FACULTAD DE CIENCIAS CONTABLES, ECONÓMICAS Y FINANCIERAS
ESCUELA PROFESIONAL DE CONTABILIDAD Y FINANZAS

LA AUDITORÍA INTERNA Y SU INCIDENCIA EN EL FRAUDE INFORMÁTICO EN LA BANCA DIGITAL EN LIMA METROPOLITANA EN EL AÑO 2022

PRESENTADO POR
HÉCTOR JESÚS ALEXANDER DEL CARPIO CASTRO
NICOLE PATRICIA VALENZUELA CHINCHAY

ASESOR
ARLENE PRADO AYALA

TESIS
PARA OPTAR EL TÍTULO PROFESIONAL DE CONTADOR PÚBLICO

LIMA – PERÚ
2024

USMP

UNIVERSIDAD DE
SAN MARTÍN DE PORRES

FACULTAD DE CIENCIAS CONTABLES ECONÓMICAS Y FINANCIERAS

ESCUELA PROFESIONAL DE CONTABILIDAD Y FINANZAS

LA AUDITORÍA INTERNA Y SU INCIDENCIA EN EL FRAUDE INFORMÁTICO EN LA BANCA DIGITAL EN LIMA METROPOLITANA EN EL AÑO 2022

PARA OPTAR EL TÍTULO PROFESIONAL DE CONTADOR PÚBLICO

PRESENTADO POR:

HÉCTOR JESÚS ALEXANDER DEL CARPIO CASTRO

NICOLE PATRICIA VALENZUELA CHINCHAY

ASESOR:

MTR. PRADO AYALA ARLENE

LIMA, PERÚ

2024

LA AUDITORÍA INTERNA Y SU INCIDENCIA EN EL FRAUDE INFORMÁTICO EN LA BANCA DIGITAL EN LIMA METROPOLITANA EN EL AÑO 2022

ASESORA Y MIEMBROS DEL JURADO

ASESORA:

MTR. ARLENE PRADO AYALA

MIEMBROS DEL JURADO:

PRESIDENTE:

Dr. SABINO TALLA RAMOS

SECRETARIO:

Dra. LUZ MARÍA GALINDO URIBE

MIEMBRO DE JURADO:

Dr. GIOVANNI TOMAS SEBASTIANI MIRANDA

DEDICATORIA

Esta tesis está dedicada a nuestras familias, por ser nuestra guía y principal motivación, de igual manera a nuestros asesores, por su constante apoyo, confianza y seguimiento durante el proceso de elaboración.

AGRADECIMIENTO

Agradecemos a nuestros padres, abuelos y familiares cercanos, por confiar siempre en nosotros y acompañarnos durante la elaboración de la tesis, asimismo queremos agradecer a nuestros asesores Arlene Prado y Miguel Cotrina por motivarnos a la culminación de la tesis.

TURNITIN

Similarity Report

PAPER NAME

Tesis Del Carpio Castro y Valenzuela Chinchay - Turnitin al 14.01.docx

AUTHOR

NICOLE PATRICIA VALENZUELA CHINCHAY

WORD COUNT

24699 Words

CHARACTER COUNT

135483 Characters

PAGE COUNT

153 Pages

FILE SIZE

2.3MB

SUBMISSION DATE

Jan 14, 2024 6:30 PM GMT-5

REPORT DATE

Jan 14, 2024 6:46 PM GMT-5

20% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

- 19% Internet database
- 3% Publications database
- Crossref database
- Crossref Posted Content database
- 10% Submitted Works database

Excluded from Similarity Report

- Bibliographic material
- Quoted material
- Cited material
- Small Matches (Less then 10 words)
- Manually excluded text blocks

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

En el presente trabajo de investigación, se narra el problema identificado en las empresas del sector banca digital, el cual consta de la poca revisión y constatación de efectividad en sus controles, esto debido a que diversas compañías no cuentan con un departamento de auditoría que sea capaz de determinar y procesar los puntos de control, es ahí donde algunas personas con malos hábitos que pueden ser externos o internos, aprovechan las estas falencias para ejecutar el fraude informático.

En este sentido, la presente tesis titulada “La auditoría interna y su incidencia en el fraude informático en la banca digital en Lima Metropolitana en el año 2022”, tiene como principal objetivo determinar si la auditoría interna incide en la detección del fraude informático, tomando en cuenta el aumento repentino de los ciberdelitos.

Esta investigación se ha ejecutado bajo un enfoque de tipo aplicada, con un nivel descriptivo, explicativo, correlacional y un diseño no experimental. Se han utilizado métodos de análisis estadísticos, deductivos e inductivos, en la cual se ha realizado una encuesta a una muestra de 69 profesionales especialistas en el área de Información de tecnología (TI), auditoría interna y revisión de controles internos, los cuales nos brindaron los datos necesarios para realizar por medio del sistema SPSS métodos estadísticos como el Alfa de Cronbach y prueba de Chi Cuadrado, los cuales nos han permitido determinar la confiabilidad de la técnica de investigación y la relación entre las variables, los indicadores e índices del presente estudio.

Logrando concluir en base a los datos de las encuestas, opinión de distintos autores e interpretación propia que la auditoría interna incide favorablemente en la detección del fraude informático en Lima Metropolitana en el año 2022.

ABSTRACT

In this research work, the problem identified in companies in the digital banking sector is narrated, which consists of the little review and verification of effectiveness in their controls, this is due to the fact that various companies do not have an audit department that is capable of determining and processing control points, this is where some people with bad habits that may be external or internal, take advantage of these flaws to carry out computer fraud.

In this sense, this thesis entitled "The internal audit and its impact on computer fraud in digital banking in Metropolitan Lima in 2022", has as its main objective to determine if the internal audit affects the detection of computer fraud, taking into account the sudden increase in cybercrimes.

This research has been carried out under an applied approach, with a descriptive, explanatory, correlational level and a non-experimental design. Statistical, deductive and inductive analysis methods have been used, in which a survey has been carried out on a sample of 69 professionals specializing in the area of Information Technology (IT), internal audit and review of internal controls, which provided us the data necessary to carry out statistical methods such as Cronbach's Alpha and Chi Square Test through the SPSS system, which have allowed us to determine the reliability of the research technique and the relationship between the variables, indicators and indices of the present study.

Managing to conclude based on the survey data, opinion of different authors and own interpretation that the internal audit has a favorable impact on the detection of computer fraud in Metropolitan Lima in the year 2022.

INTRODUCCIÓN

La presente tesis titulada **“LA AUDITORÍA INTERNA Y SU INCIDENCIA EN EL FRAUDE INFORMÁTICO EN LA BANCA DIGITAL EN LIMA METROPOLITANA EN EL AÑO 2022”,** tiene como finalidad promover la aplicación de auditorías internas en el sector banca digital, buscando de esta manera intentar disminuir el fraude informático.

Según la definición recogida por diversos autores, las auditorías internas han ido tomando cada vez un papel más importante en las empresas, esto se debe a la óptica que te da a la hora de identificar vulnerabilidades en la empresa, de igual forma nos brinda la oportunidad de detectar actividades anómalas y evalúa los controles internos.

Por consiguiente, la composición de esta tesis se constituye por seis capítulos: planteamiento del problema, marco teórico, hipótesis y variables, metodología, resultados y discusión. De igual forma, la tesis estará relacionada con tres anexos: matriz de consistencia, encuesta, tabla de Chi Cuadrado.

El capitulo uno resalta la realidad problemática, la cual dio inicio a esta tesis en donde se estableció el problema principal y los problemas secundarios, asimismo vinculados a los problemas previamente mencionados se determinó el objetivo principal y los objetivos secundarios, seguido de la justificación de la investigación, la importancia, limitaciones y, por último, la viabilidad de esta investigación.

El capítulo dos de esta tesis, se exploraron los antecedentes a nivel nacional e internacional, brindándonos una comprensión más profunda de la magnitud de la problemática abordada. Se indagó acerca del interés previo de otros autores en

nuestro tema de investigación. Además, se detallaron los fundamentos teóricos de las variables principales junto con sus índices e indicadores. Se examinaron los aspectos legales relacionados con las variables de estudio. Finalmente, en este mismo capítulo se esbozaron las definiciones de los términos técnicos relevantes para el tema de investigación.

El capítulo tres de la tesis, se formularon tanto la hipótesis principal como las secundarias del estudio, al mismo tiempo que se llevó a cabo la operacionalización de la variable independiente y dependiente.

El capítulo cuatro aborda la metodología, donde se definió la naturaleza y el alcance de la investigación, incluyendo el tipo, nivel, método y diseño de la misma. También se especificaron la población y la muestra involucradas en la investigación. En este capítulo, se detallaron las técnicas e instrumentos seleccionados para la recopilación de datos, junto con los procedimientos realizados para verificar la validez y confiabilidad de dichos instrumentos. Por último, se abordaron los aspectos éticos aplicados durante la ejecución de la investigación.

El capítulo cinco presenta los resultados derivados de la aplicación de las técnicas de recopilación de datos.

El capítulo seis, se procedió a analizar los hallazgos obtenidos, delineando tanto las conclusiones como las recomendaciones como elementos fundamentales del resultado del estudio de investigación.

Por último, se incluyeron las referencias bibliográficas y los apéndices como componentes integrantes de este trabajo de investigación.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

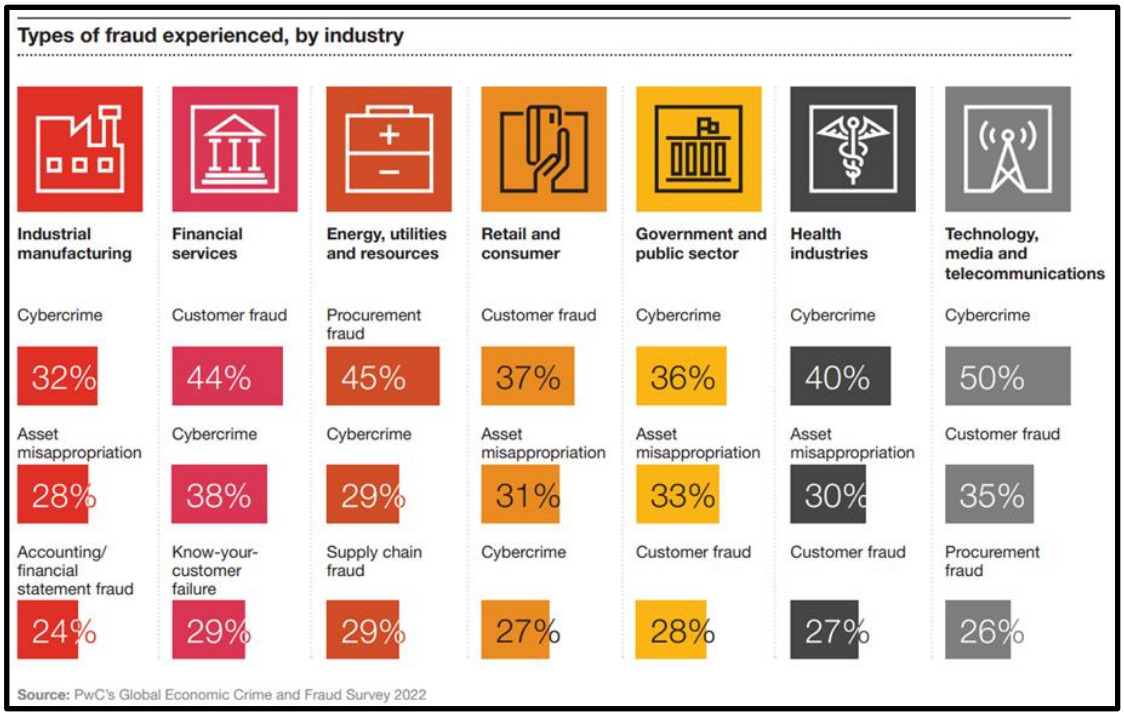
1.1. Descripción de la realidad problemática

Desde el inicio de la pandemia las organizaciones en todo el mundo han experimentado transformaciones significativas en el entorno empresarial y en el comportamiento de los consumidores. Estos cambios han impulsado una rápida adopción de la transformación digital y, al mismo tiempo, han aumentado drásticamente el nivel de riesgo en cuanto a la ciberseguridad.

