de la información en una organización: Una revisión sistemática.* https://doi.org/10.54943/ricci.v4i1.384

McMeekin, N., Wu, O., Germeni, E., & Briggs, A. (2020). *How methodological frameworks are being developed: Evidence from a scoping review | BMC Medical Research Methodology*. Enlace de naturaleza de Springer. https://link.springer.com/article/10.1186/s12874-020-01061-4

Meijer, M. W. (2019). *Mplementando el ciclo de aprendizaje experiencial de Kolb mediante el enlace real Experiencia, discusión basada en casos y simulación*. https://doi.org/10.1177/23821205221091511

Mutlutürk, M., Wynn, M., & Metin, B. (2024). *Phishing and the Human Factor: Insights from a Bibliometric Analysis*. 26. https://doi.org/10.3390/info15100643

National Institute of Standards and Technolog. (2024, noviembre 9). *Building an Information Technology Security Awareness and Training Program*.

Ncubukezi, T. (s. f.). *Human Errors: A Cybersecurity Concern and the Weakest Link to Small Businesses*. 9. https://doi.org/10.34190/iccws.17.1.51

NIST, C. C. (2009). *Sensitive information*. https://csrc.nist.gov/glossary/term/sensitive_information

OECD. (2023). *Building a Skilled Cyber Security Workforce in Latin America: Insights from Chile, Colombia and Mexico*. OECD Publishing. https://doi.org/10.1787/9400ab5c-en

Olushola, A., Mayowa, A., & Kushanu, D. (s. f.). *EMPLOYEE CYBERSECURITY AWARENESS TRAINING PROGRAMS CUSTOMIZED FOR SME CONTEXTS TO REDUCE HUMAN-ERROR RELATED SECURITY INCIDENTS*. https://doi.org/10.60087/jklst.vol3.n3.p382-409

Oroni, C., Ndunguru, D., Xianping, F., & Arsenyan, A. (2025). *Mejorar la ciberseguridad en entornos de e-learning mediante la concienciación sobre ciberseguridad y el cumplimiento de la seguridad de la información: Análisis PLS-SEM y FsQCA*. https://doi.org/doi.org/10.1016/j.cose.2024.104276

Ortiz Ocaña, A. (2013). *Modelos pedagógicos y teorías de aprendizaje*.

Paas, F., & . van Merriënboer4, J. (2020). *Cognitive-Load Theory: Methods to Manage Working Memory Load in the Learning of Complex Tasks*. https://doi.org/10.1177/0963721420922183

Parsons, K., McCormac, A., & Butavicius, M. (2014). *Determinación de la conciencia de los empleados mediante el cuestionario de aspectos humanos de la seguridad de la información (HAIS-Q)*. https://doi.org/10.1016/j.cose.2013.12.003

Patel, M., & Patel, N. (2019). *Exploring Research Methodology: Review Article*. (3).

Piñón, L. C., Sapién, A. L., & Gutierrez, M. del C. (2023, diciembre). *Capacitación en ciberseguridad en una empresa mexicana*. 10.

Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security*, *136*, 103585. https://doi.org/10.1016/j.cose.2023.103585

Reidl-Martínez, L. M. (2012). Marco conceptual en el proceso de investigación. *Investigación en Educación Médica*, *1*(3), 146-151. https://doi.org/10.22201/fm.20075057e.2012.03.00007

Reyes, J. (2025). *PHISHING Y ROBO DE IDENTIDAD EN HONDURAS: UN ANALISIS DE LA EFICACIA DE LA REPUESTA DEL SISTEMA JUDICIAL PENAL*.

Sampieri, R., Hérnandez, C., & Baptista, M. del P. (2010). *Metodología de la Investigación*.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). *¿Quién cae en el phish?: Un análisis demográfico de la susceptibilidad y efectividad de las intervenciones al phishing*. https://doi.org/10.1145/1753326.1753383

Sui, J., & Yang, L. (2023). *Eficacia y evaluación del aprendizaje mixto online y offline para un curso práctico de diseño electrónico*. https://doi.org/doi.org/10.4018/IJDET.318652

T. Siponen, M. (2000). *Una base conceptual para la conciencia sobre la seguridad de la información organizacional*. https://doi.org/10.1108/09685220010371394

The IIA. (2026). *Risk in focus*. https://www.theiia.org/globalassets/site/foundation/latest-research-and-products/risk-in-focus/2026/2026-latam-briefing-es-riskinfocus.pdf

Universidad de Minnesota. (2025). *Primary, Secondary, and Tertiary Sources | University of Minnesota Crookston*. Universidad de Minnesota Crookston. https://crk.umn.edu/library/primary-secondary-and-tertiary-sources

Universidad de Nueva Gales del Sur. (2025). *Primary and secondary sources*. UNSW Library. https://www.library.unsw.edu.au/using-the-library/information-resources/primary-and-secondary-sources

ANEXOS

ANEXO I – CUESTIONARIO APLICADO AL PERSONAL DE GRUPO VESTA SPS

Encuesta sobre métodos de capacitación del personal y error humano Grupo Vesta 2026.

