

MUST UNIVERSITY

MASTER OF SCIENCE IN BUSINESS ADMINISTRATION

FERNANDO ANTONIO COTALLAT PESANTES

**ESTRATEGIA PARA IMPLEMENTAR UN MODELO DE
SEGURIDAD DE DATOS INSTITUCIONAL: UN ENFOQUE
EN NÓMINA Y FINANZAS**

FLORIDA – USA

2024

FERNANDO ANTONIO COTALLAT PESANTES

**ESTRATEGIA PARA IMPLEMENTAR UN MODELO DE
SEGURIDAD DE DATOS INSTITUCIONAL: UN ENFOQUE
EN NÓMINA Y FINANZAS**

Trabajo de Conclusión Final presentado como
requisito parcial para la obtención del título de
MAESTRÍA en el Curso de MASTER OF
SCIENCE IN BUSINESS
ADMINISTRATION de MUST
UNIVERSITY – Florida USA.

Orientador: MSc. Diego Fernando Cardona
Madriaga, PhD.

FLORIDA – USA

2024

LISTA DE TABLAS

Tabla 1 Sistema actual de protección de datos	17
Tabla 2 Capacitación sobre políticas de seguridad de datos.....	18
Tabla 3 Nivel de protección contra ciberataques en finanzas.....	19
Tabla 4 Medidas de confidencialidad en datos	20
Tabla 5 Sistema de organización para detectar violaciones de seguridad	21
Tabla 6 Actualización de políticas de seguridad.....	22
Tabla 7 Gestión de contraseñas en el sistema de finanzas.....	23
Tabla 8 Medidas de prevención en acceso no autorizados	24
Tabla 9 Falta de recursos y la seguridad de datos.....	25
Tabla 10 Políticas de manejo en información en su departamento.....	26

LISTA DE GRÁFICOS

Gráfico 1 Sistema actual de protección de datos	17
Gráfico 2 Capacitación sobre políticas de seguridad de datos.....	18
Gráfico 3 Nivel de protección contra ciberataques en finanzas.....	19
Gráfico 4 Medidas de confidencialidad en datos	20
Gráfico 5 Sistema de organización para detectar violaciones de seguridad	21
Gráfico 6 Actualización de políticas de seguridad	22
Gráfico 7 Gestión de contraseñas en el sistema de finanzas.....	23
Gráfico 8 Medidas de prevención en acceso no autorizados	24
Gráfico 9 Falta de recursos y la seguridad de datos.....	25
Gráfico 10 Políticas de manejo en información en su departamento.....	26

LISTA DE ABREVIATURAS Y SIGLAS

- TI: Tecnología de la información
- ISO: Organización internacional de normalización
- GDPR: Reglamento general de protección de datos
- SI: Seguridad de la información
- CISO: Director de seguridad de la información
- CSIRT: Equipo de respuesta a incidentes de seguridad informática
- NIST: Instituto nacional de estándares y tecnología
- SOC: Centro de operaciones de seguridad
- VPN: Red privada virtual
- ERP: Planificación de recursos empresariales
- MFA: Autenticación multifactor

RESUMEN

El presente estudio posee como objetivo diseñar una estrategia para implementar un modelo de seguridad de datos aplicado en las áreas de y finanzas cumplir los estándares definidos. En referencia a la metodología, se basó en un estudio básico, diseño no experimental, enfoque cuantitativo, la investigación se realizó en una población limitada de 43 empleados del área de soporte técnico de una sucursal de una empresa que labora a nivel nacional, la técnica empleada fue la encuesta, mediante el instrumento de un cuestionario estructurado en base a la escala de tipo Likert. En referencia a los resultados, se evidenciaron diferentes contextos donde se determinó que el 21% determinó que los sistemas siempre protegen los datos, mientras que el 28% indicó que esto se evidencia casi siempre, en base al 51% se determinaron percepciones inciertas o negativas, estos, resultados revelan deficiencias en las políticas actuales en base a la seguridad de datos. En conclusión, es imperativo en fortalecer las medidas preventivas y correctivas mediante el modelo seguro que contempla las revisiones periódicas, actualizaciones y programas que capacitan a concienciar el personal sobre la seguridad de datos. La estrategia debe centrarse en asegurar que los sistemas sean más eficaces, fiables y aptos para evitar infracciones de seguridad, favoreciendo de esta manera un tratamiento más seguro y eficaz de la información en estos sectores críticos.

Palabras clave: Seguridad de datos. Nómina. Finanzas. Capacitación. Estrategias.

ABSTRACT

The objective of this study is to design a strategy to implement a data security model applied in the areas of finance and compliance with the defined standards. In reference to the methodology, it was based on a basic study, non-experimental design, quantitative approach, the research was carried out in a limited population of 43 employees of the technical support area of a branch of a company that works at the national level, the technique The survey was used, using the instrument of a structured questionnaire based on the Likert-type scale. In reference to the results, different contexts were evident where it was determined that 21% determined that the systems always protect the data, while 28% indicated that this is evident almost always, based on 51% uncertain or negative perceptions were determined. These results reveal deficiencies in current policies based on data security. In conclusion, it is imperative to strengthen preventive and corrective measures through the secure model that includes periodic reviews, updates and programs that train staff to raise awareness about data security. The strategy should focus on ensuring that systems are more effective, reliable and capable of avoiding security breaches, thus promoting more secure and effective processing of information in these critical sectors.

Keywords: Data security. Roster. Finance. Training. Strategies.

ESTRATEGIA PARA IMPLEMENTAR UN MODELO DE SEGURIDAD DE DATOS
INSTITUCIONAL: UN ENFOQUE EN NÓMINA Y FINANZAS

31 de diciembre del 2024

SUMARIO

1. Introducción	1
1.1 Planteamiento del problema.....	2
1.2 Objetivos del estudio.....	3
1.2.1 Objetivo General.....	3
1.2.2 Objetivos Específicos.....	3
1.3 Justificación	3
1.4 Alcance y limitaciones	4
1.4.1 Alcance	4
1.4.2 Limitaciones.....	4
2. Fundamento Teórico	6
2.1 Seguridad de datos	6
2.2. Modelos de seguridad de datos	6
2.3. Riesgos en las áreas de nómina y finanzas	7
2.4. Normativas relevantes.....	8
2.5. Estrategias de seguridad física empresarial	9
2.6. Seguridad del ambiente y gestión de desastres	10
2.7. Tecnologías emergentes en seguridad empresarial.....	11
2.8. Revisión de incidentes de seguridad.....	12
2.9. Procedimiento de elaboración de estrategias de seguridad.....	12
3. Metodología	14
3.1 Tipo de estudio.....	14

3.2 Enfoque de estudio.....	14
3.3 Diseño de estudio.....	14
3.4 Población y muestra de estudio.....	15
3.5 Técnica e instrumentos de estudio	15
4. Resultados	17
4.1 Análisis de resultados	17
5. Consideraciones finales	27
Referencias Bibliográficas.....	29
Anexos	33

1. Introducción

En el actual entorno se ha determinado que las organizaciones enfrentan un aumento de complicaciones en cuanto a la protección y gestión de datos sensibles, esencialmente en zonas críticas como la de finanzas y nóminas donde la información personal y financiera de los proveedores y empleados debe ser resguardada rigurosamente, la digitalización de los procesos ha causado un beneficio pero también tiene un aumento de complicaciones que se relaciona con la filtraciones ciberataque y acceso no autorizado por lo cual es importante que las instituciones puedan implementar un modelo de datos seguro que no solamente cumplan con estas normas, sino que, además, integre la disponibilidad y confidencialidad de los datos.

Este estudio se enfoca en diseñar una estrategia para implementar un modelo de seguridad de datos institucional esencialmente los que se encuentra dirigido en área de nómina y finanzas, con el propósito de cumplir todos los estándares de protección de datos la seguridad en esta área es importante no solamente para evitar pérdidas económica, sino que, además de asegurar la confianza de los usuarios y proveedores los cuales confían sus datos de manera responsable y segura mediante un enfoque integrado se pretende establecer diferentes medidas métodos de detección de incidente y la rápida respuesta ante posibles complicaciones en la seguridad los cuales se alinean organizaciones que tienen las mejores prácticas internacionales para proteger los datos relevantes.

En cuanto al desarrollo tuyo será determinado dentro del capítulo 1 la presentación de la introducción, el planteamiento del problema, el objetivo del estudio, la justificación de la investigación, el alcance y las limitaciones del estudio, destacando así la relevancia de desarrollar una estrategia basada en la seguridad de datos y las áreas mencionadas. En cuanto el capítulo 2 se ha determinado el análisis del marco teórico abordando diferentes conceptos importantes sobre la seguridad de datos vulneraciones amenazas específicas en cuanto a las finanzas y la nómina.