Este cambio deja a relucir una clara problemática, el descubrimiento de fraude informático en la banca digital de una conocida empresa de servicios, en donde un hacker logró infiltrarse en el sistema digital de dicha empresa para realizar supuestos depósitos de dinero que nunca ingresaron en las cuentas de la organización y de esta forma obtener un beneficio personal a las deficiencias del sistema de seguridad.

Todo esto nos demuestra la poca infraestructura de seguridad informática que poseen la mayoría de empresas en el Perú, no tomando en consideración la importancia que conlleva tener un sistema apto para combatir con este tipo de programas malignos, los cuales pueden darle al defraudador el poder para sumergirse en los sistemas de la organización y así detectar las vulnerabilidades en los controles internos, áreas informáticas poco vigiladas o cualquier otra deficiencia proveniente por parte de la empresa.

Figura N°1: Types of fraud experienced, by industry (Traducción: Tipos de Fraude por industria (2022))



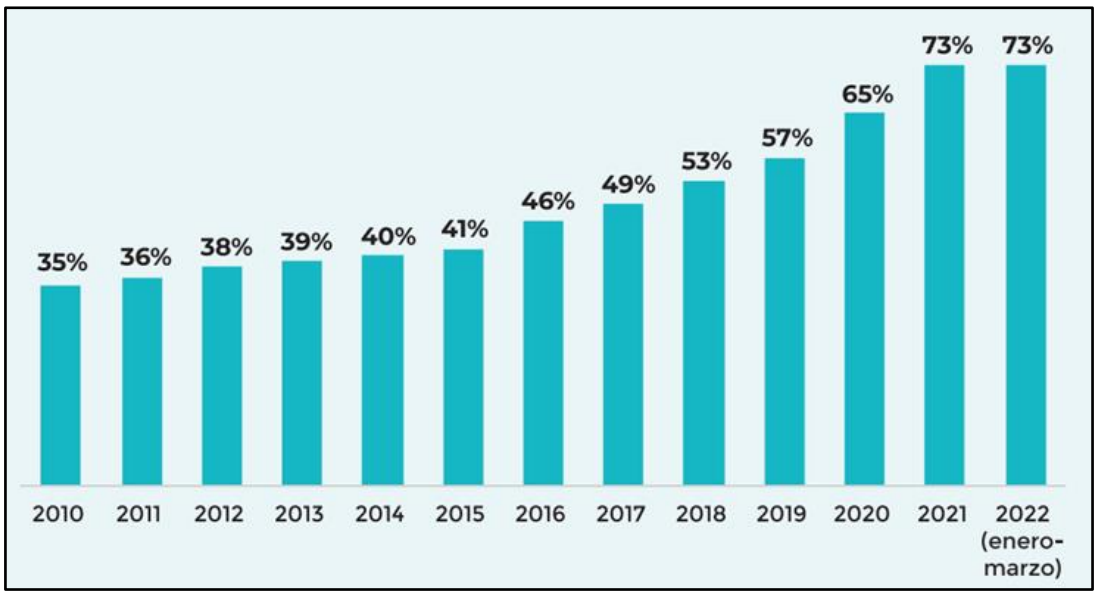
Fuente: PwC's Global economic crime and fraud survey 2022

Se observa en la figura n°1 un cuadro donde distribuyen los distintos tipos de empresas por industria y/o rubro de negocio junto con el porcentaje de la mayor cantidad de casos conocidos de fraude a nivel global, en primer lugar, se menciona a la industria de telefonía, media y comunicaciones con un 50% por

fraudes de delitos informáticos, al igual que el sector de salud (40%), sector público y gubernamental (36%) y la industria manufacturera (32%). Entre otros casos se tiene al sector minorista y consumidora y el sector financiero con la mayoría de casos de fraude al cliente (37%) y finalmente a la industria eléctrica y de energía con fraude por adquisición (45%).

Es de importancia enfatizar el número de cifras por casos de fraude informático, también conocido como delitos informáticos, vigentes al año 2022, el cual en una comparativa con los años anteriores se aprecia un incremento brutal dado por los avances tecnológicos que ocurren de forma veloz al igual que el ingenio de las personas con malicia quienes crean diferentes maneras de dañar el sistema que manejan las organizaciones.

Figura N°2: Población que accede a internet (Perú, 2010 - 2022)

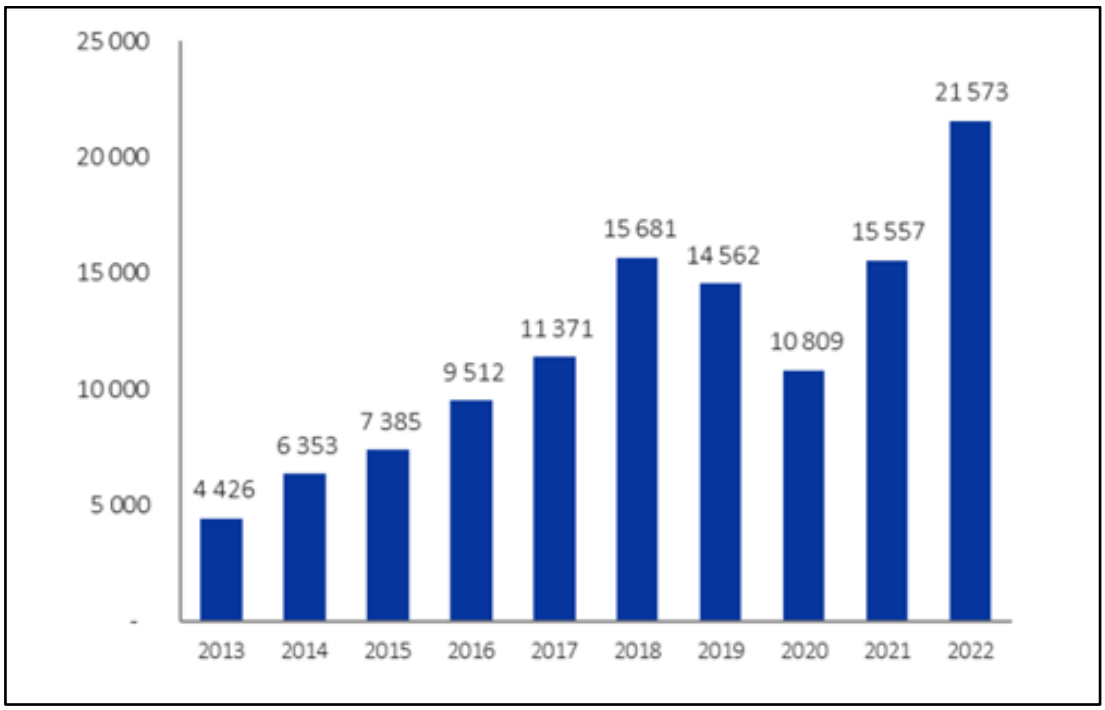


Fuente: INEI

Elaboración: Defensoría del Pueblo

Como se puede observar en el figura n°2 el porcentaje de población que posee internet se ha incrementado considerablemente en los últimos 10 años esto se debe a que el internet se ha ido transformando en una necesidad para todos, si bien es cierto el aumento porcentual de las personas que poseen conexión web trae más pros que contras, el mismo incremento llama la atención de defraudadores informáticos, los cuales buscan el mínimo error o descuido para poder sumergirse en las profundidades de los sistemas de las empresas y poder manipular sus datos, operaciones o cualquier artilugio para obtener un beneficio personal.

Figura N°3: Número de ROS (Reportes de operaciones sospechosas) recibidos anualmente (Perú, enero 2013 a diciembre 2022)



Fuente: SBS

En la figura n°3 se logra observar el enorme incremento que han tenido los reportes de operaciones sospechosas (ROS) en estos últimos años,

concretamente se puede notar que desde el año de pandemia en el 2020 existía un total de 10,809 reportes a nivel nacional, sin embargo a raíz que todo empezó a digitalizarse se observa un incremento que prácticamente duplica el número de reportes llegando a la suma de 21,573 casos de actividad sospechosa en el año 2022, tomando en consideración los números antes mencionados se puede llegar a la conclusión de que si bien es cierto la era de la digitalización trae muchos beneficios, también trae ciertos riesgos los cuales pueden ser disminuidos si se lleva de manera correcta los controles internos en las empresas.

Los grupos de crimen organizado reclutan nuevos miembros más fácilmente en tiempos de crisis económica cuando incrementa el desempleo. Por lo tanto, es fundamental aumentar la vigilancia de los riesgos de fraude durante una recesión, prestando especial atención a amenazas que puedan surgir inesperadamente.

El aumento constante de incidentes de violación de datos en los últimos años está generando un desafío cada vez mayor para las empresas en cuanto a la salvaguarda de la información confidencial y la identificación personal de sus clientes. Estas brechas de seguridad están sometiendo a prueba las estrategias de autenticación basadas en el conocimiento que las organizaciones han adoptado para defenderse contra posibles fraudes.

Esto implica documentar lo ocurrido, determinación de los puntos débiles y ajustar los controles necesarios para prevenir que tales situaciones se repitan en el futuro. En resumen, es importante aprender de las experiencias pasadas y mejorar los mecanismos de control y supervisión.

Los trabajadores en las empresas tiene que estar debidamente capacitados para realizar sus actividades de forma correcta y segura, sin embargo en ocasiones algunos colaboradores se desvían de esa misión evadiendo los controles internos de la empresa los cuales nos ayudan a organizar de forma adecuada las actividades, los protocolos y los procesos por los cuales circula el dinero producto de la utilidad del negocio, es en este punto donde se puede ejecutar una malversación de fondos la cual mayormente tiene lugar en los puestos gerenciales, esto pasa debido a que tienen un mayor índice de determinación en relación al flujo económico en dichas organizaciones.

Muchas de las empresas al año 2022 en Lima Metropolitana no cuentan aún con un suficiente control que verifique el cumplimiento de las normas de auditoría (NIAS), esto genera un desproporcionado incremento en el nivel de fraude lo cual da puertas abiertas a que cualquier ciberdelincuente pueda invadir el sistema de la empresa trayendo así grandes daños económicos o reputacionales.

Un punto muy importante a la hora de realizar la auditoría interna en las empresas de Lima Metropolitana es tener la contabilidad al día y segura, lamentablemente esto no es el caso de algunas empresas las cuales sufren de ciertos retrasos en su cierre contable.