Objetivo: Recopilar información precisa sobre las percepciones, prácticas y comportamientos del personal relacionados con los métodos de capacitación en seguridad de la información y la ocurrencia de errores humanos que puedan generar pérdida de información sensible en Grupo Vesta.

Instrucciones: Responda cada una de las interrogantes que a continuación se le presentan, seleccionando la opción que mejor represente su experiencia o percepción. No existen respuestas correctas o incorrectas. Sus respuestas serán tratadas de manera confidencial y utilizadas únicamente con fines académicos.

Cuando envíe este formulario, no recopilará automáticamente sus detalles, como el nombre y la dirección de correo electrónico, a menos que lo proporcione usted mismo.

* Obligatorio

Contenido

1. Edad *

- ◯ 18 – 25 años
- ◯ 26 – 35 años
- ◯ 36 – 45 años
- ◯ 46 – 55 años
- ◯ 56 – 65 años

2. Género *

- ◯ Femenino
- ◯ Masculino

Contenido

3. ¿En qué medida considera que el contenido de las capacitaciones en seguridad de la información es claro y fácil de comprender? *

- ◯ Nada claro
- ◯ Poco claro
- ◯ Regular
- ◯ Claro
- ◯ Muy claro

4. El contenido de las capacitaciones en seguridad de la información es relevante para mis actividades diarias dentro de la organización *

- ◯ Totalmente en desacuerdo
- ◯ En desacuerdo
- ◯ Ni de acuerdo ni en desacuerdo
- ◯ De acuerdo
- ◯ Totalmente de acuerdo

5. ¿Qué tan relevantes considera los temas abordados durante las capacitaciones? *

- ◯ Nada relevante
- ◯ Poco relevante
- ◯ Medianamente relevante
- ◯ Relevante
- ◯ Muy relevante

6. ¿Las sesiones de capacitación incluyeron explicaciones sobre errores humanos comunes y cómo evitarlos? *

- ◯ Totalmente en desacuerdo
- ◯ En desacuerdo
- ◯ Neutral
- ◯ De acuerdo
- ◯ Totalmente de acuerdo

Modalidad

7. ¿Ha recibido capacitaciones relacionados con buenas practicas de seguridad de la información? *

- ◯ Si
- ◯ No

8. ¿Qué modalidad predominó en las capacitaciones que recibió? (marque una) *

- ◯ Presencial
- ◯ E-learning (a distancia)
- ◯ Mixto
- ◯ Micro-learning (módulos breves)
- ◯ Boletines informativos

9. ¿La modalidad de capacitación facilitó su aprendizaje? *

	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
Presencial	◯	◯	◯	◯	◯
E-learning (a distancia)	◯	◯	◯	◯	◯
Mixto	◯	◯	◯	◯	◯
Micro-learning (módulos breves)	◯	◯	◯	◯	◯
Boletines informativos	◯	◯	◯	◯	◯

10. ¿La duración de las sesiones fue adecuada para comprender la información presentada?

- ◯ Totalmente en desacuerdo
- ◯ En desacuerdo
- ◯ Ni de acuerdo ni en desacuerdo
- ◯ De acuerdo
- ◯ Totalmente de acuerdo

Frecuencia y Refuerzo

11. ¿Cuántas sesiones o módulos de capacitación en seguridad de la información recibió en los últimos 12 meses?

- ◯ 0 sesiones
- ◯ 1 – 2 sesiones
- ◯ 3 – 4 sesiones
- ◯ 5 – 6 sesiones
- ◯ Más de 6 sesiones

12. ¿Con qué frecuencia recibe recordatorios o materiales de refuerzo sobre buenas prácticas de seguridad?

	Nunca	Anual	Semestral	Mensual	Semanal
Tips	◯	◯	◯	◯	◯
Boletines informativos	◯	◯	◯	◯	◯
Micro learnings/Módulos breves	◯	◯	◯	◯	◯

Interactividad y Evaluación

13. En las capacitaciones recibidas, ¿con qué frecuencia se incluyeron actividades prácticas? *

	Nunca	Rara vez	A veces	Frecuentemente	Muy frecuente
Simulaciones	◯	◯	◯	◯	◯
Ejercicios	◯	◯	◯	◯	◯
Laboratorios	◯	◯	◯	◯	◯
Correos de Phishing simulado	◯	◯	◯	◯	◯

14. ¿En las capacitaciones recibidas se le aplicó una evaluación o prueba después de la capacitación? (p. ej. quiz, examen, post-test) *