El desarrollo del capítulo 3 se detalla la metodología de la investigación que se utilizó en el correspondiente estudio explicando el enfoque el diseño de investigación las técnicas y el análisis de datos además de la población y la muestra de estudio. En referencia el capítulo 4 se exponen los resultados que se obtiene mediante la implementación de una estrategia propuesta evaluación decir la efectividad y la posición de las mejoras. En cuanto el capítulo 5 se ofrecen las diferentes conclusiones que se relacionan con los hallazgos planteados durante la obtención de información relacionada con la seguridad de datos en una organización.

1.1 Planteamiento del problema

Hoy en día, el ámbito empresarial se encuentra con un ambiente crecientemente digital, en el que la administración de la información delicada se ha convertido en esencial para el funcionamiento y la viabilidad de las organizaciones, las áreas de sueldos y finanzas son particularmente susceptibles, dado que gestionan información delicada como datos personales de los trabajadores, sueldos, pagos a proveedores y estados financieros, no solo es esencial esta información para el correcto funcionamiento de la empresa, sino que también representa un blanco atractivo para ciberataques, estafas internas y fallos humanos.

El aumento en la complejidad de las amenazas cibernéticas ha motivado a numerosas instituciones a reevaluar sus estrategias en relación a la protección de datos, no obstante, frecuentemente se topan con retos considerables al tratar de establecer un modelo de seguridad sólido, la ausencia de una estrategia definida es uno de los desafíos más críticos, dado que numerosas organizaciones no poseen un esquema completo que les facilite reconocer, valorar y minimizar los riesgos de forma eficaz.

Los recursos escasos, ya sean financieros o humanos, constituyen otro obstáculo significativo que las organizaciones necesitan vencer, las empresas pueden carecer del presupuesto requerido para invertir en soluciones de ciberseguridad avanzadas o en la

contratación de especialistas en el campo, esto podría provocar una excesiva dependencia de tecnologías anticuadas y la ausencia de inversiones en formación constante para el personal.

¿Cómo se puede diseñar de manera efectiva una Estrategia para la Implementación de un modelo de seguridad de datos institucional en las áreas de nómina y finanzas? ¿Cuáles son los principales riesgos de seguridad de información en las áreas de nómina y finanzas? ¿Qué modelo de seguridad de información es el idóneo para implementar en estas áreas? ¿Cómo se puede asegurar el cumplimiento normativo y la eficiencia operativa mediante este modelo?

1.2 Objetivos del estudio

1.2.1 Objetivo General

- Diseñar una estrategia para implementar un modelo de seguridad de datos aplicado en las áreas de y finanzas cumplir los estándares definidos

1.2.2 Objetivos Específicos

- Sugerir un modelo de seguridad de datos que contenga medidas preventivas, detección de incidentes y respuestas antes ataques, errores humanos o fugas de información.
- Analizar las amenazas específicas y las vulnerabilidades comunes que afectan a la seguridad de los datos en las áreas de nómina y finanzas.
- Identificar las mejores prácticas internacionales y marcos normativos aplicables a la protección de datos en estas áreas.

1.3 Justificación

Esta investigación se basa en la necesidad creciente de salvaguardar la información sensible y crítica que gestionan las áreas de salarios y finanzas en las organizaciones, estas áreas tienen la tarea de administrar datos delicados, que incluyen datos personales de los empleados, información acerca de los sueldos y los pagos a proveedores, además de informes

financieros esenciales para el funcionamiento de la compañía, frente a la digitalización de los datos, la vulnerabilidad frente a ataques cibernéticos, fraudes internos y fallos humanos ha aumentado significativamente.

Este análisis tiene como objetivo desarrollar una estrategia que facilite la implementación de un modelo eficiente de seguridad de datos institucional, centrado en los sectores de nómina y finanzas, el propósito de la puesta en marcha de esta estrategia no solo es salvaguardar la información delicada, sino también reducir los riesgos vinculados a la actividad cotidiana de las empresas, ya sea por sucesos externos o internos.

1.4 Alcance y limitaciones

1.4.1 Alcance

El objetivo principal de este proyecto es el diseño y puesta en marcha de una estrategia de seguridad de datos centrada en los sectores de nómina y finanzas dentro de una entidad, esta estrategia se enfocará en implementar políticas y procedimientos que robustezcan la salvaguarda de datos delicados, como la información de los empleados, sueldos, pagos a proveedores e informes financieros, con la finalidad de reducir los peligros vinculados a ciberataques, fraudes internos y fallos humanos, además, el ámbito abarca no solo la implementación de soluciones tecnológicas, sino también la formación del personal en métodos seguros de gestión de datos, garantizando de esta manera una administración completa de la seguridad de los datos.

1.4.2 Limitaciones

El proyecto también tiene algunas restricciones que pueden afectar su ejecución, entre las posibles resistencias al cambio organizacional, que podría obstaculizar la implementación de nuevas políticas y tecnologías de seguridad. Igualmente, hay limitaciones en relación a los recursos a disposición para la puesta en marcha de sistemas de seguridad sofisticados, lo que

podría restringir la aplicación de las herramientas y tecnologías implementadas, es necesario una constante actualización ante las amenazas emergentes en ciberseguridad, lo que representa un desafío para preservar la eficacia del modelo de seguridad a lo largo del tiempo.

2. Fundamento Teórico

2.1 Seguridad de datos

La seguridad de datos es un componente importante para poder sobre guardar la información crítica y sensible de una entidad este proceso incluye diferentes estrategias y políticas que se diseñan para protección de información frente a acceso no permitido alteraciones o ciberataque que se conforman de acuerdo a las actividades corporativas la seguridad de datos se vuelve un factor importante ya que asegura solamente la disponibilidad de la información y la integridad, sino que, también permite la confianza de los usuarios instaurando un sistema importante de protección requiriendo si un análisis continuo de la vulnerabilidades y e implementación de la tecnología actuales para la infraestructura como los procesos de gestión de datos (Carvajal & León, 2021).

La tecnología de seguridad y la protección de datos requiere una sensibilización y diseño de método seguro los fallos humanos son una de las principales importancias de las infecciones en la seguridad debido a la formación y entrenamiento, lo que se establece el protocolo de protección resultan importante para reducir los peligros y teniendo en cuenta la organización de seguridad, también ha ido robustecer la protección de datos internos y externo promoviendo el ambiente donde cada integrante de la organización adoptando rol importante de información delicada (Lucas et al., 2022).

2.2. Modelos de seguridad de datos

Los modelos de seguridad de datos son estructuras conceptuales con metodología que guían la defensa de apuntes considerables y fundamentales en una corporación, estos ejemplares incluyen directrices, métodos y ciencias que, al englobarse, forman una resistente garantía que contra ingresos denegados, y reformas y descuido de apuntes, al crear un ejemplar de infalibilidad, es indispensable distinguir las peticiones comunes de la corporación, sus contingencias específicas y el margen normal con el que encontrará la

solución con la finalidad de que el ejemplar brinde las necesidades y fines de la corporación (Coronel & Quirumbay, 2022).

Los modelos de seguridad están basados comúnmente en el usuario y el personal de dominio de accesibilidad los cuales son dos ejemplares que sobresalen, el primero está direccionado en poner un límite a la indagación según el rol y el desenvolvimiento particularmente que este tenga dentro de la organización, demostrando que solamente van a tener accesibilidad los colaboradores que mantengan tareas determinadas dentro de los modelos, esta táctica ayuda a disminuir el riesgo de la restricción por difusión de información a una parte de participantes específicos, lo que va a dar como resultado principalmente el que se va a beneficiar es el sector financiero junto a la nómina, donde los ejemplares van a estar más susceptibles (Coronel & Quirumbay, 2022, p. 45).

Igualmente, el modelo va a brindar seguridad a los apuntes que constantemente deben estar en actualización y revisión, para que se puedan incorporar los distintos dictámenes tecnológicos, junto con el avance de la progresión cibernética que se puede encontrar en las amenazas, por lo cual, se va a exigir a las autoridades que exista un cambio constante en las políticas que brindan seguridad, ya que esto no solamente va a ayudar a que exista una mejora en la seguridad de las herramientas, así como también va a forjar formación personal y va a existir una constante indagación de los estatutos que ya están establecidos (Tenelema et al., 2020).

2.3. Riesgos en las áreas de nómina y finanzas

Las áreas de nómina y finanzas se encuentran característicamente puesta a diferentes riesgos como la confidencialidad y la información crítica que se gestiona en el contexto de la nómina, la divulgación de datos personales los números telefónicos y las cuentas bancaria de los usuarios puede resultar en robos de identidad y estafas económicas (Loaiza, 2022).

En el área financiera la gestión de datos vinculadas a ingresos costos pagos e inversiones a proveedores se transforman en este sector un objetivo atractivo para los ataques cibernéticos otra de las amenazas de ciberseguridad es el acceso no autorizado a estos datos, provocando alteraciones de contabilidad teniendo un impacto en las decisiones y riesgos de supervisión (Carrillo, 2021).