1.2 Formulación del problema

1.2.1 Problema General

- ¿De qué manera la auditoría interna incide en la detección del fraude informático en la banca digital en Lima Metropolitana, año 2022?

1.2.2 Problemas Específicos

a. ¿De qué manera el control interno incide en la disminución de la malversación de fondos en la banca digital?
b. ¿En qué medida la exigencia del Cumplimiento de las normas de auditoría y de información financiera (NIAS) incide en la gestión de riesgo de fraude en la banca digital?
c. ¿De qué manera la vulneración de controles por parte de la gerencia incide en la aplicación de la ciberseguridad en la banca digital?

1.3 Objetivos de la Investigación

1.3.1 Objetivo General

- Determinar si la auditoría interna incide en la detección del fraude informático financiero en la banca digital en Lima Metropolitana, año 2022.

1.3.2 Objetivos Específicos

a. Determinar si el control interno incide en la disminución de la malversación de fondos en la banca digital.
b. Analizar si el cumplimiento de las normas de auditoría y de información financiera (NIAS) incide en la gestión de riesgo de fraude en la banca digital.
c. Definir si la vulneración de controles por parte de la gerencia incide en la aplicación de la ciberseguridad en la banca digital.

1.4. Justificación de la investigación

1.4.1 Justificación

La presente investigación se llevó a cabo debido al creciente índice de fraude informático, el cual genera perjuicios económicos y reputaciones a las empresas afectadas, en este caso buscamos ayudar a detectar el fraude informático en empresas del sector banca digital, donde se han identificado un mayor daño en relación a sus sistemas digitales.

1.4.2 Importancia

La presente investigación aporta información a los lectores interesados en la seguridad informática y a las empresas que poseen bancas digitales a llevar auditorías de manera constante para de esta forma disminuir el nivel de riesgo de fraude informático, de igual forma esto nos ayuda a mantener un adecuado control interno referente a los procesos ejecutados por parte de las empresas del sector en cuestión.

1.5 Limitaciones de la investigación

En la presente investigación se presentaron algunas limitaciones tales como la obtención de referencias de autores, ya que, al ser un tema novedoso en el Perú, no existen muchas bases teóricas en donde apoyarnos. Se hizo la búsqueda de información en Fuentes como libros, tesis de grados superiores, revistas académicas y otras Fuentes de información necesarias para avalar el entendimiento de la problemática.

1.6 Viabilidad de la investigación

La recopilación de la información requerida se realizó mediante una búsqueda de información proporcionada por autores de libros, revistas, artículos y tesis digitales de valor académico las cuales nos sirvieron como Fuentes confiables para respaldar la veracidad y credibilidad de la información utilizada.

CAPÍTULO II: MARCO TEÓRICO

2.1 Antecedentes de la Investigación

2.1.1 Antecedentes Nacionales

Mengoa, V. (2021), en su tesis para grado de maestría de derecho en la Universidad César Vallejo-Perú, “Punibilidad del comportamiento del phisher-mule en el delito de fraude informático en el Perú”, señala lo siguiente acerca del fraude informático:

> La investigación aborda la problemática del delito de fraude informático en el Perú, el cual ha evidenciado un aumento significativo en la frecuencia de ciberdelitos a nivel nacional en comparación con años anteriores. Este incremento se atribuye, en parte, al entorno actual de globalización, donde las personas comparten sus datos personales y

confidenciales en internet, lo que brinda una mayor facilidad para la comisión de delitos informáticos. La creciente interconexión digital y la dependencia de la tecnología han ampliado las oportunidades para los perpetradores de fraude informático, subrayando la necesidad de medidas más sólidas en términos de seguridad cibernética y concienciación sobre las amenazas en línea.

Esta investigación resulta muy importante en relación a nuestro estudio debido a que hace mención al incremento de la globalización también aumenta el nivel de riesgo de fraude informático, esto se debe al verse expuestos los datos personales, información y hasta la ubicación actual en algunos casos, los cuales brindan facilidades a aquellos inescrupulosos piratas informáticos a perpetrar documentación valiosa para la empresa, de igual manera sabemos que en la actualidad muchas empresas utilizan el teletrabajo, por lo que es necesario que gran parte de la información se encuentre colgada en la red dándole un grado más de vulnerabilidad a la empresa si es que esta no lleva de manera adecuada los controles internos necesarios para impermeabilizar dicha información.

De la Torre, M. (2018), en su artículo “Gestión del riesgo organizacional de fraude y el rol de auditoría interna” de la Universidad Pontificia Católica del Perú-Perú, revista Contabilidad y negocios, volumen 13, número 5.

El presente artículo realizado por De la Torre nos menciona la temática del nivel de fraude y el papel que cumple la auditoría, el cual ha abarcado en gran parte al sector banca digital debido a fallos en sus controles internos los cuales ha involucrado a las empresas en grandes pérdidas

económicas y también reputacionales, es por ello que las empresas afectadas han creado controles propicios para que la ciberdelincuencia criminal organizada no realice más prácticas corruptas. Entre algunos tipos de fraude destaca el fraude corporativo, con menciones particulares a los escándalos a nivel mundial protagonizados por multinacionales como Odebrecht, WorldCom, Enron, Parmalat o Volkswagen. Estos casos subrayan la necesidad urgente de fortalecer los mecanismos de control y la ética empresarial para prevenir y combatir prácticas fraudulentas y corruptas en el ámbito corporativo.

Este antecedente es tomado de un artículo de investigación ya que el tema de ciberseguridad es novedoso a nivel nacional y no existe la información necesaria en tesis de maestrías o grados superiores, no obstante es importante como antecedente ya que el autor menciona que muchas empresas no han logrado establecer los controles debidos ya sea porque el diseño del control no logra cubrir el riesgo, o su implementación no es la debida para el tipo de riesgo que trata de mitigar la organización, este tipo de situaciones solo deja en una evidente vulnerabilidad en los procesos de la empresa y es ahí donde algunos colaboradores corruptos aprovechan estas intenciones para obtener beneficios propios.

Como resultado de los antecedentes nacionales descritos en la parte superior se puede detectar que en el Perú aún existen deficiencias en cuanto a los controles manejados por las empresas y más aún cuando se enfocan en el rubro informático, esto se debe a que la tecnología ha tomado un nivel de importancia a un ritmo apresurado dejando en evidencia las carencias de seguridad frente a los riesgos de fraude informático, generando de esta forma

ventanas de inseguridad en los sistemas de data con los que cuenta la empresa y usuarios poniendo en riesgo su integridad y estabilidad.

2.1.2 Antecedentes Internacionales

Gumucio, J. (2021) para la tesis para optar al grado de Magíster en Gestión y dirección de empresas de la Universidad de Chile-Chile, resalta lo siguiente:

> La tesis en cuestión creada por Gumucio enfatiza su información y aborda el tema del fraude cibernético en las entidades financieras las cuales deben utilizar de manera segura, transparente y responsable sus herramientas y canales digitales para proteger la información y datos de sus clientes. Una gestión deficiente de la seguridad de la información puede resultar en pérdidas económicas debido a la ciberdelincuencia. Además, la entidad podría enfrentar responsabilidad civil y penal, procesos judiciales por parte de clientes afectados o el estado, multas y sanciones de reguladores, y la pérdida de reputación, lo que afectaría su negocio. Para los clientes, la pérdida de datos personales podría llevar a la pérdida de dinero, fraude, suplantación de identidad y extorsión.

En referencia a lo descrito por parte del autor se puede evidenciar su preocupación acerca de una vertiente en crecimiento la cual trata acerca del fraude cibernético. El creador de esta tesis nos hace referencia a los riesgos presentes a la hora de realizar alguna acción de manera digital si su banco o aplicativo no cuenta con un adecuado sistema de seguridad informática podría presentar algunos prejuicios como por ejemplo la pérdida económica, reputacional o en algunos casos hasta la suplantación de identidad.

Carbajal, A. (2017) para la tesis para optar al grado de Maestra en Auditoría de la Universidad Nacional Autónoma de México-México, manifiesta que:

> La presente investigación para el grado de maestría realizada por Carbajal aborda el tema de los fraudes cibernéticos en México y señala que, entre algunos tipos de fraudes, los más comunes en las empresas mexicanas abarcan robos de activos físicos o inventarios (30%), corrupción y sobornos (25%), fraudes financieros cibernéticos (25%), y fraudes relacionados con vendedores, proveedores y adquisiciones (23%). Según una encuesta, el 72% de los fraudes involucraron a al menos una persona que trabajaba dentro de la empresa, y el 32% fue detectado a través de denuncias internas. La gerencia descubrió el 52% de los fraudes, mientras que el 51% se detectó mediante auditorías internas y solo el 10% a través de auditorías externas.

Como se puede analizar el problema del fraude cibernético ataca a todos los países del mundo, esto se debe a que muchas organizaciones tuvieron que implementar la digitalización de forma repentina, y en su mayoría no se encontraban preparadas para afrontar un peligro cibernético de complejidad superior, de igual forma podemos connotar que la mayoría de fraudes se dieron a cabo gracias a la presencia de uno o más trabajadores sin ética profesional los cuales perjudicaron a la empresa donde laboraban.

Paiva, R. (2021) para la tesis para optar al grado de Magíster en Derecho de la Universidad Nacional de Colombia-Colombia, menciona lo siguiente:

> La presente investigación para tesis de maestría realizada por parte de Paiva aborda el tema de fraude electrónico, el cual nos menciona que, en el año 2021, la interpretación de la Corte Suprema de Justicia (CSJ) respecto a la responsabilidad civil de las entidades bancarias en casos de fraude electrónico, donde terceros no autorizados sustraen dinero de cuentas corrientes y de ahorro, se basa en una imputación de responsabilidad objetiva por riesgo creado o riesgo social. Esta interpretación se fundamenta en la aplicación analógica del pago de cheques falsos y el artículo 2356 del Código Civil. Sin embargo, esta perspectiva no considera que, en casos de fraude electrónico, en los contratos de cuenta corriente y ahorro, debería existir previamente una relación contractual de depósito irregular. Por lo tanto, es necesario examinar la responsabilidad del banco en eventos de fraude electrónico bajo los parámetros del régimen general de las obligaciones, especialmente las obligaciones de resultado.

Tal como nos resalta Paiva R. conocer los riesgos de la digitalización en la banca es fundamental para tomar conciencia y prevenir algunas acciones que puedan dejarnos al descubierto en frente del peligroso y creciente fraude cibernético, el cual ha presentado gran controversia debido a que muchas organizaciones de bancas digitales no cuentan con un adecuado sistema de protección de datos e información, por lo cual muchos usuarios se vieron afectados económicamente, de igual forma el autor centra la atención en mencionar las políticas de ciberseguridad las cuales son importantes para el adecuado funcionamiento de los sistema de seguridad implementados por las entidades pertinentes.

Tomando en consideración todos los antecedentes internacionales se llega a la conclusión que la seguridad informática ha ido tomando mayor relevancia a nivel mundial, esto se puede evidenciar con la creación de departamentos de ciberseguridad, auditorías para la revisión de los controles que posee la empresa, las cuales no solo se encargan de revisar los estados financieros, sino también contratar expertos en seguridad digital para establecer que tan confiable son los sistemas utilizados para guardar data, realizar transacciones virtuales y certificar los procedimientos por donde pasa el flujo de efectivo de la organización.