- ◯ Si
- ◯ No

15. ¿Las capacitaciones incluyeron ejemplos o casos prácticos aplicables a su trabajo? *

- ◯ Nunca
- ◯ Rara vez
- ◯ A veces
- ◯ Frecuentemente
- ◯ Siempre

16. ¿Qué tan satisfecho(a) está con la calidad general de las capacitaciones recibidas? *

- ◯ Muy insatisfecho(a)
- ◯ Insatisfecho (a)
- ◯ Ni satisfecho(a) ni insatisfecho(a)
- ◯ Satisfecho(a)
- ◯ Muy satisfecho(a)

Conductas inseguras

17. ¿Las capacitaciones modificaron mis hábitos o rutinas al manejar información sensible? *

- ◯ Totalmente de acuerdo
- ◯ De acuerdo
- ◯ Neutral
- ◯ En desacuerdo
- ◯ Totalmente en desacuerdo

18. ¿Con qué frecuencia deja visible información sensible en su computadora o documentos impresos al retirarse de su puesto de trabajo? *

- ◯ Nunca
- ◯ Rara vez
- ◯ A veces
- ◯ Frecuentemente
- ◯ Siempre

19. ¿Con qué frecuencia guarda, descarga o comparte información sensible en dispositivos o plataformas no autorizadas? *

	Nunca	Rara vez	A veces	Frecuentemente	Siempre
USB personal	◯	◯	◯	◯	◯
Correo personal	◯	◯	◯	◯	◯
Aplicaciones no aprobadas	◯	◯	◯	◯	◯

20. ¿Con qué frecuencia revisa cuidadosamente enlaces o archivos antes de hacer clic para evitar caer en intentos de phishing? *

- ◯ Nunca
- ◯ Rara vez
- ◯ A veces
- ◯ Casi siempre
- ◯ Siempre

21. ¿Con qué frecuencia utiliza contraseñas seguras (complejas, únicas y no compartidas) para acceder a sistemas o información sensible? *

- ◯ Nunca
- ◯ Rara vez
- ◯ A veces
- ◯ Casi siempre
- ◯ Siempre

22. ¿En mi trabajo diario, sigo las políticas y procedimientos de seguridad al manejar información sensible? *

- ◯ Nunca
- ◯ Rara vez
- ◯ A veces
- ◯ Casi siempre
- ◯ Siempre

23. ¿Antes de enviar información sensible, verifico cuidadosamente que el destinatario sea el correcto? *

- ◯ Nunca
- ◯ Rara vez
- ◯ A veces
- ◯ Casi siempre
- ◯ Siempre

Incidentes atribuibles a error humano

24. En los últimos 12 meses, ¿con qué frecuencia ha ocurrido que, por un error suyo, se perdió, borró o quedó inaccesible información sensible? *

- ◯ Nunca
- ◯ Una vez
- ◯ 2-3 veces
- ◯ 4-5 veces
- ◯ Mas de 5 veces

25. En los últimos 12 meses, ¿con qué frecuencia ha ocurrido que, por un error suyo, se envió o expuso información sensible a personas no autorizadas? *

- ◯ Nunca
- ◯ Una vez
- ◯ 2-3 veces
- ◯ 4-5 veces
- ◯ Mas de 5 veces

Conciencia y autoeficacia

26. ¿Considero que un error mío en el manejo de información sensible podría generar consecuencias graves para la organización? *

- ◯ Totalmente en desacuerdo
- ◯ En desacuerdo
- ◯ Ni de acuerdo ni en desacuerdo
- ◯ De acuerdo
- ◯ Totalmente de acuerdo

27. ¿Tengo claro qué la información que manejo en mi trabajo se considera sensible? *

- ◯ Si
- ◯ No

28. ¿Me considero capaz de identificar situaciones en las que podría cometer un error que afecte información sensible? *

- ◯ Totalmente en desacuerdo
- ◯ En desacuerdo
- ◯ Ni de acuerdo ni en desacuerdo
- ◯ De acuerdo
- ◯ Totalmente de acuerdo

29. ¿Cuando tengo dudas sobre cómo manejar información sensible, sé a quién consultar o dónde buscar la información correcta para evitar errores? *

- ◯ Totalmente en desacuerdo
- ◯ En desacuerdo
- ◯ Ni de acuerdo ni en desacuerdo
- ◯ De acuerdo
- ◯ Totalmente de acuerdo

30. ¿Después de las capacitaciones, me siento más seguro(a) al manejar información sensible? *

- ◯ Totalmente en desacuerdo
- ◯ En desacuerdo
- ◯ Ni de acuerdo ni en desacuerdo
- ◯ De acuerdo
- ◯ Totalmente de acuerdo