Los ataques cibernéticos constituyen en diferentes fallos humanos o siendo otro de los peligros que se encuentran expuestos lo que vinieron impacto directo en la información financiera y la exactitud en las normas, por tal motivo, resulta importante establecer diferentes estrategias de protección de datos incluyendo la tecnología de seguridad, sino que, también las políticas de capacitación y los procesos que reducen los riesgos relacionados con las intervenciones humanas (Lascano, 2023).

2.4. Normativas relevantes

Dentro del contexto de la seguridad de datos hay regulaciones fundamentales que orientan a una organización para salvaguardar y destinar de forma adecuada al relato importante en lo que corresponde a las nóminas y las finanzas, en cuanto a las normas más sobresalientes se determina la protección de datos en la Unión Europea que dicta diferentes normas rigurosas para el manejo de información personal, este tipo de regulación establece una responsabilidad para asegurar la integridad privacidad y disponibilidad de datos con penalizaciones significativo en caso de que exista algún incumplimiento (Saa, 2023).

Otra de la regularizaciones significativas de la ley Sarbanes-Oxley (SOX) en Estados Unidos que se aplica esencialmente para la integridad de la información financiera y contabilidad en diferentes entidades este tipo de ley impone normas estrictas en cuanto a la comprobación y se va a abordar datos financiero forzando así a las organizaciones imponer

en marcha diferentes auditorías internas, así como métodos tecnológicos que puedan asegurar la protección de registro financiero (García, 2019).

En el Ecuador la legislación principal es la vinculación desde salvaguardar la información mediante una Ley Orgánica de Protección de Datos Personal que fue establecida en el año 2021, esta normativa define un contexto jurídico basado en el manejo recopilación y salvar guardar datos personales en todo territorio ecuatoriano, se encuentra inspirado en diferentes fundamentos basado en un reglamento de protección de datos de la Unión Europea la cual tiene como objetivo asegurar la privacidad y el control de la población aumentando diferentes hábitos seguros y responsable en la administración de datos privado y público en diferentes entidades (Rovira et al., 2023).

2.5. Estrategias de seguridad física empresarial

La seguridad física empresarial es un componente importante para salvaguardar recursos y activos de una organización tratando como una utilidad, de acuerdo a su infraestructura como protección de los usuarios y los recursos materiales, una de las estrategias importantes de marcha de diferentes controles que supervisan y limitan el ingreso y egreso de personas a diferentes áreas que se encuentra el sistema digital, como tarjeta de identificación, código de acceso, lectores biométricos, no solamente este tipo de control puede restringir el acceso a diferentes personas, sino también, que se dispone el paso para personal autorizado (Estupiñán & Obando, 2019).

Una estrategia eficiente de un sistema de vigilancia continuo aplicado en diferente cámara de seguridad, este método de seguimiento a distancia atienden a diferentes zonas estratégicas de una empresa teniendo la supervisión para poder detectar acciones sospechosas y riesgosas, para poder tener una reacción pronta ante posibles amenazas, además, se dispone

un centro de vigilancia en tiempo real lo cual mejora el proceso de coordinación y situaciones de emergencia disminuyendo así el peligro por pérdida o robos (Ríos et al., 2019).

Finalmente, una de las estrategias de seguridad física se sitúan en los planes contingentes teniendo diferentes respuestas ante situaciones de catástrofes, incendios o vulneraciones de seguridad, al llevar a cabo este tipo de ejercicios se realiza una proporción de capacitaciones basada en la seguridad las compañías, no solamente disminuyen el efecto de los sucesos negativos, sino que, también promueve la cultura de seguridad entre los usuarios y los trabajadores creando así un ambiente más seguro y resguardado ante peligros físicos (Londoño et al., 2022).

2.6. Seguridad del ambiente y gestión de desastres

La protección de datos es un componente importante para cualquier entidad debido a que se protegen información delicada es importante para poder tener una integridad y el correcto desempeño de diferentes organización en un ambiente digital complejo, las entidades se toman siempre con diferentes complicaciones como la integridad privacidad y accesibilidad de información es relevante (Lecca et al., 2023).

La administración de datos conlleva diferente situaciones como reconocer y minimizar los peligros vinculados con la accesibilidad y la pérdida de datos se consigue esto mediante una puesta en marcha de política de seguridad sólida, la aplicación de tecnología de vanguardia como el cifrado y autenticación multifactorial, dentro de este proceso es necesario llevar auditoría regular y evaluar la vulnerabilidad para poder detectar diferentes fallos en la seguridad y asegurar las acciones puestas en marcha que sean eficientes (García, 2020).

Por último, es importante fomentar la cultura de seguridad de datos dentro de una empresa debido a que todos los empleados desde la dirección superior ante el personal básico puede entender la importancia de asegurar la información de cada uno de los empleados, así

mismo se promueve un entorno de protección de datos siendo una prioridad compartida no solamente para mejorar este tipo de datos, sino que, también son medidas de protección que contribuyen a evitar diferentes complicaciones o fallos humanos que podrían derivar este tipo de infecciones por seguridad de información (Saltos, 2023).

2.7. Tecnologías emergentes en seguridad empresarial

La tecnología en auge en el área de seguridad empresarial está siendo transformada año a año, diferentes empresas reguladoras tienen recursos e importantes dentro de tecnología como la inteligencia artificial después tiene un rol fundamental así todos los procesos de seguridad y la detención de diferentes patrones dentro de la conducta de cada usuario (Bayo & Calderón, 2021).

Otra tecnología importante es la cadena de bloques lo cual proporciona un método descentralizado para poder administrar diferentes datos y operación según la estructura constante y clara, no solamente aumenta la protección de datos, sino que, además disminuye la posibilidad de fraude y complicación la compañía pueden aplicar el blockchain para garantizar registro financiero mediante diferentes operaciones, brindando así una confianza y protección para los usuarios (Corredor & Díaz, 2019).

El internet también ofrece diferentes oportunidades de reto dentro de la seguridad de los negocios diferentes aparatos se vinculan en internet de un sistema de control y como pueden ser las cámaras de vigilancia, lo cual potencia la seguridad dentro de un establecimiento, también es importante tener en cuenta que la tecnología de seguridad creada por el IoT como red privadas y soluciones de encriptación resultan ser importantes para poder salvaguardar este tipo de información que se la gestiona dentro de los aparatos informáticos (Campillo, 2021).

2.8. Revisión de incidentes de seguridad

El análisis de diferentes procesos incidente en la seguridad es una situación importante lo que posibilita diferentes organizaciones, emprender y valorar las diferentes sucesos que han puesto en riesgo la seguridad de los métodos informáticos, este proceso conlleva la recolección y estudio de datos acerca de suceso anterior con el propósito de detectar diferentes patrones causan diferentes falencias en las estrategias de seguridad (Villarreal & Gorozabel, 2023).

La evaluación de incidentes de seguridad logra realizarse mediante diferentes métodos que comprenden auditorías internas análisis y simulaciones de ataque los cuales se evalúan constantemente y se determina los elementos técnicos como los procedimientos organizativos que pueden tener diferentes errores, es posible estudiar las propiedades de la red teniendo en cuenta los protocolos de acceso y la práctica de gestión de datos (Tugnarelli, 2019).

Además, es importante transmitir y documentar los procesos de revisión incidentes para poder tener una mejor transparencia y perfeccionamiento constante, es fundamental que la enseñanza adquirida no solamente sean difundidas al equipo de seguridad, sino que, además toda la organización promueve un mayor entendimiento en base a la seguridad (C. Carvajal, 2019).

2.9. Procedimiento de elaboración de estrategias de seguridad

El procedimiento para segmentar diferentes fases y la elaboración de estrategia de seguridad es necesario tener en cuenta lo siguiente;

- Evaluación de riesgo es una etapa esencial donde se ejecuta un estudio detallado sobre los diferentes activos de la organización para poder tener en cuenta que son delicados y esenciales

- El establecimiento de propósito de seguridad una vez detectado los diferentes riesgos se definen cuáles son las seguridades más concretas y precisas este tipo de meta deben estar en sintonía con la visión y la misión de la organización, además de los propósitos operativos y estratégicos de cada uno.
- La elaboración de políticas y procedimientos son las metas establecidas se llevan a cabo mediante una ejecución de política de seguridad y procesos operativos los cuales se orientan en base a las estrategias establecidas.
- El establecimiento de medida de seguridad se sitúa en una fase que enviaba una implementación de diferentes políticas y procesos establecidos acorde a la organización.
- El seguimiento y la evaluación es una fase donde se implementa mediante las estrategias de seguridad lo cual resulta impredecible implementando un método de vigilancia constante para una medida efectiva.
- La actualización y avance constante de una mejora continua se lleva en relación a la seguridad de un proceso lo cual es importante actualizar y revisar las estrategias de forma regular para poder acoplarla a las variaciones en el entorno tecnológico (Pérez et al., 2019).