2.2 Bases Teóricas

Variable Independiente: Auditoría Interna

2.2.1 Marco Legal

Según la **Contraloría General del Perú en la Ley N° 27785 "Ley orgánica del sistema nacional de control y de la contraloría general de la república"**, publicada el 23 de julio del 2002; en el artículo 7 indica lo siguiente:

> El control interno abarca las medidas de precaución anticipada, simultánea y de revisión posterior, llevadas a cabo por la entidad sujeta a control, con el objetivo de garantizar que la administración de sus recursos, activos y operaciones se lleve a cabo de manera precisa y eficiente. El ejercicio del control interno se realiza de manera anticipada, simultánea y posterior. (s.p.)

Teniendo en cuenta lo dicho en la Ley N°27785 podemos resaltar la importancia de llevar idóneamente los controles internos en una empresa, esto se debe a

que dicho control revisa el paso a paso de los procesos realizados por parte de la entidad, esto es beneficioso para la empresa porque no solo regula la seguridad informática, sino también ayuda a la organización a administrar sus recursos lo más productivo posible.

2.2.2 Marco Conceptual

Auditoría Interna

De acuerdo con el Instituto Mexicano de Auditores Internos A.C. (IMAI) (2018) menciona que:

> La auditoría interna se caracteriza como una función independiente y objetiva cuyo propósito principal es fortalecer el control interno en los procedimientos de las empresas. Su misión se centra en añadir valor y perfeccionar las operaciones de la organización. El objetivo fundamental de la auditoría interna es contribuir al cumplimiento de los objetivos de la entidad mediante la aplicación de un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno. (s.p.)

Apoyando la interpretación brindada por los autores del Instituto Mexicano de Auditores Internos, la auditoría interna consiste en una actividad llevada a cabo por contadores especializados, con el fin de valorar y perfeccionar la eficacia de los procedimientos relacionados con la gestión de riesgos, control y gobierno dentro de dicha entidad. Esta función busca proporcionar garantía y asesoramiento, con el propósito de añadir valor y cooperar con el cumplimiento de las metas de la organización.

Rizo, P. (2019) manifiesta que:

> A lo largo de los años, la función de la auditoría interna ha experimentado cambios significativos. Inicialmente, se centraba en una labor "detectivesca" destinada a descubrir posibles fraudes o errores en los registros contables. Sin embargo, en la actualidad, sus objetivos han evolucionado considerablemente, abarcando la mejora de las operaciones en la entidad y la adición de valor. Diversos factores influyen en los propósitos de la auditoría interna, incluyendo el entorno normativo, social y político del país donde opera la entidad, la perspectiva del auditor a cargo, la naturaleza del negocio, su tamaño (micro, pequeño, mediano o grande), la complejidad de las operaciones y elementos externos que podrían impactar la empresa, como la inflación, cambios en las tecnologías de la información (TI), modificaciones en las normas contables y regulaciones relevantes para la empresa.(p. 30)

De la mano de lo mencionado por el autor, se puede rescatar que la auditoría interna en empresas, independientemente de su tamaño, consiste en la revisión de controles dentro de la organización, esto con la finalidad de examinar y perfeccionar la eficacia de los procesos relacionados al rubro de la compañía. En el caso de empresas más pequeñas, la auditoría interna tiende a concentrarse en la evaluación y mejora de procesos específicos, ya que estas organizaciones suelen tener una estructura más simple y menos compleja. En contraste, en empresas de mayor tamaño, la auditoría interna aborda una variedad más extensa de procesos y operaciones, dada la mayor complejidad y diversidad de funciones presentes en la empresa.

Rodríguez, E. (2014) menciona que:

> Frente a los desafíos intrínsecos en la definición de la función de auditoría interna, tal como establece el Instituto de Auditores Internos, se hace necesario intensificar la investigación con el objetivo de descubrir nuevas metodologías que optimicen el proceso de aseguramiento. Este proceso está condicionado por diversos factores, siendo la destreza, formación y experiencia del equipo humano el más destacado. No obstante, este aspecto experimenta cambios tanto cualitativos como cuantitativos de manera continua. Cualitativamente, se observa una evolución a medida que los miembros maduran o se incorporan individuos con nuevas perspectivas. Cuantitativamente, el equipo puede cambiar debido a la entrada o salida de miembros, ya sea por retiro de la empresa o asunción de otras responsabilidades, generando preocupación respecto a la posible pérdida de conocimiento acumulado. (p. 4)

Tomando en consideración lo mencionado por el autor se puede concretar que es fundamental para el funcionamiento eficaz de una auditoría interna contar con el personal adecuado y gestionarlo de manera efectiva. La retención y atracción de talento competente son aspectos cruciales para garantizar que el departamento cuente con las habilidades y conocimientos necesarios para cumplir con sus responsabilidades de manera eficiente y efectiva. La gestión adecuada de este personal implica no solo reclutar y mantener a profesionales calificados, sino también proporcionar un entorno de trabajo que fomente el desarrollo continuo y la colaboración efectiva en el equipo. La combinación de educación, formación, experiencia y cualificación profesional contribuye directamente al éxito y la calidad de las auditorías internas realizadas.

Control Interno

Al explorar una materia tan significativa como el que aborda este trabajo de investigación, nos hemos encontrado con diversos autores que conceptualizan las variables desde perspectivas y enfoques distintos, evidenciando así la diversidad de opiniones, tales como:

Urdanegui, R. (2019) indica lo siguiente:

> El control interno se refiere al conjunto de procedimientos esenciales que una compañía debe llevar a cabo para reducir los riesgos a niveles aceptables. Este mecanismo tiene como objetivo prevenir situaciones como la malversación de fondos, la pérdida de activos, el incumplimiento de normativas legales, fraudes, entre otros. A través del sistema de control interno, se busca anticipar los riesgos identificando, evaluando e implementando controles para mitigarlos. Esto no solo genera confianza, sino que también protege el valor de la empresa y permite focalizar los esfuerzos. Aunque el compromiso con el cumplimiento de los objetivos de control es responsabilidad de todos los miembros de la empresa, la implementación efectiva recae principalmente en la gerencia. (p. 13)

Los controles de la empresa son una parte crucial para poder mantener lo más bajo posible el nivel de riesgo de fraude informático, con lo cual nos brindará una mayor confiabilidad de los procesos en las empresas que poseen la banca digital, con esto poder lograr el cumplimiento de los objetivos planteados, este tipo de controles normalmente son implantados por la gerencia, para así obtener una vigilancia constante de que las actividades sean realizadas correctamente y de la manera más segura posible.

Pereira, C. (2019) define que:

> El diseño e implementación del control interno deben orientarse a reducir al mínimo el impacto de los diversos tipos de riesgos que podrían afectar de manera negativa los resultados esperados de la compañía. Para lograr esto, es necesario establecer controles específicos que ayuden a mitigar los riesgos identificados. (p. 10)

Como se sabe toda actividad monetaria posee un nivel de riesgo alto, el cual puede complicar la situación económica, integral y reputacional de una empresa, este tipo de riesgo de fraude informático se pueden aminorar implantando controles adecuados tanto en el diseño como también en la forma en que se verá implementado el control, estas dos características son claves para determinar la eficacia operativa del mismo, en donde se examinará el nivel de riesgo y la frecuencia del control.

Pereira, C. (2019) asegura que:

> En un estudio científico llevado a cabo en Indonesia, el objetivo principal fue investigar cómo el control interno impacta en el liderazgo, estilo de liderazgo y el trabajo en equipo. Este estudio adoptó un enfoque cuantitativo, encuestando a un mínimo de 110 empleados a través de cuestionarios como instrumento de investigación, y los datos fueron analizados utilizando el software estadístico SPSS. Los resultados revelaron que tanto el control interno como el trabajo en equipo tienen una influencia positiva en el éxito de los proyectos. (p. 30)

Concordando con la información brindada observamos la clara importancia de los controles internos en las empresas de servicios, detallando la influencia indudable en los éxitos conllevados por una eficiente cadena de controles

dando así un índice superior en referencia a la veracidad del cumplimiento adecuado de los procesos, los cuales ayudarán a lograr las metas de la empresa, de igual forma estos controles nos proporcionan disminuir el nivel de riesgo de fraude informático.

Cumplimiento de normas de auditoría

Reátegui, R. (2016) indica que:

> Las normas internacionales de auditoría (NIA) representan un conjunto integral de directrices, políticas y procedimientos que garantizan la consistencia y calidad de la auditoría independiente realizada por contadores públicos en todos los países que forman parte de la Federación Internacional de Contabilidad (IFAC) (p. 5)

Las NIAS son las normas de auditoría las cuales fueron estandarizadas de modo que se pueda usar metodológicamente de forma internacional, de esta manera establecer un alto índice de calidad y paridad en las auditorías realizadas en cual sea el país siempre y cuando este pertenezca a la Federación Internacional de Contabilidad o conocida por sus siglas IFAC, esta normativa es beneficiosa ya que brinda una mayor fiabilidad de la información financiera.

Alberca, E. (2017) manifiesta que:

> De acuerdo con las normas generalmente aceptadas de auditoría, las normas internacionales de auditoría y los estándares generales de control gubernamental, el auditor asume la responsabilidad de planificar y llevar a cabo la auditoría utilizando su juicio profesional. El objetivo es obtener evidencia suficiente y pertinente para mitigar los riesgos de

> auditoría a un nivel adecuado. Esto le permite al auditor emitir una opinión objetiva e imparcial sobre los estados financieros, así como sobre los procedimientos administrativos y operativos. (p. 11)

Las NIAS permiten al auditor poder esclarecer su dictamen en referencia a la fiabilidad de los informes financieros esto se debe ya que dichas normas tienen como objetivo proporcionar evidencia de auditoría suficiente y apropiada, esta normativa deberá ser interpretada por parte del auditor según sea la circunstancia a la hora de realizar la auditoría.

Chambi, E. (2022) indique que:

> Después del código de ética profesional, se encuentran las normas de control de calidad que se aplican a las firmas de contadores públicos encargadas de llevar a cabo auditorías y revisiones de información financiera. Estas normas tienen como objetivo garantizar la entrega de servicios de alta calidad en el ámbito empresarial. Las normas internacionales de auditoría y control de calidad (NICC) son medidas establecidas por la profesión y que, según la ley, deben ser cumplidas para asegurar que la prestación del servicio sea de calidad y que los procedimientos y objetivos de la auditoría sean los apropiados. (p. 20)

Tal como nos menciona Chambi el cumplimiento de las normas de auditoría es fundamental para poder ejercer un mayor control en referencia al fraude, en especial a la modalidad de fraude cibernético, ya que al ser un tipo de fraude relativamente nuevo se tiene que poner énfasis en sus controles de modo que se logre mitigar los riesgos que conlleva las nuevas tecnologías, de igual forma el autor hace mención a los estándares internaciones de auditoría y calidad, las

cuales sirven como un medidor para establecer qué clase de auditoría se realizó.