3. Metodología

3.1 Tipo de estudio

En este estudio se emplea un tipo de investigación básica o fundamental la cual se sitúa en la creación de un contexto teórico conceptual vinculado al tema en relación.

Es importante determinar que el estudio básico se enfatiza en la prevención de un concepto teórico vinculado con problemas concreto teniendo en cuenta la tensión y la comprensión de los diferentes principios basados en un enfoque donde se diseñan diferentes modelos y teorías conceptuales que se pueden aplicar el funcionamiento como futuros estudios siendo esencial para diferente progreso académico (Rodríguez, 2020).

3.2 Enfoque de estudio

En base al enfoque de estudio, en esta investigación se estableció la metodología cuantitativa basada en el análisis estadístico de cada una de las respuestas que se obtendrán de los participantes.

La metodología cuantitativa se particulariza por la utilización de diferentes datos y técnicas estadísticas que facilitan el proceso de medición mediante instrumento como encuesta, este método se intensifica creando vínculos y patrones que permiten la recopilación de datos numéricos (Márquez et al., 2020).

3.3 Diseño de estudio

El diseño de estudio se enfatiza en un tipo no experimental lo cual significa que no se ejecutarán ninguna modificación en las variables establecidas como tal en el estudio ni se registrarán supervisiones en cuanto a las condiciones de la investigación.

Este diseño se enfoca en el análisis y observación de los problemas que surgen en un entorno natural, sin intervención ni modificación en el progreso del estudio, esto simplifica la recopilación de información pertinente vinculada con las variables en estudio, un diseño no experimental se distingue

por examinar fenómenos en un entorno cotidiano, evitando la intervención en las variables (Ramos, 2021).

3.4 Población y muestra de estudio

La población de estudio se la considera al personal que laboran el área de soporte técnico de una empresa asegurando datos a nivel nacional en todas las sucursales de dicha institución.

La población de estudios se basa en el conjunto total de personas que tienen diferentes radios similares y son el propósito de un estudio simbolizando diferentes conjuntos, los cuales se pretenden recopilar la información basadas diferentes interrogantes relacionadas con el problema de estudio (Otzen & Manterola, 2019).

La muestra de estudio se conforma por 43 personas que laboran dentro de un área de soporte técnico, se considera toda la población como parte del estudio investigativo al ser muy limitada.

La muestra de estudio se lo considera también como un segmento del universo de la población total, donde se ejecuta la investigación existen diferentes métodos para poder establecer un número o una cantidad de muestra por medio de fórmulas o lógicas, la muestra representa una proporción representativa del universo de la investigación (J. A. García et al., 2019).

3.5 Técnica e instrumentos de estudio

En este estudio se emplea la encuesta como parte de la recopilación de información lo que facilita la adquisición de datos constitutivos mediante un cuestionario estructural que es gestionado por todos los participantes del estudio.

La encuesta es un proceso eficiente que permite la recopilación de datos estandarizados en un conjunto de personas permitiendo de esta manera establecer diferentes

patrones y tendencias en cuanto a la respuesta, lo que resulta importante para alcanzar los propósitos establecidos dentro de la investigación (Casas et al., 2023).

El método de recopilación de datos es un instrumento importante lo cual se sitúa en un cuestionario estructurado con diferentes opciones de respuesta tipo Likert lo que facilite la evaluación de diferentes actitudes y percepciones de los participantes en relación a los métodos evaluativos del estudio.

Es importante determinar que el cuestionario es un instrumento que facilite el proceso y análisis de información ofreciendo así diferentes opciones de respuesta predefinida, lo que permite una evaluación en cuanto a nivel de acuerdo o desacuerdo en vinculación con cada enunciado, es importante tener en cuenta la consistencia de las respuestas que se obtiene mediante la interpretación de varios resultados confiabilidad y validez (Bracho et al., 2021).

4. Resultados

4.1 Análisis de resultados

1. ¿Considera que el sistema actual protege adecuadamente los datos sensibles en el área de nómina y finanzas?

Gráfico 1 Sistema actual de protección de datos

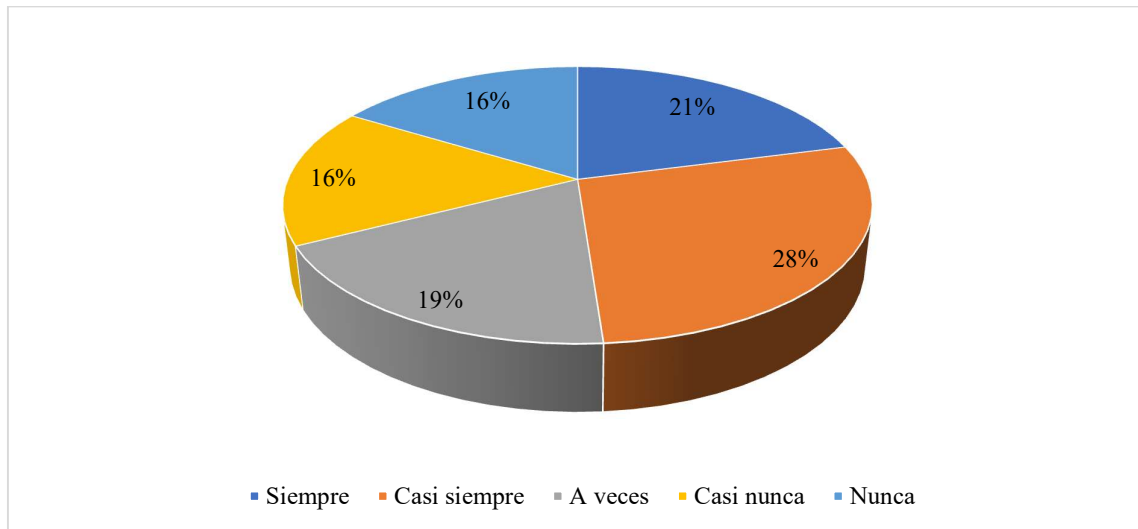


Tabla 1 Sistema actual de protección de datos

Variables	Frecuencia	Porcentaje
Siempre	9	21%
Casi siempre	12	28%
A veces	8	19%
Casi nunca	7	16%
Nunca	7	16%
Total	43	100%

Análisis e interpretación: Los hallazgos muestran una opinión dividida acerca de la salvaguarda de datos delicados en el sector de nómina y finanzas, dado que únicamente el 21% de los participantes en la encuesta piensa que el sistema "siempre" asegura la seguridad, mientras que un 28% considera que esto sucede "casi siempre", sumando un 49% con perspectivas moderadamente favorables. No obstante, más del 50% de los participantes (51%) posee percepciones negativas o desconocidas, que varían entre "en ocasiones" (19%),

"casi nunca" (16%) y "nunca" (16%). Este escenario pone de manifiesto la necesidad de perfeccionar los actuales sistemas de seguridad, incrementar la confianza de los usuarios y asegurar la puesta en marcha eficaz de medidas que salvaguarden los datos delicados, teniendo en cuenta que las opiniones adversas podrían estar asociadas a fallos en los protocolos vigentes.

2. ¿Con qué frecuencia recibe capacitación sobre políticas de seguridad de datos en su área de trabajo?

Gráfico 2 Capacitación sobre políticas de seguridad de datos

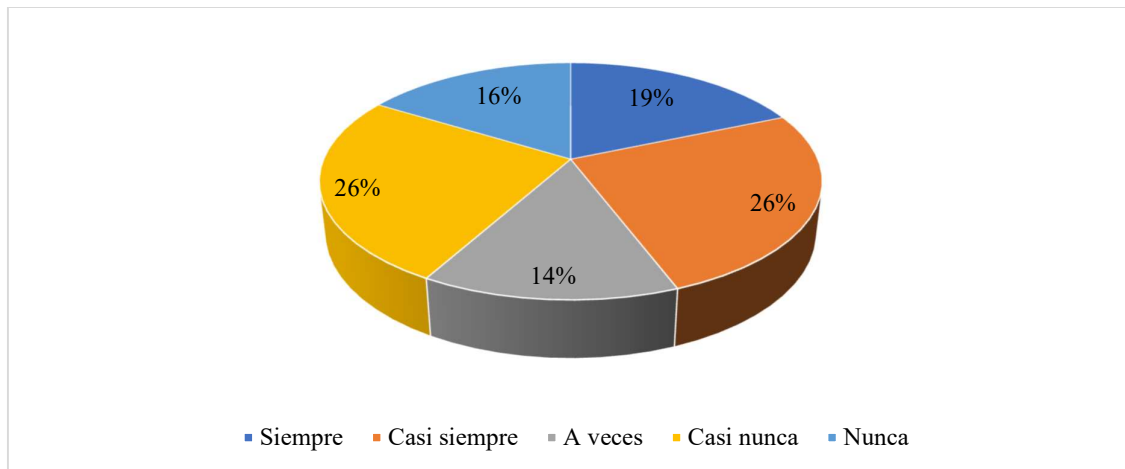


Tabla 2 Capacitación sobre políticas de seguridad de datos

Variables	Frecuencia	Porcentaje
Siempre	8	19%
Casi siempre	11	26%
A veces	6	14%
Casi nunca	11	26%
Nunca	7	16%
Total	43	100%

Análisis e interpretación: Los hallazgos indican que la formación en políticas de seguridad de datos en el entorno laboral es vista como deficiente o irregular, dado que únicamente el 19% de los participantes en la encuesta sostiene recibirla "siempre" y un 26% "casi siempre", lo que equivale a apenas el 45% de respuestas favorables. En contraposición, un porcentaje considerable de participantes (55%) manifiesta opiniones negativas o inciertas, que oscilan

entre "en ocasiones" (14%), "casi nunca" (26%) y "nunca" (16%). Estos datos indican la necesidad de incrementar la regularidad y la calidad de las formaciones, dado que la ausencia de capacitación constante podría poner en riesgo la adecuada aplicación de las políticas de seguridad y, en consecuencia, la salvaguarda eficaz de los datos delicados en el ambiente de trabajo.

3. ¿Qué tan efectivo considera el nivel de protección contra ciberataques en los sistemas de nómina y finanzas?

Gráfico 3 Nivel de protección contra ciberataques en finanzas

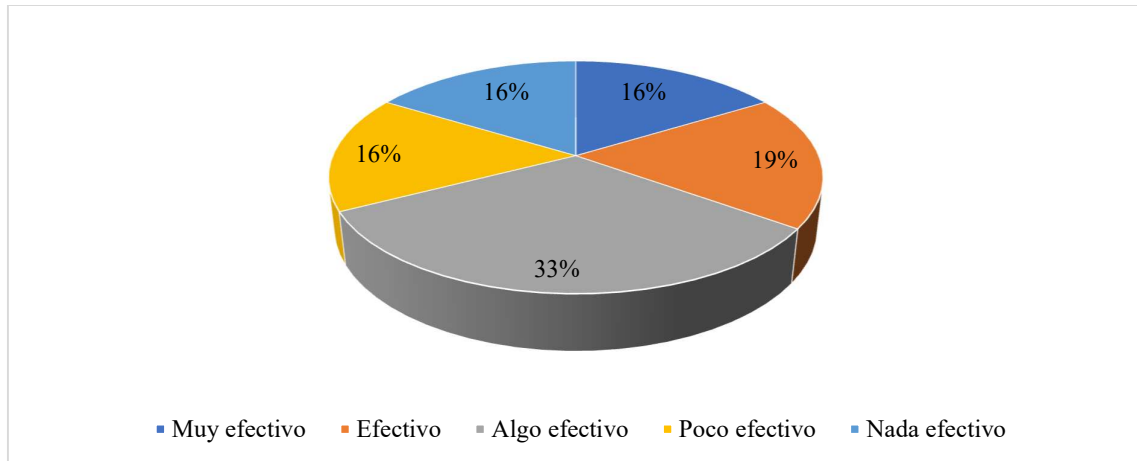


Tabla 3 Nivel de protección contra ciberataques en finanzas

Variables	Frecuencia	Porcentaje
Muy efectivo	7	16%
Efectivo	8	19%
Algo efectivo	14	33%
Poco efectivo	7	16%
Nada efectivo	7	16%
Total	43	100%

Análisis e interpretación: Los resultados indican que las percepciones sobre la efectividad del nivel de protección contra ciberataques en los sistemas de nómina y finanzas están divididas. Solo el 35% de los encuestados considera la protección "muy efectiva" (16%) o

"efectiva" (19%), mientras que el 33% opina que es "algo efectiva", lo que refleja dudas sobre su solidez. Además, un preocupante 32% percibe la protección como "poco efectiva" (16%) o "nada efectiva" (16%), destacando una percepción de vulnerabilidad significativa. Estos datos subrayan la necesidad de mejorar las medidas de ciberseguridad, ya que las respuestas reflejan una confianza limitada en la capacidad actual de los sistemas para prevenir ciberataques.

4. ¿Con qué frecuencia toma medidas para asegurar la confidencialidad de los datos de empleados y proveedores?

Gráfico 4 Medidas de confidencialidad en datos

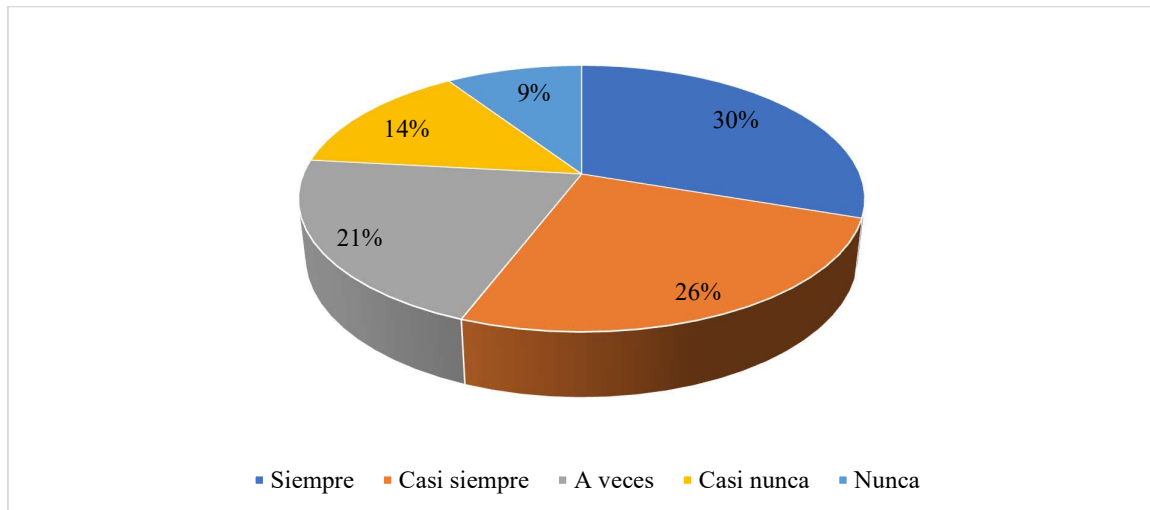


Tabla 4 Medidas de confidencialidad en datos

Variables	Frecuencia	Porcentaje
Siempre	13	30%
Casi siempre	11	26%
A veces	9	21%
Casi nunca	6	14%
Nunca	4	9%
Total	43	100%

Análisis e interpretación: Los hallazgos indican que la mayoría de los participantes en la encuesta adopta acciones con regularidad para garantizar la privacidad de la información de

empleados y proveedores, dado que el 30% indicó "siempre" y el 26% "casi siempre", lo que suma un 56% con medidas de protección habituales. No obstante, un 21% lo hace "ocasionalmente", mientras que un 23% reconoce que no toma estas acciones "casi nunca" (14%) o "nunca" (9%), lo que demuestra que casi un cuarto de los participantes no da prioridad a la seguridad de los datos de forma constante. Esto evidencia la importancia de fortalecer la concienciación y las normativas relativas a la confidencialidad para asegurar un mayor cumplimiento con las prácticas de protección.

5. ¿Cree que los sistemas de su organización permiten una detección oportuna de posibles violaciones de seguridad?

Gráfico 5 Sistema de organización para detectar violaciones de seguridad

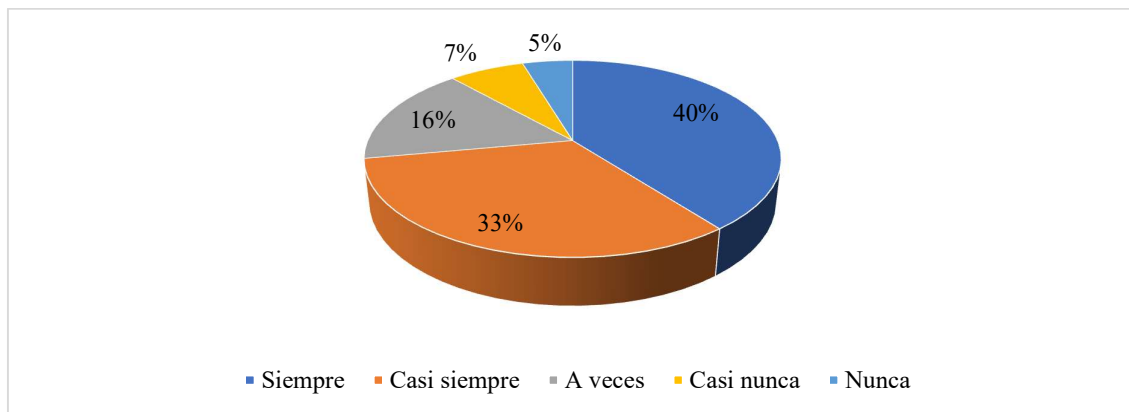


Tabla 5 Sistema de organización para detectar violaciones de seguridad

Variables	Frecuencia	Porcentaje
Siempre	17	40%
Casi siempre	14	33%
A veces	7	16%
Casi nunca	3	7%
Nunca	2	5%
Total	43	100%

Análisis e interpretación: Los hallazgos señalan que la mayoría de los participantes en la encuesta confían en que los sistemas de su entidad facilitan la identificación temprana de

posibles infracciones de seguridad, dado que el 40% contestó "siempre" y el 33% "casi siempre", lo que equivale a un 73% de respuestas favorables. No obstante, un 16% indicó que esto sucede "en ocasiones", mientras que un 12% expresó grados bajos de confianza al responder "casi nunca" (7%) o "nunca" (5%). Esta información resalta un escenario principalmente positivo, aunque todavía hay aspectos a mejorar para asegurar una identificación proactiva y fiable en todas las situaciones.