Vulneración de controles por parte de la gerencia

De La Torre, M. (2018) menciona que:

> Los riesgos de fraude y la capacidad de la administración para eludir el control interno están presentes en todas las organizaciones. El principal responsable del diseño, implementación y mantenimiento del control interno es el consejo de administración (directorio), seguido de la gerencia, lo que expone a la entidad al riesgo de que la administración pueda anular los controles, ya sea en una entidad pública, privada, sin fines de lucro o gubernamental. Cuando la oportunidad de eludir el control interno se combina con fuertes incentivos para alcanzar los objetivos contables, la alta dirección puede estar involucrada en la presentación de informes financieros fraudulentos. (p. 5)

La vulneración de controles por parte de la gerencia es una situación compleja que puede llegar a tener graves implicaciones para una entidad. Esto ocurre cuando los miembros de la alta dirección o gerencia, que deberían ser responsables de establecer y mantener controles y políticas, no siguen o incluso evaden intencionadamente estos controles de seguridad, ignorando procedimientos de seguridad que posee la empresa, ingresando a investigar acerca de información importante de la empresa sin una justificación o en algunos casos llegando a ignorar políticas de privacidad de la entidad.

Castañeda, R.; Guevara, O. y Rojas, K. (2018) manifiesta que:

> El consejo de directores, la alta gerencia y, a nivel funcional, la gerencia encargada de la gestión del riesgo operacional debe demostrar un alto grado de compromiso para mantener una cultura de control interno sólida. Esto implica que las actividades relacionadas con el control del riesgo operacional se integren de manera inherente en los procesos diarios de la entidad. Además, es responsabilidad de las entidades financieras establecer planes de contingencia y de continuidad de la actividad que aseguren la continuación de su capacidad operativa y reduzcan las pérdidas en caso de interrupción de la actividad. (p. 23)

La gerencia de una entidad tiene una serie de responsabilidades críticas para asegurar el buen funcionamiento y la integridad del negocio tanto en el ámbito operativo, como también en el aspecto financiero es por ello que se debe tomar en cuenta la gestión de riesgos financieros la cual trata acerca de un proceso integral cuyo objetivo es salvaguardar los activos e intereses financieros de la entidad y tomando en cuenta también los riesgos de mercado, crédito y liquidez los cuales son de los más importantes para una efectiva gestión de riesgos.

KPMG (2016) afirma que:

> El 34% de los defraudadores corresponde a ejecutivos o directores no ejecutivos; el 32% se compone de gerentes, mientras que el 20% está conformado por miembros del personal. (En 2013, las proporciones respectivas fueron del 32 por ciento, 25 por ciento y 16 por ciento).
>
> El 42 por ciento de las agresoras son miembros del personal (en comparación con el 46 por ciento en 2010), el 38 por ciento son gerentes (en comparación con el 28 por ciento en 2010) y el 13 por ciento son

> ejecutivas. Sus homólogos masculinos representaron sólo el 15 por ciento de los defraudadores a nivel de personal y el 32 por ciento a nivel directivo. (p. 56)

Los defraudadores ejecutivos, a veces conocidos como defraudadores de cuello blanco o delincuentes corporativos, son individuos que ocupan cargos de alta dirección en una organización y que cometen actos de fraude o conducta delictiva para obtener beneficios personales o para manipular los resultados financieros de la empresa. Estas acciones pueden afectar de manera considerable la salud económica y la reputación de la entidad.

2.2.3 Marco Legal

Según el **Congreso de la república en la Ley N.º 30096 "Ley de delitos informáticos"** nos menciona lo siguiente:

> El propósito de la presente legislación es prevenir y castigar los comportamientos ilícitos que perjudican a los sistemas y datos informáticos, así como otros bienes jurídicos de relevancia penal. Estos actos se llevan a cabo mediante el uso de tecnologías de la información o la comunicación, con el objetivo de asegurar una lucha eficaz contra la ciberdelincuencia.
>
> Artículo 2.- Acceso ilícito: Quien ingrese a un sistema informático total o parcialmente sin autorización, siempre que esta acción implique la violación de las medidas de seguridad establecidas para evitarlo, enfrentará una sanción que incluirá una pena privativa de libertad de uno a cuatro años y una multa que oscilará entre treinta y noventa días.

El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado. Artículo 3.- Atentado contra la integridad de datos informáticos: El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

Artículo 3.- Atentado a la integridad de datos informáticos: El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

Artículo 4.- Atentado contra la integridad de sistemas informáticos: Quien, mediante el uso de tecnologías de la información o la comunicación, deshabilite total o parcialmente un sistema informático, obstaculice el acceso a éste, dificulte o impida su funcionamiento o la prestación de sus servicios, enfrentará una sanción que conllevará una pena privativa de libertad no inferior a tres años ni superior a seis años, junto con una multa que oscilará entre ochenta y ciento veinte días. Atentado a la integridad de sistemas informáticos: Quien de manera intencionada y sin legitimidad deshabilite, total o parcialmente, un

> sistema informático, obstaculice el acceso a este, obstaculice o impida su funcionamiento o la provisión de sus servicios, será sancionado con una pena de privación de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

Conociendo la Ley N°30096 del Congreso de la república podemos resaltar la creciente ola de fraude cibernético que afronta el país debido a la falta de controles, deficiencias en los sistemas o simplemente falta de capacitación al personal para mantener siempre su información bien resguardada, de igual forma la ley nos menciona algunas de las sanciones establecidas según sea el tipo de delito cometido y señalando que las sanciones por delitos informáticos son no menores a tres años de pena privativa de la libertad.

Variable Dependiente: Fraude informático

Jiménez, D. y Namuche, J. (2019) indican que:

> Es esencial tener en cuenta que muchos de los riesgos no se originan externamente a la empresa, sino que surgen internamente en los centros de trabajo o áreas usuarias. Estos riesgos incluyen la presencia de errores, omisiones, fraudes, prácticas indebidas, concentración excesiva de funciones administrativas y operativas, así como empleados desmotivados, descuidados, mal remunerados o deshonestos. Por esta razón, la función y la atención de la auditoría informática son fundamentales. Su objetivo es garantizar una seguridad adecuada que proteja todos los recursos informáticos, desde los datos más simples hasta el activo más valioso: el talento humano, que impulsa el desarrollo y la vitalidad de los sistemas de información. (p. 59)

Es por ello que resaltamos la función de la auditoría informática, la cual ha evolucionado de ser simplemente un respaldo para el auditor financiero a convertirse en una tarea independiente y en constante desarrollo. Esto se alinea de manera más adecuada con la creciente importancia que los sistemas informáticos y la información tienen para las empresas, los cuales son el enfoque central de estudio y análisis por parte de esta función. Este cambio refleja la necesidad de abordar de manera específica y proactiva los desafíos y riesgos asociados con la tecnología de la información, reconociendo su papel crítico en el funcionamiento y éxito de las organizaciones en el presente y en el futuro.

KPMG (2022) menciona lo siguiente:

> Las compañías de mayor tamaño enfrentan un riesgo significativamente mayor de fraude. Asimismo, tienen una probabilidad más elevada de incurrir en pérdidas debido a fraudes internos (originados por empleados, gerentes, funcionarios o propietarios) o fraudes externos (iniciados por terceros, como clientes o proveedores). De aquellos encuestados pertenecientes a empresas con ingresos de al menos USD 10,000 millones, solo el 15% afirmó no haber experimentado pérdidas por fraude en el último año. Este porcentaje es aproximadamente la mitad en comparación con las empresas más pequeñas, donde el 29% informa la ausencia de pérdidas por fraude. Resulta evidente que los perpetradores identifican mayores oportunidades en las organizaciones de mayor tamaño. (p. 4)

Tomando en consideración lo mencionado, se puede constatar el peligro inminente que afrontan las organizaciones, de igual forma se connota que las

empresas de mayor tamaño tienen un riesgo más elevado de afrontar fraude debido a que los trabajadores corruptos pueden identificar falencias con mayor facilidad.

PwC (2018) manifiesta que:

> Existe un elemento esencial que no podemos pasar por alto, ya que es claramente el factor principal en este proceso, y ese factor es el ser humano. Detrás de cada máquina, detrás de cada acto fraudulento, hay un individuo que desempeña un papel destacado en este escenario. ¿Cuáles son las razones que llevan a una persona o a un tercero de una empresa a decidir participar en actividades de fraude informático? Se pueden enumerar diversas razones, pero sin duda hay una que se aplica a todos: los principios y valores que guían a una sociedad ética quedan relegados a un segundo plano, y el individuo está dispuesto a pasar por alto estos principios, asumiendo los riesgos y las consecuencias que puedan derivarse, con el fin de alcanzar sus objetivos. (p. 4)

Como se puede apreciar el autor enfatiza en un factor fundamental para que se dé a cabo el fraude informático, este factor es el humano, el cual se encarga de identificar fallos en los controles internos de la compañía y así perpetrar a sus sistemas de información para extraer datos o documentos importantes, beneficiándose de esta forma y generando un perjuicio a la empresa en cuestión.

Malversación de Fondos

Pariona, R. (2019) menciona que:

> La malversación de fondos se considera un delito penal conforme al artículo 389 del Código Penal. Este artículo sanciona conductas que causan un perjuicio significativo al funcionamiento de la administración pública y a la prestación de servicios públicos a los ciudadanos. La malversación de fondos públicos implica desviar recursos hacia un propósito diferente al previamente establecido, causando un daño grave y duradero a los servicios brindados por el estado. (p. 6)

Como sabemos la malversación de fondos es un delito penal que ha existido durante muchos años en distintas entidades ya sean públicas o privadas, no obstante una de las mejores formas para moderar el incremento de dicho accionar ilícito es realizar controles de forma constante en todos los procesos que contengan un mayor índice de riesgo de fraude, en cuanto al sistema de bancas digitales se han encontrado múltiples fallos de seguridad los cuales fueron detectados a tiempo y sin que se genere un daño significativo a la entidad gracias a los oportunos controles que efectuaba la compañía.

Torres, V. (2020) indica que:

> Cuando se detectan malversaciones de fondos, la información suele ser conocida en primer lugar por la población, los medios de comunicación y, por supuesto, la contraloría general de la república. Sin embargo, en muchos casos, las autoridades intentan evadir cualquier tipo de control, desconociendo que los mecanismos de supervisión eventualmente descubrirán estas irregularidades. A la luz de estos comentarios y hechos, se considera pertinente proponer, a través de esta

> investigación, un plan de auditoría forense como una herramienta de control y supervisión para identificar posibles actividades ilegales en la municipalidad de Eten en el futuro, como la malversación de fondos. De esta manera, se estaría demostrando a la ciudadanía un compromiso efectivo en la lucha contra la corrupción, que tanto perjudica el desarrollo social de una ciudad y en general, de nuestro país. (p. 12)

Aunque es evidente que con el transcurso del tiempo se han introducido nuevos enfoques para eludir los controles que la entidad puede llevar a cabo con el fin de proteger sus intereses, eventualmente todo queda al descubierto, esto se llega a dar a cabo gracias a la auditoría forense, la cual muchas veces se utiliza como una herramienta de supervisión para los controles de las empresas, de esta forma lograr identificar los fallos pasados, así como también los posibles fallos a futuro, para poder así erradicar los terribles índices de corrupción por la cual pasa nuestro país.