6. ¿Con qué frecuencia se revisan o actualizan las políticas de seguridad de datos en su área?

Gráfico 6 Actualización de políticas de seguridad

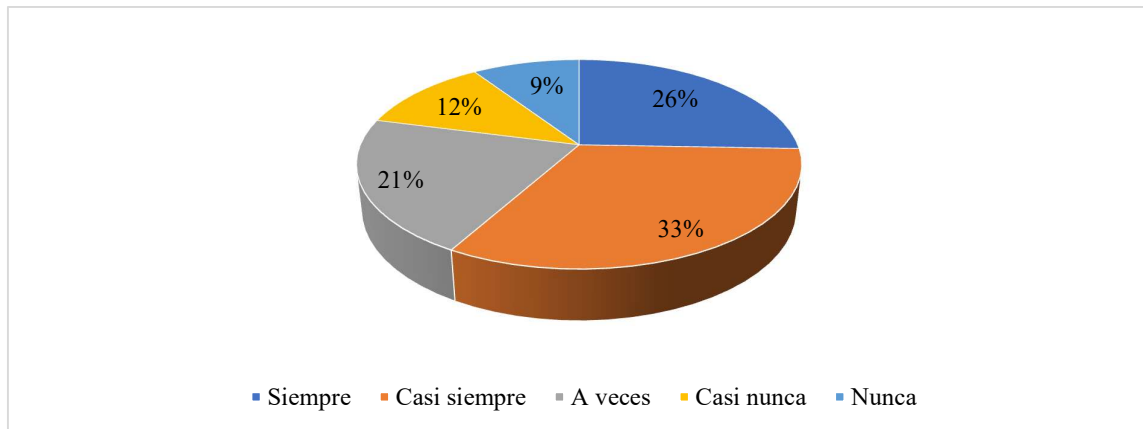


Tabla 6 Actualización de políticas de seguridad

Variables	Frecuencia	Porcentaje
Siempre	11	26%
Casi siempre	14	33%
A veces	9	21%
Casi nunca	5	12%
Nunca	4	9%
Total	43	100%

Análisis e interpretación: Los hallazgos indican que las políticas de protección de datos en el sector son revisadas o renovadas con cierta periodicidad, dado que un 26% de los participantes en la encuesta sostuvo que esto sucede "siempre" y un 33% "casi siempre", lo

que totaliza un 59% de respuestas favorables. No obstante, un 21% señaló que estas actualizaciones se producen "ocasionalmente", mientras que otro 21% expresó una frecuencia reducida al responder "casi nunca" (12%) o "nunca" (9%). Esto indica que, pese a un esfuerzo considerable por mantener las políticas al día, aún existe un porcentaje significativo de áreas donde este proceso podría robustecerse.

7. ¿Qué tan segura considera que es la gestión de contraseñas en el sistema utilizado para nómina y finanzas?

Gráfico 7 Gestión de contraseñas en el sistema de finanzas

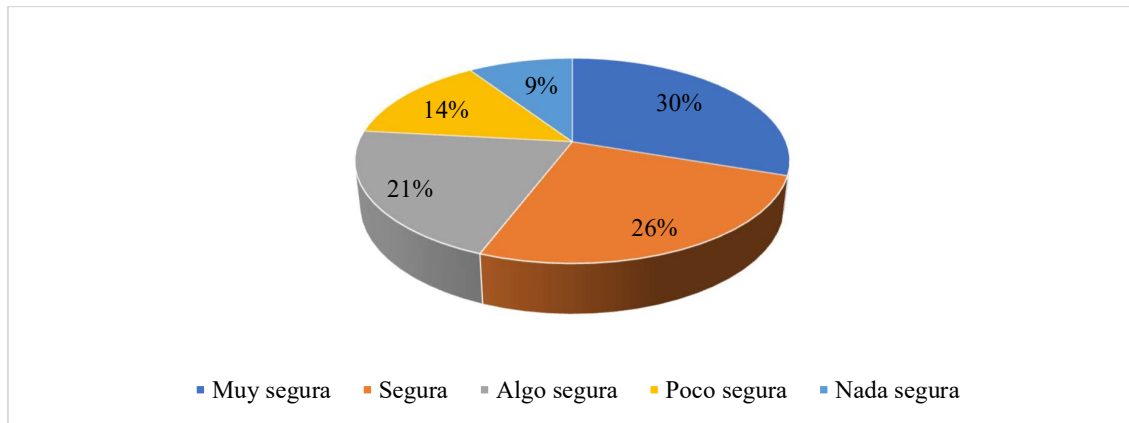


Tabla 7 Gestión de contraseñas en el sistema de finanzas

Variables	Frecuencia	Porcentaje
Muy segura	13	30%
Segura	11	26%
Algo segura	9	21%
Poco segura	6	14%
Nada segura	4	9%
Total	43	100%

Análisis e interpretación: Los hallazgos indican que la mayoría de los participantes en la encuesta ven la administración de contraseñas como apropiada, dado que el 30% la califica como "muy segura" y el 26% como "segura", lo que suma un 56% de puntos de vista favorables. Sin embargo, un 21% la catalogó como "algo segura", lo que señala cierta duda acerca de su efectividad. En cambio, un 14% la califica como "poco segura" y un 9% la

califica como "nada segura", lo que demuestra que hay una percepción de vulnerabilidad entre un grupo de usuarios que podría aprovechar mejoras en la administración de contraseñas.

8. ¿Con qué frecuencia se aplican medidas para prevenir el acceso no autorizado a datos confidenciales?

Gráfico 8 Medidas de prevención en acceso no autorizados

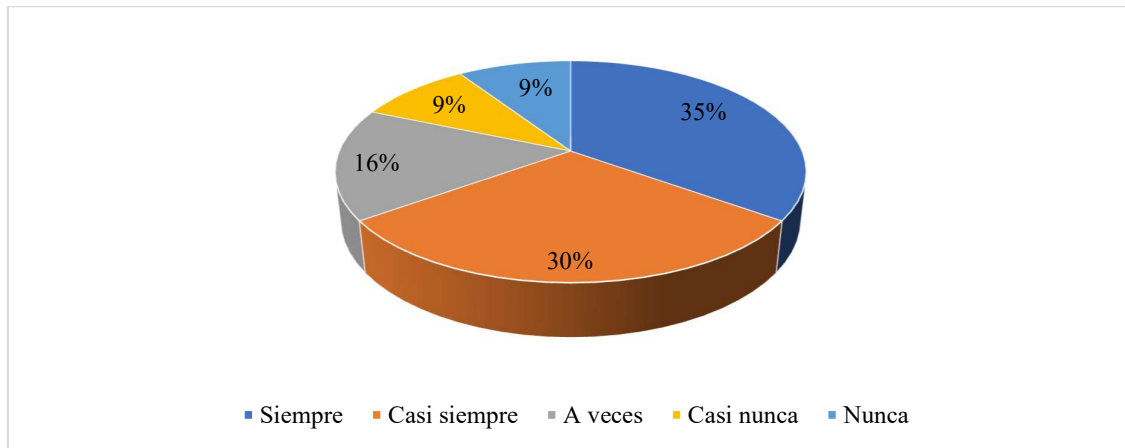


Tabla 8 Medidas de prevención en acceso no autorizados

Variables	Frecuencia	Porcentaje
Siempre	15	35%
Casi siempre	13	30%
A veces	7	16%
Casi nunca	4	9%
Nunca	4	9%
Total	43	100%

Análisis e interpretación: Los hallazgos señalan que, en la mayoría de las situaciones, se aplican medidas para evitar el acceso indebido a información confidencial. Esto se debe a que el 35% de los participantes en la encuesta indicaron que estas medidas se aplican "siempre", mientras que el 30% sostuvo que se aplican "casi siempre", lo que demuestra un compromiso considerable en esta área. No obstante, el 16% indicó que estas medidas se implementan "ocasionalmente", mientras que el 18% (sumando "casi nunca" y "nunca") considera que

estas acciones son insuficientes o poco habituales, subrayando la importancia de robustecer y asegurar la uniformidad en las prácticas de seguridad.

9. ¿Considera que la falta de recursos o personal especializado afecta la seguridad de datos en su área?

Gráfico 9 Falta de recursos y la seguridad de datos

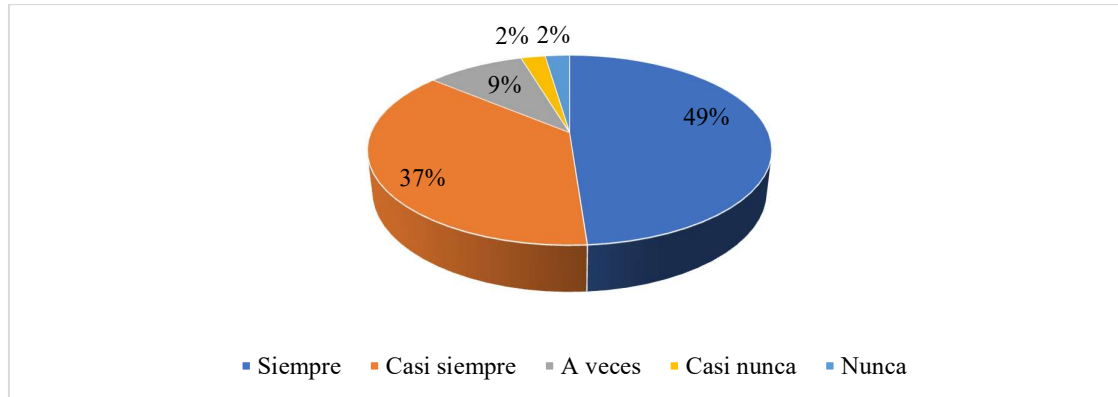


Tabla 9 Falta de recursos y la seguridad de datos

Variables	Frecuencia	Porcentaje
Siempre	21	49%
Casi siempre	16	37%
A veces	4	9%
Casi nunca	1	2%
Nunca	1	2%
Total	43	100%

Análisis e interpretación: Los hallazgos indican que la percepción de que la escasez de recursos o personal especializado impacta en la protección de datos es considerable, con un 49% de los participantes en la encuesta respondiendo "siempre" y un 37% indicando "casi siempre", lo que refleja una problemática constante en el sector analizado. Solo un 9% piensa que esta circunstancia sucede "ocasionalmente", mientras que un escaso 4% (sumando "casi nunca" y "nunca") considera que no constituye un asunto de importancia, destacando la importancia de destinar recursos y personal especializado para minimizar los riesgos de seguridad.

10. ¿Qué tan consciente se siente acerca de las políticas de manejo seguro de la información en su departamento?

Gráfico 10 Políticas de manejo en información en su departamento

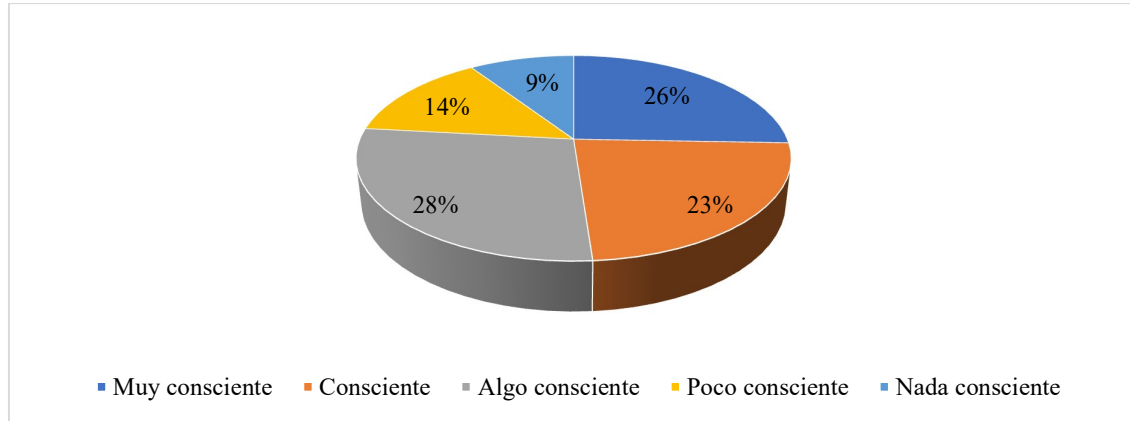


Tabla 10 Políticas de manejo en información en su departamento

Variables	Frecuencia	Porcentaje
Muy consciente	11	26%
Consciente	10	23%
Algo consciente	12	28%
Poco consciente	6	14%
Nada consciente	4	9%
Total	43	100%

Análisis e interpretación: Los hallazgos indican que la mayoría de los participantes en la encuesta tienen conciencia acerca de las políticas de gestión segura de la información, con un 26% que se percibe como "muy consciente" y un 23% que se percibe como "consciente". No obstante, un 28% se percibe como "algo consciente", lo que señala que existe un segmento considerable de la población con conocimientos restringidos en este asunto. En cambio, un 14% se percibe como "poco consciente" y un 9% como "nada consciente", lo que indica que hay una desigualdad en la educación y conciencia acerca de las políticas de seguridad de la información en el departamento. Esto subraya la importancia de fortalecer las campañas de concienciación y formación en protección de datos.

5. Consideraciones finales

Basado en los resultados que se han obtenido este tuyo se evidenciado que la seguridad de datos en la área de nómina y finanzas requiere una significativa mejora esencialmente, en cuanto a la capacitación y conciencia sobre la política de seguridad un modelo de seguridad de datos robusto debe ser aplicado de una forma estructurada empezando por una revisión de las políticas y procedimientos moderno la estrategia debe incluir un plan de capacitación para los empleados con el propósito de asegurar que estén bien informados sobre la relevancia de la protección de datos y de la manera de cómo hacerlo, además, se deben implementar sistemas integrados donde se aborda la gestión de contraseñas y accesibilidad al monitoreo continuo de los sistemas.

El modelo propuesto debe incorporarse de acuerdo con las medidas preventivas, detección de incidentes y respuestas efectivas, las medidas preventivas incluyen diferentes intersección de datos y sistema de autenticación multifactorial, así como las segmentación de redes para asegurar los datos confidenciales, la detención de incidente debe basarse en el método de monitoreo continuo que alertan sobre las conductas sospechosas y acceso no autorizado, en base a la respuestas efectivas la formación de los empleados en la forma de manejar los incidente de seguridad y creación de un plan de recuperación ante situaciones complejas son importantes, estas permitirán reducir los daños y restaurar la seguridad de la información de una forma más eficiente.

Las amenazas específicas que tiene una mayor afectación en la seguridad de estos en diferentes áreas de finanzas y no son los ataques cibernéticos, así como los ataques de negación del servicio los cuales pueden prometerse tanto los métodos de seguridad de datos de los empleados y de los proveedores, además se determinan los errores humanos como una vulnerabilidad común ya que esto puede ser aplicado sin ninguna intención y se divulgan datos importantes que no son autorizados la vulnerabilidad, además, se encuentra un déficit

de un control adecuado basado en accesibilidad de información lo que logra permitir que las personas no autorizadas tengan accesibilidad a datos confidenciales.

Para asegurar un enfoque de protección de datos importante tener diferentes prácticas y marcos normativos aplicables los cuales se encuentran establecidos como estándar para la protección de datos personales este tiene en principios claros sobre la recopilación y proceso de almacenamiento de datos importantes, las organizaciones deben asegurarse de cumplir con los requisitos de seguridad y privacidad teniendo en cuenta que las leyes nacionales de protección de datos son respetadas y se promueven de acuerdo a la cultura de seguridad favoreciendo así la integridad y la confidencialidad de la información adaptadas a la práctica particulares de diferentes áreas de finanzas o nóminas.