Chanjan, R.; Torres, D. y Gonzales, M. (2020) refiere que:

> El delito de malversación de fondos tiene como sujeto activo al funcionario o servidor público que desvía de manera definitiva el dinero o bienes que administra hacia un propósito diferente al destinado originalmente. En este contexto, no es suficiente ser simplemente un funcionario público; es necesario que exista una conexión funcional con el dinero o los bienes del estado. Esta conexión se establece a través del cargo que ocupa como administrador de dichos bienes, permitiendo su aplicación para fines oficiales. El sujeto pasivo de este delito es el estado, ya que se está utilizando parte de su patrimonio para propósitos distintos a los establecidos en beneficio del interés público. (p. 9)

En referencia a lo mencionado por parte del autor, se puede resaltar el terrible accionar que se ejecuta cuando hablamos de malversación de fondos, ya que al producirse dicha malversación la persona no solo pierde su integridad, sino también defrauda la confianza y utiliza de forma ilícita un dinero destinado a una actividad puntual para obtener un beneficio propio.

Gestión de riesgo de fraude

Hernández, W.; López, H. y Valencia, B. (2015) asegura que:

> La gestión del riesgo de fraude, al igual que cualquier otro riesgo empresarial, requiere ser manejada, lo que implica la comprensión, evaluación y reducción de dicho riesgo. La responsabilidad recae en la alta dirección y las personas que componen el área de auditoría, quienes deben garantizar la implementación de sistemas efectivos para la preparación, detección y respuesta.
>
> **Prevención:**
>
> - Implementación de controles diseñados para mitigar el riesgo de ocurrencia.
> - Establecimiento de un código de ética.
> - Evaluación de antecedentes éticos de empleados, proveedores y clientes.
> - Existencia de políticas de comunicación y entrenamiento en ética y fraude.
> - Implementación de procesos específicos de control de riesgos.
>
> **Detección:**
>
> - Uso de procedimientos orientados a identificar fraudes después de su ocurrencia.

- Auditoría interna.
- Monitoreo de actividades.
- Implementación de líneas éticas.
- Auditoría forense proactiva.

Respuesta:

- Establecimiento de protocolos para llevar a cabo investigaciones.
- Implementación de medidas correctivas.
- Remediación de los daños.
- Desarrollo de planes de acción.
- Implementación de estrategias de comunicación. (p. 26)

Todas las empresas tienen un nivel de riesgo de fraude el cual puede variar entre un nivel alto, intermedio o bajo; esta variación se debe a la calidad y cantidad de controles efectuados por la compañía, es ahí donde toma importancia la gestión de riesgo de fraude ya que dicha gestión nos menciona que el riesgo debe ser conocido, evaluado y mitigado; de esta manera podremos proteger nuestros activos financieros y evitar que el desfalco llegue a ser significativo para la empresa.

De La Torre, M. (2018) menciona que:

> La inclusión de una unidad de auditoría interna en las actividades de una organización es un indicador crucial del compromiso de la misma para establecer un control interno efectivo y gestionar el riesgo de fraude. Los auditores internos desempeñan un papel proactivo al llevar a cabo auditorías destinadas a identificar casos de malversación de activos y presentación de información falsa. Este enfoque puede involucrar el uso de técnicas de auditoría asistidas por computadora (TAAC), como la

> minería de datos, para detectar formas específicas de fraude. Asimismo, los auditores internos pueden aplicar procedimientos analíticos y otros métodos para identificar partidas inusuales y realizar análisis detallados de cuentas y transacciones de alto riesgo, todo con el objetivo de identificar posibles fraudes (IIA, 2009). (p. 6)

La gestión de riesgo de fraude es primordial para detectar de forma temprana algún problema operativo, administrativo o económico, al analizar y comprender los riesgos de fraude específicos a los que está comprometida una organización puede desarrollar estrategias de mitigación más efectivas. Esto puede incluir la puesta en marcha de mecanismos de protección, la capacitación del personal y la adopción de tecnologías avanzadas.

Bermeo, M.; Grajales, D.; Valencia, A. y Palacios, L. (2021) aseguran que:

> El fraude siempre representa una amenaza latente, siendo resultado de una mala administración, ineficacia en el control interno y un exceso de confianza. Este fenómeno conlleva impactos negativos que pueden traducirse en pérdidas económicas, deterioro de la reputación e incluso la desaparición o cierre de la empresa. La propagación de esta conducta antiética, no profesional e ilegal se asemeja a un virus que afecta incluso a las entidades más grandes y prestigiosas a nivel mundial. Por lo tanto, es esencial que las organizaciones reconozcan su papel crucial en la gestión del riesgo de fraude a través de procesos de auditoría, como la auditoría forense, que posibilita la detección, divulgación y certificación de fraudes y delitos en el ámbito tanto público como privado. (p. 739).

Lograr detectar el fraude cibernético es un desafío continuo, esto se debe a que los hackers maliciosos están en un continuo desarrollo de nuevas modalidades

y técnicas para introducirse en los sistemas de las entidades financieras para sustraer dinero o en algunos casos información valiosa por la cual sacaran un beneficio personal en el futuro. Sin embargo, existen varias medidas que las organizaciones y los individuos pueden tomar para reducir significativamente el riesgo de fraude cibernético entre algunas de estas se puede encontrar la actualización constante de los software y sistemas que utilice la entidad ya sea para cargar data o directamente sistemas por los cuales transcurra el dinero de la compañía.

Ciberseguridad

Newmeyer, K. (2015) menciona que:

> Para el propósito actual, definimos la ciberseguridad como el conjunto de prácticas, políticas, entrenamientos y tecnologías diseñadas para proteger el entorno cibernético con el objetivo de garantizar la integridad de la información y la capacidad de conectar dispositivos para que operen según su diseño previsto. (p. 9)

La seguridad informática desempeña un rol fundamental en la detección y prevención del fraude más aún cuando hacemos referencia a entornos digitales, con el paso de los años y el abrupto crecimiento de las tecnologías se han ido desarrollando algunas herramientas que ayudan a disminuir el riesgo de fraude cibernético, como el sistema de prevención y detección de Intrusiones el cual juega un papel importante para detectar y bloquear ataques en tiempo real, así como también los comportamientos anómalos los cuales pueden ser causados por un virus o directamente un hacker queriendo ingresar al sistema utilizado por la empresa.

Gutiérrez, G. y Necochea, P. (2020) indican que:

> La ciberseguridad se refiere a la seguridad de los dispositivos en línea, abarcando tanto el hardware como el software y los datos, contra las amenazas digitales. En el ámbito informático, la seguridad incluye tanto la ciberseguridad como la seguridad física. Ambas son utilizadas por las empresas con el fin de resguardarse contra accesos no autorizados a centros de datos y otros sistemas informáticos. La seguridad de la información, que busca preservar la confidencialidad, integridad y disponibilidad de los datos, constituye un subconjunto de la ciberseguridad. (p. 33)

El fraude cibernético, también conocido como ciberfraude, se refiere a las prácticas delictivas que se realizan mediante el uso de tecnologías de la información y comunicación. Este tipo de fraude puede variar en complejidad y pueden afectar a individuos, empresas, gobiernos e incluso organizaciones sin fines de lucro, en la actualidad existen muchos tipo de fraude cibernético, entre los más resaltantes se encuentra el phishing, Ransomware y estafas de soporte técnico, este último tipo de fraude se produce cuando los ciberestafadores se hacen pasar por personal del área de soporte técnico de empresas relacionadas y convencen a la persona de brindar algunos datos personales dando de esta forma acceso a información valiosa.

Salinas, A. (2020) manifiesta que:

> Las herramientas fundamentales de ciberseguridad, como firewalls y defensas contra malware, siguen siendo esenciales, pero ya no se consideran necesariamente como inversiones de alto costo. Estas son medidas básicas de seguridad cibernética destinadas a identificar y

> bloquear la mayoría de las amenazas conocidas, por lo que aún conservan su valor. Sin embargo, resulta evidente que no son suficientes por sí solas. El nuevo paradigma de ciberseguridad se enfoca en tecnologías como la autenticación multifactorial, el análisis de comportamiento y la tecnología de engaño. A nivel global, varios países están priorizando el desarrollo de estrategias y modelos de ciberseguridad que puedan hacer frente a la evolución creciente, sofisticada y rápida de los ciberataques. Además, se están estableciendo diversas relaciones y acuerdos internacionales para respaldarse mutuamente en esta área crítica. (p. 12)

La creciente ola de ciberdelitos ha obligado a muchas empresas a optar por un sistema de defensa superior como la autenticación multifactorial el cual es un método de seguridad que requiere más de una forma de autenticación de un usuario antes de concederle acceso a un sistema o servicio. Este enfoque añade un nivel extra de resguardo, ya que incluso si un factor de autenticación se ve comprometido, el acceso no se concede a menos que se proporcionen otros factores válidos.

2.3. Términos técnicos.

- **Auditoría Interna:** La auditoría interna es un procedimiento estructurado y objetivo de evaluación y análisis de las operaciones, procedimientos, controles y sistemas de una organización, realizado por un departamento interno o equipo de auditores independientes.

- **Ciberseguridad:** Mayormente conocida como seguridad de la tecnología de la información (TI) o seguridad digital, se refiere a un conjunto de prácticas,

tecnologías y medidas diseñadas para salvaguardar conexiones, datos y dispositivos contra amenazas y riesgos cibernéticos.

- **Controles Internos:** Son operaciones, políticas y prácticas establecidos para contribuir a la organización en el cumplimiento de sus objetivos, así como proteger sus bienes, asegurar la veracidad de la información financiera y operativa, y cumplir con las leyes y normativas vigentes. Estos controles son esenciales para la gestión eficaz de riesgos y la prevención de fraudes.

- **Fraude:** Es una acción deliberada y engañosa, llevada a cabo con el propósito de obtener ganancias financieras, bienes, servicios o ventajas de manera ilegítima o injusta, a expensas de otra persona, entidad o grupo. En esencia, el fraude implica engañar a alguien con el propósito de obtener beneficios indebidos.

- **Fraude Cibernético:** También conocido como cibercrimen, es un término que se refiere a actos delictivos que involucran el uso de tecnología informática y redes de comunicación para cometer engaños, robos, estafas u otros delitos cibernéticos. Estos delitos se realizan en línea y a menudo se dirigen a sistemas informáticos, redes, datos, usuarios o dispositivos electrónicos. El fraude cibernético puede afectar a individuos, empresas, gobiernos y otras organizaciones, y puede tomar diversas formas.

- **Fraude Interno:** Se refiere a actos fraudulentos llevados a cabo por empleados, directivos u otros individuos dentro de la organización. A diferencia del fraude externo, que involucra a personas o entidades externas a la empresa, el fraude interno se origina y se ejecuta desde dentro de la misma organización.

- **Malversación de fondos:** También conocida como desfalco o apropiación indebida de fondos, es un delito financiero que implica la apropiación o desvío ilegal de dinero o activos de una organización o entidad, generalmente con el propósito de beneficio personal. Este acto implica que una persona confiada con el manejo o la custodia de los fondos o activos de una entidad los utilice de manera indebida.

- **Riesgo de fraude:** Hace referencia a la factibilidad de que ocurra un acto de fraude que pueda causar daño financiero, operativo o reputacional a la organización. Los riesgos de fraude pueden tomar diversas formas y pueden involucrar a empleados, clientes, proveedores u otras partes relacionadas.

- **Vulneración de Controles:** Se trata de circunstancias en las que los mecanismos internos diseñados para proteger los activos, asegurar la veracidad de la información financiera, y cumplir con las normativas, resultan ineficientes o están en riesgo de ser vulnerados. Esta vulneración puede ocurrir por diversas razones, como errores, omisiones, negligencia, falta de supervisión, malas prácticas, fraudes o fallas en la implementación de los controles.