Referencias Bibliográficas

- Bayo, M., & Calderón, D. (2021). Blockchain y Propiedad Intelectual: Aplicando una tecnología innovadora en la gestión de Derechos Intangibles. *THEMIS Revista de Derecho*, 6(79), 345-357. <https://doi.org/10.18800/themis.202101.019>
- Bracho, M. S., Fernández, M., & Díaz, J. (2021). Técnicas e instrumentos de recolección de información: Análisis y procesamiento realizado por el investigador cualitativo. *Revista Científica UISRAEL*, 8(1), Article 1. <https://doi.org/10.35290/rcui.v8n1.2021.400>
- Campillo, S. (2021). Ciberseguridad y Blockchain. *Revista Blockchain e Inteligencia Artificial*, 1(3), 1-18. [https://doi.org/10.22529/rbia.2021\(3\)05](https://doi.org/10.22529/rbia.2021(3)05)
- Carrillo, X. (2021). Gestión financiera y administración de riesgos: Portafolios de inversión, financiamiento, riesgos financieros y riesgos operativos. *Estudios de la Gestión: Revista Internacional de Administración*, 9, Article 9. <https://revistas.uasb.edu.ec/index.php/eg/article/view/2577>
- Carvajal, A., & León, H. (2021). *Seguridad en bases de datos*. 5(1), 1-13. <https://www.redalyc.org/articulo.oa?id=378343671005>
- Carvajal, C. (2019). La encriptación de datos empresariales: Ventajas y desventajas | RECIMUNDO. *Recimundo*, 3(2), 980-997. <https://recimundo.com/index.php/es/article/view/487>
- Casas, J., Repullo, J., & Donado, J. (2023). La encuesta como técnica de investigación. Elaboración de cuestionarios y tratamiento estadístico de los datos (I). *Atención Primaria*, 31(8), 527-538. <http://www.elsevier.es/es-revista-atencion-primaria-27-articulo-la-encuesta-como-tecnica-investigacion-elaboracion-cuestionarios-13047738>

- Coronel, I., & Quirumbay, D. (2022). Vista de Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web. *Revista Científica y Tecnológica UPSE*, 9(2), 39-47.
<https://incyt.upse.edu.ec/ciencia/revistas/index.php/rctu/article/view/672/578>
- Corredor, J., & Díaz, D. (2019). Blockchain y mercados financieros: Aspectos generales del impacto regulatorio de la aplicación de la tecnología blockchain en los mercados de crédito de América Latina. *Derecho PUCP*, 5(81), 405-439.
<https://doi.org/10.18800/derechopucp.201802.013>
- Estupiñán, B., & Obando, C. (2019). La Criptografía como elemento de la seguridad informática. *Polo del Conocimiento*, 3(2), Article 2.
<https://doi.org/10.23857/pc.v3i2.456>
- García, A. (2020). Aplicación de técnicas de inteligencia de negocios y análisis de datos en el entorno empresarial cubano: Retos y perspectivas. *Revista Cubana de Ciencias Informáticas*, 14(4), 191-209.
http://scielo.sld.cu/scielo.php?script=sci_abstract&pid=S2227-18992020000400191&lng=es&nrm=iso&tlng=es
- García, G. (2019). *Fundamentos de la Ley Sarbanes-Oxley* (3.^a ed., Vol. 3). IMCP.
- García, J. A., Reding, A., & López, J. C. (2019). Cálculo del tamaño de la muestra en investigación en educación médica. *Investigación en Educación Médica*, 2(8), 217-224. [https://doi.org/10.1016/S2007-5057\(13\)72715-7](https://doi.org/10.1016/S2007-5057(13)72715-7)
- Lascano, W. (2023). Beneficios Económicos en la Prevención de Riesgos Laborales en la Empresa FAENZA IPC. Estudio de Caso. *Revista Científica Hallazgos*, 8(2), 166-176. <https://revistas.pucese.edu.ec/hallazgos21/article/view/629>
- Lecca, L. R., Paz, H. J., & Mendoza, A. C. (2023). Medidas de control interno para preservar la seguridad de los datos dentro de las empresas e-commerce: Una revisión

- sistemática. *Revista Ciencia, Tecnología e Innovación*, 21(27), 23-34.
<https://doi.org/10.56469/rcti.v21i27.881>
- Loaiza, A. (2022). Diseño de Controles Internos para el área de cuentas por pagar para la empresa PFI Group, Inc. *Finanzas y Negocios*, 2(3), Article 3.
<https://revistas.ulatina.edu.pa/index.php/Finanzasynegocios/article/view/265>
- Londoño, J. L., Dorado, D. R., & Giraldo, D. (2022). *Gerencia de la seguridad en la información de las organizaciones*. 4(1), 38-56.
<https://digitk.areandina.edu.co/handle/areandina/4535>
- Lucas, G. I. C., Tejena, L. E. D., Solorzano, B. R. P., & Merino, M. J. M. (2022). Riesgos de seguridad de los datos en la web. *Journal TechInnovation*, 1(2), Article 2.
<https://doi.org/10.47230/Journal.TechInnovation.v1.n2.2022.43-49>
- Márquez, L., Sánchez, L., Labarca, N., & Cartay, R. (2020). Análisis teórico desde un enfoque cuantitativo. *Revista de ciencias sociales*, 26(1), 233-253.
<https://dialnet.unirioja.es/servlet/articulo?codigo=7384417>
- Otzen, T., & Manterola, C. (2019). Técnicas de Muestreo sobre una Población a Estudio. *International Journal of Morphology*, 35(1), 227-232.
<https://doi.org/10.4067/S0717-95022017000100037>
- Pérez, J., Gil, T., & Universidad Autonoma de Barcelona. (2015). Security Strategies: Tools to fight for more Liberty and Security world. A view from Spain. *Revista de Derecho Uninorte*, 2(44), 333-360. <https://doi.org/10.14482/dere.44.7178>
- Ramos, C. A. (2021). Diseños de investigación experimental—Preexperimental. *CienciAmérica: Revista de divulgación científica de la Universidad Tecnológica Indoamérica*, 10(1), 1-7. <https://dialnet.unirioja.es/servlet/articulo?codigo=7890336>

- Rí-os, N., Morales, E., & Sandoya, S. (2019). Seguridad Informática, un mecanismo para salvaguardar la Información de las empresas. *Revista Publicando*, 4(10 (2)), Article 10 (2). <https://revistapublicando.org/revista/index.php/crv/article/view/367>
- Rodríguez, L. (2020). Investigación Básica. *Revista Eular*, 3(1), 1-27.
https://eulareview.ser.es/2019/files/pdf/7_post.pdf
- Rovira, Z., Robles, L., & Castillo, J. (2023). Protección de datos en el contexto de la promulgación de la Ley Orgánica de Protección de Datos Personales en Ecuador. *Dialnet*, 8(8), 1355-1373. <https://dialnet.unirioja.es/servlet/articulo?codigo=9152423>
- Saa, Y. (2023, mayo 15). Desarrollan nueva tecnología para proteger datos de los gobiernos y las empresas. *Revista Economía*. <https://www.revistaeconomia.com/desarrollan-nueva-tecnologia-para-proteger-datos-de-los-gobiernos-y-las-empresas/>
- Saltos, A. (2023, septiembre 1). *Apuesta Furukawa por la relevancia de la protección de datos—Revista Mas Seguridad*. <https://www.revistamasseguridad.com.mx/apuesta-furukawa-por-la-relevancia-de-la-proteccion-de-datos/>
- Tenelema, E., Méndez, P., & Villa, H. (2020). Modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube con base en las normas ISO 27017 y 27018. *Revista Espacios*, 41(17).
<https://www.revistaespacios.com/a20v41n17/20411720.html>
- Tugnarelli, M. (2019). Análisis de metodologías de recolección de datos digitales. *UNLP*, 3(1), 1-67. <https://sedici.unlp.edu.ar/handle/10915/62613>
- Villarreal, E., & Gorozabel, N. (2023). Aplicación del Sistema de Comando de Incidentes en mando y control de datos. *INNOVACIÓN & SABER*, 7(7), Article 7.
<https://innovacionsaber.isupol.edu.ec/index.php/innovacion/article/view/217>

Anexos

Encuesta dirigida al personal del área de soporte técnico

11. ¿Considera que el sistema actual protege adecuadamente los datos sensibles en el área de nómina y finanzas?

- Siempre
- Casi siempre
- A veces
- Casi nunca
- Nunca

12. ¿Con qué frecuencia recibe capacitación sobre políticas de seguridad de datos en su área de trabajo?

- Siempre
- Casi siempre
- A veces
- Casi nunca
- Nunca

13. ¿Qué tan efectivo considera el nivel de protección contra ciberataques en los sistemas de nómina y finanzas?

- Muy efectivo
- Efectivo
- Algo efectivo
- Poco efectivo
- Nada efectivo

14. ¿Con qué frecuencia toma medidas para asegurar la confidencialidad de los datos de empleados y proveedores?

- Siempre
- Casi siempre
- A veces

- Casi nunca
- Nunca

15. ¿Cree que los sistemas de su organización permiten una detección oportuna de posibles violaciones de seguridad?

- Siempre
- Casi siempre
- A veces
- Casi nunca
- Nunca

16. ¿Con qué frecuencia se revisan o actualizan las políticas de seguridad de datos en su área?

- Siempre
- Casi siempre
- A veces
- Casi nunca
- Nunca

17. ¿Qué tan segura considera que es la gestión de contraseñas en el sistema utilizado para nómina y finanzas?

- Muy segura
- Segura
- Algo segura
- Poca segura
- Nada segura

18. ¿Con qué frecuencia se aplican medidas para prevenir el acceso no autorizado a datos confidenciales?

- Siempre
- Casi siempre
- A veces
- Casi nunca

Nunca

19. ¿Considera que la falta de recursos o personal especializado afecta la seguridad de datos en su área?

- Siempre
- Casi siempre
- A veces
- Casi nunca
- Nunca

20. ¿Qué tan consciente se siente acerca de las políticas de manejo seguro de la información en su departamento?

- Muy consciente
- Consciente
- Algo consciente
- Poco consciente
- Nada consciente