CAPÍTULO III: HIPÓTESIS Y VARIABLES

3.1 Hipótesis General

La auditoría interna incide favorablemente en la detección del fraude informático en sector banca digital en Lima Metropolitana, año 2022.

3.2 Hipótesis Específica

a. El control interno incide en la disminución de la malversación de fondos en la banca digital

b. El cumplimiento de las normas de auditoría y de información financiera (NIAS) incide en la gestión de riesgo de fraude en la banca digital.

c. La vulneración de controles por parte de la gerencia incide en la aplicación de la ciberseguridad en las empresas en la banca digital.

3.3 Operacionalización de variable

3.3.1 Variable Independiente: La auditoría interna

Tabla 1. Operacionalización de la variable independiente: La auditoría interna

<table>
<tr><td>Definición Conceptual</td><td colspan="2">La auditoría interna:
Consejo de administración del The institute of internal auditors- IIA (2011):
La función de auditoría interna consiste en una actividad objetiva e independiente de garantía y asesoramiento, diseñada para mejorar y añadir valor a las operaciones de una organización. Contribuye al logro de los objetivos organizativos mediante la aplicación de un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos relacionados con la gestión de riesgos, control y gobierno.</td></tr>
<tr><td rowspan="4">Definición Operacional</td><td>Indicadores</td><td>Índices</td></tr>
<tr><td rowspan="2">X1. Control Interno</td><td>X.1.1. Seguridad electrónica</td></tr>
<tr><td>X.1.2. Controles informáticos</td></tr>
<tr><td>X2. Cumplimiento de las Normas De Auditoría y</td><td>X.2.1. Normas de Información Financiera</td></tr>
</table>

	de Información Financiera (NIAS)	(NIIF)
		X.2.2. Normas frente a casos de fraude cibernético
	X3. Vulneración de Controles por parte de la Gerencia	X.3.1. Riesgo significativo
		X.3.2. Especialista externo dentro del área de TI
Escala Valorativa	Nominal / Ordinal	

Fuente: Elaboración propia

3.3.2. Variable Dependiente: Fraude informático: Fraude informático

Tabla 2. Operacionalización de la variable independiente

Definición Conceptual	**Fraude informático:** Acosta, M.; Benavides, M. y García, N (2020): El fraude informático en las empresas se refiere a prácticas fraudulentas que involucran la utilización de tecnologías digitales para cometer actos ilegales con el objetivo de obtener beneficios económicos, acceso no autorizado a información confidencial, o causar daño a la empresa. Estos fraudes pueden manifestarse de diversas formas y afectar diferentes

	aspectos de la operación empresarial.	
Definición Operacional	Indicadores	Índices
	Y1. Malversación de fondos	Y.1.1. Gestión de recursos tecnológicos
		Y.1.2. Cambios en los patrones de gastos
	Y2. Gestión de riesgo de fraude	Y.2.1. Programa de prevención de fraude
		Y.2.2. Nivel de confianza en los controles
	Y3. Ciberseguridad	Y.3.1. Amenazas digitales
		Y.3.2. Infraestructura tecnológica
Escala Valorativa	Nominal / Ordinal	

Fuente: Elaboración propia

CAPÍTULO IV: METODOLOGÍA

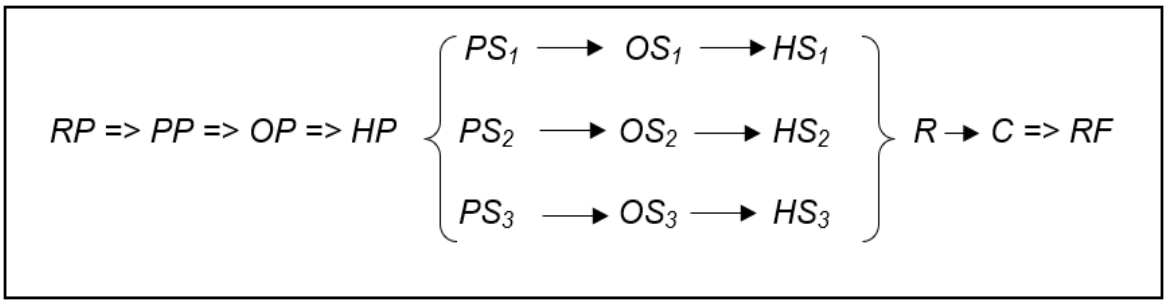
4.1 Diseño Metodológico

4.1.1 Tipo de investigación

La presente tesis titulada “La auditoría interna y su incidencia en el fraude informático en la banca digital en Lima Metropolitana en el año 2022” reúne las características necesarias para ser denominada “Investigación Aplicada”, ya que el estudio busca dar solución a una determinada situación o planteamiento de problema a través de la aplicación y consolidación de conocimientos adquiridos, al mismo tiempo permitirá obtener nuevos conocimientos que enriquecerán el desarrollo científico.

Figura 4. Tipo de investigación

Tipo de investigación



Donde:

RP: Realidad problemática PE^{i}: Problemas secundarios ^{i}= 1,2,3.

PG: Problema principal OE^{i}: Objetivos secundarios ^{i}= 1,2,3.

OG: Objetivo principal HE^{i}: Hipótesis secundarias ^{i}= 1,2,3.

HG: Hipótesis principal C: Conclusiones

R: Resultado RF: Recomendaciones finales

4.1.2 Nivel de investigación

En lo que respecta al alcance de la investigación, este estudio se ubica en el nivel descriptivo-correlacional. En este contexto, se detallan las particularidades y teorías relacionadas con el proceso de la auditoría interna enfocada en la detección de fraudes cibernéticos. Además, se lleva a cabo una

evaluación del grado de relación que existe entre las distintas variables e indicadores pertinentes.

4.1.3 Método

Los métodos que se aplicarán en la presente tesis titulada “La auditoría interna y su incidencia en el fraude informático en la banca digital en Lima Metropolitana en el año 2022” son el analítico, estadístico, descriptivo y de síntesis, entre otros.

4.1.4 Diseño

El diseño que se aplicará en la actual tesis titulada “La auditoría interna y su incidencia en el fraude informático en la banca digital en Lima Metropolitana en el año 2022” es el no experimental. Se seleccionó una muestra en la que se satisface la relación.

M= Ox r Oy

Donde:

M = muestra.

O = observación.

x = beneficios tributarios.

y = rentas de trabajo.

r = relación de variables.

4.2. Población y muestra

4.2.1 Población

La investigación se compone de un conjunto específico de individuos que conforman la población y que ha sido claramente definido en términos de sus características y criterios de inclusión por las cantidades de empresas de banca digital.

Tabla 3. Empresas a encuestar

N°	***Empresas***	***Número de trabajadores***	***Población específica de trabajadores especializados***
1	*Pride*	*482*	*20*
2	*Young*	*453*	*18*
3	*KIPA*	*421*	*18*
4	*Nivas*	*408*	*15*
5	*BHS*	*354*	*12*
6	*Timmy*	*269*	*12*
TOTAL		***2387***	***95***

Elaboración propia

Nota: Se ha modificado el nombre de las compañías referidas en la Tabla 1 con el fin de preservar la confidencialidad de dichas entidades.

4.2.2 Muestra

Se aplicará el método de muestreo aleatorio simple con el fin de obtener una estimación de las proporciones correspondientes a una población conocida, permitiendo así determinar el tamaño adecuado de la muestra.

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

Donde:

n = muestra por hallar.

N = tamaño de la población, conformado por 95 profesionales con experiencia en áreas relacionadas a la auditoría interna, controles internos y tecnología de la informática ubicados en Lima Metropolitana.

p = probabilidad de éxito (0.8).

q = probabilidad de fracaso (0.2).

Z = valor de distribución normal estándar que esté asociado a un nivel de confianza. Para el estudio presentado se considera una probabilidad de error equivalente a un intervalo de confianza del 95%. Teniendo un valor de Z= 1.96.

E = margen de error 5%.

Remplazando se obtiene:

$$n = \frac{(0.8 * 0.2) * 1.96^2 * 95}{(0.05)^2(95-1) + (0.8 * 0.2)\ 1.96^2}$$

***n** = 69 personas*

Como consecuencia, se ha obtenido una muestra conformada por 69 individuos. Este valor será empleado para calcular el factor de distribución muestral, el cual a su vez determinará la cantidad de trabajadores que deben ser encuestados por cada empresa mediante la aplicación de la fórmula que se detalla a continuación:

$(fdm) = n/N$ n_i=n/N*Ni, donde i=1,2,3…,k

k = número de trabajadores en la población específica.

$\boldsymbol{Fdm}$ **=** 69/95.

$\boldsymbol{fdm}$ **=** 0.726316.

Verificación:

95 * 0.726316 = 69, como resultado se obtiene un número entero aproximado a 69, valor que es coincidente con lo establecido en la muestra en la sección 4.2.2. del presente trabajo de investigación.

Sustituyendo la fórmula proporcionada para cada entidad empresarial, se calculan las cifras correspondientes de empleados a ser encuestados. Estos resultados representan los valores obtenidos a partir de la muestra, como se indica a continuación:

Tabla 4: Muestra considerada a encuestar por cada empresa

N°	Empresas	N	Muestra
1	Pride	*20*	15
2	*Young*	*18*	13
3	*KIPA*	*18*	13
4	*Nivas*	*15*	10
5	*BHS*	*12*	9
6	*Timmy*	*12*	9
TOTAL		**95**	**69**

Fuente: Portal Sunat

Elaboración propia

4.3 Técnicas de recolección de datos

4.3.1 Descripción de los métodos, técnicas e instrumentos

En el presente trabajo de investigación se utilizará como técnica de recolección de datos a la encuesta y como instrumento al cuestionario, el cual se compone por un total de 14 preguntas relacionadas con las variables, indicadores e índices, cada pregunta cuenta con 5 opciones de respuestas de la escala de Likert con el fin de brindar a nuestros encuestados una variedad de alternativas en las que puedan escoger la que les parezca la más acertada posible.

4.3.2 Procedimientos de comprobación de la validez y confiabilidad de los instrumentos

Validez

El propósito de la etapa de validación es verificar la eficiencia, eficacia y efectividad de las técnicas de investigación empleadas. Con el objetivo de evaluar la confiabilidad de dichas técnicas, se procederá a enviar el trabajo a profesionales expertos, quienes lo revisarán minuciosamente y proporcionarán su aprobación como proceso de validación.

Tabla 5. Tabla de Validez

Calificación del instrumento de la validez por juicio de expertos

N°	Expertos	Calificación
01	Mtr. Prado Ayala, Arlene	Aprobado
02	Dr. Huarca Ochoa, Javier Marcelo	Aprobado
03	Dr. Centeno Cardenas, Josue Giraldo	Aprobado

Fuente: Elaboración propia

Confiabilidad

La confiabilidad implica que los datos recopilados a través de la utilización de los instrumentos son coherentes y estables. En otras palabras, son seguros y fiables para fundamentar conclusiones y recomendaciones válidas y efectivas en el contexto de este estudio de investigación.

Se realizará una prueba piloto en un 10% de la muestra de los trabajadores del área de administración de personal y contabilidad de las empresas de telecomunicaciones del distrito de Santiago de Surco, con el fin de asegurar la confiabilidad en el presente estudio.

Tras la aplicación de las técnicas de recopilación de datos, específicamente la encuesta en este caso, los resultados obtenidos serán sometidos a procesamiento mediante el uso de las herramientas informáticas Microsoft Excel y SPSS. Este procedimiento tiene como objetivo determinar el indicador de confiabilidad conocido como el Alfa de Cronbach.

Rango de variación

$0 \leq \alpha \leq 1$

Los datos derivados de las encuestas se considerarán altamente seguros, confiables y robustos, siempre que el índice α sea igual o superior a 0.7. En este estudio en particular, se empleará el método de varianzas para el cálculo, y la fórmula correspondiente se llevará a cabo mediante el uso de las herramientas estadísticas proporcionadas por los programas SPSS y Microsoft Excel.

$$\alpha = \frac{K}{K\text{-}1}\left[1 - \frac{\sum_{i=1}^{k} S_i^2}{S_T^2}\right]$$

Siendo:

K = número de ítems.

$\mathbf{S_i^2}$= varianza del número de ítems.

$\mathbf{S_t^2}$= varianza total de los valores observados.

Se utilizará la metodología de Alfa de Cronbach, aplicándolo al 10% de la muestra, la cual está representada por 6 trabajadores del área de auditoría interna y controles

internos. Para la selección de estos colaboradores, se usó el muestreo aleatorio sistemático, Así se logra obtener el resultado correspondiente utilizando ambos programas de validación:

Microsoft Excel

Tabla 6: Resumen procesamiento de datos

Encuestado	X	X.1.1	X.1.2	X.2.1	X.2.2	X.3.1	X.3.2	Y	Y.1.1	Y.1.2	Y.2.1	Y.2.2	Y.3.1	Y.3.2	Total
3	1	2	1	1	1	1	1	1	2	1	2	1	1	2	18
12	1	1	1	1	1	1	1	1	1	1	1	1	1	1	14
15	1	2	1	2	1	2	1	1	2	1	2	1	1	1	19
33	1	2	1	1	1	1	1	1	1	1	1	1	1	1	15
44	1	2	2	1	2	2	1	1	2	1	2	2	1	1	21
46	1	1	2	1	1	2	1	1	2	2	2	1	2	1	20
Var. P.	0.00	0.22	0.22	0.14	0.14	0.25	0.00	0.00	0.22	0.14	0.22	0.14	0.14	0.14	107

Fuente: Resultado de la encuesta

Elaboración propia

Para obtener el Alfa de Cronbach se hallará lo siguiente:

ΣS_i^2= Varianza del número de ítems.

ΣS_i^2 = 0.00 +0.22 +0.22 +0.14 +0.14+ 0.25 +0.00 +0.00 +0.22 +0.14 +0.22 +0.14 +0.14 +0.14

ΣS_i^2 = 1.97222

S_t^2=Varianza total de los valores observados.

S_t^2 =VAR.P(18+14+19+15+21+20)

S_t^2 = 6.472222

K = 14 (catorce preguntas)

Reemplazando los datos obtenidos en la siguiente fórmula:

$$\alpha = \frac{K}{K\text{-}1}\left[1 - \frac{\sum_{i=1}^{k} S_i^2}{S_T^2}\right]$$

$$a = \frac{14}{14-1}[1 - \frac{1.97222}{6.47222}]$$

a = 0.7488

Software estadístico SPSS

Una vez reemplazados los datos para identificar el Alfa de Cronbach usando Microsoft Excel, validaremos la respuesta por medio del software estadístico SPSS, del cual se obtiene los resultados en mención:

Tabla 7: Resumen de procesamiento de datos

		N	%
Casos	Válido	6	100,0
	Excluido[a]	0	,0
	Total	6	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Fuente: Programa SPSS versión 25 - Resultado de la encuesta

Elaboración Propia

Tabla 8: Estadísticas de fiabilidad

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,806	14

Fuente: Programa SPSS versión 25

Elaboración Propia

La prueba piloto calculada en el presente estudio muestra un resultado de 0.806, lo que indica un nivel excelente de confiabilidad según la tabla 5

Tabla 9: Rangos de confiabilidad

RANGO	CONFIABILIDAD
0.53 a menos	Confiabilidad nula
0.54 a 0.59	Confiabilidad baja
0.60 a 0.65	Confiable
0.66 a 0.71	Muy confiable
0.72 a 0.99	Excelente confiabilidad
1	Confiabilidad perfecta

Fuente: Análisis de confiabilidad y validez de un cuestionario sobre entornos personales de aprendizaje.

Concluyendo que una vez realizado la validación técnica con los programas SPSS y Microsoft Excel y obtener los mismos resultados, se confirma la confiabilidad de la técnica e instrumento de investigación.

CAPÍTULO V: RESULTADOS

5.1. Presentación

El presente capítulo corresponde al trabajo de campo realizado a nuestros 69 profesionales encuestados especialistas en auditoría interna y fraude informático ubicados en Lima Metropolitana, seleccionados de una población de 95 especialistas, los cuales cuentan con una vasta experiencia en temas relacionados a nuestra investigación “La auditoría interna y su incidencia en el fraude informático en la banca digital en Lima Metropolitana en el año 2022”.

Los resultados obtenidos corresponden al desarrollo de los siguientes objetivos específicos:

a. Se determinó si el control interno incide en la disminución de la malversación de fondos en la banca digital.

b. Se analizó si el cumplimiento de las normas de auditoría y de información financiera (NIAS) incide en la gestión de riesgo de fraude en la banca digital.

c. Se definió si la vulneración de controles por parte de la gerencia incide en la aplicación de la ciberseguridad en la banca digital.

5.2. Interpretación de resultados

Por medio de la aplicación de la técnica de encuesta dirigida a auditores especialistas en fraude informático, se presenta e interpreta los siguientes resultados:

Variable Independiente (X): Auditoría interna

5.2.1. Ante la pregunta ¿Está usted de acuerdo que las empresas de banca digital deben contar con un área de auditoría interna especializada en fraude cibernético?

Tabla 10: Auditoria interna

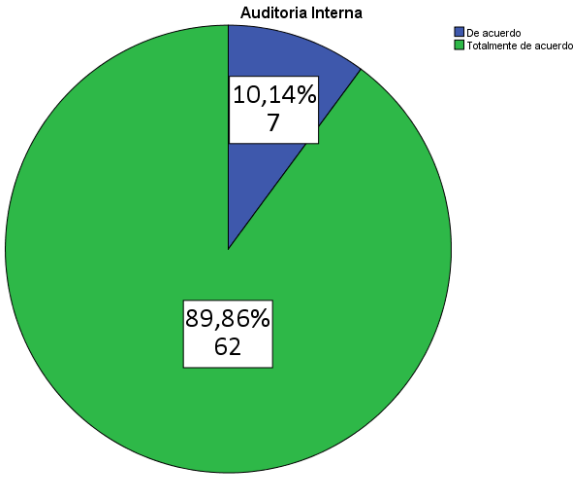
Auditoria Interna

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	De acuerdo	7	10,1	10,1	10,1
	Totalmente de acuerdo	62	89,9	89,9	100,0
	Total	69	100,0	100,0	

Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

Figura 5: Auditoría interna



Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

Con relación a la tabla 10 y figura 5, se observó que el 89.86% de encuestados indicaron que están totalmente de acuerdo con que las empresas de banca digital deben contar con un área de auditoría interna especializada en fraude cibernético, de igual forma un 10.14% manifestaron que se encuentran de acuerdo en que las empresas de banca digital deben contar con un área de auditoría interna especializada en fraude cibernético.

Este resultado sugiere que las empresas de banca digital ubicadas en Lima Metropolitana deben contar con un área de auditoría interna especializada en fraude cibernético, para de esta forma lograr un mayor control en sus sistemas de seguridad y disminuir el nivel de riesgo de fraude.

5.2.2. Ante la pregunta ¿Está usted de acuerdo que tomar en cuenta las recomendaciones de la auditoría interna beneficia a la seguridad electrónica de la empresa al detectar el fraude cibernético?

Tabla 11: Seguridad electrónica

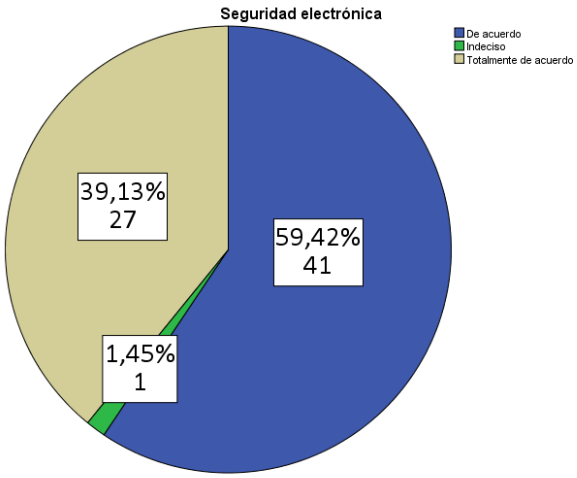
Seguridad electrónica

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	De acuerdo	41	59,4	59,4	59,4
	Indeciso	1	1,4	1,4	60,9
	Totalmente de acuerdo	27	39,1	39,1	100,0
	Total	69	100,0	100,0	

Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

Figura 6: Seguridad electrónica



Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

En relación a la tabla 11 y figura 6, se observó que el 59.42% de los especialistas encuestados se encuentran de acuerdo con tomar en cuenta las recomendaciones de la auditoría interna beneficia a la seguridad electrónica de la empresa al detectar el fraude cibernético, de igual manera el 39.13% de los encuestados se encuentran totalmente de acuerdo y el 1.45% hace mención a encontrarse indeciso.

En base a los resultados obtenidos en la encuesta se puede inferir que tomar en cuenta las recomendaciones de la auditoría interna beneficia a la seguridad electrónica de la empresa al detectar el fraude cibernético, por lo tanto, deberían considerarlas con mayor frecuencia.

5.2.3. Ante la pregunta ¿Está usted de acuerdo que el control interno debería implementar controles informáticos previamente aprobados por la gerencia de Tecnología de la Información (TI)?

Tabla 12: Controles informáticos

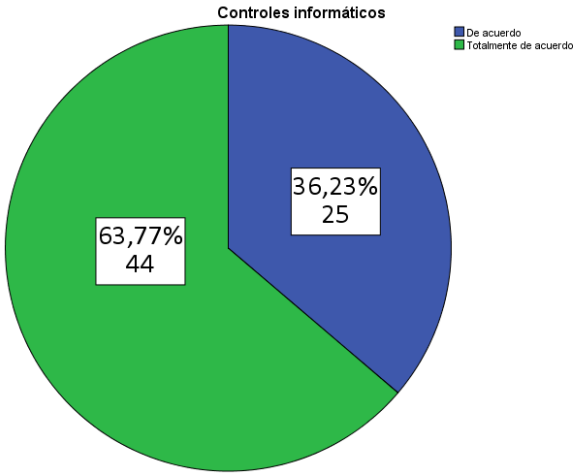
Controles informáticos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	De acuerdo	25	36,2	36,2	36,2
	Totalmente de acuerdo	44	63,8	63,8	100,0
	Total	69	100,0	100,0	

Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

Figura 7: Controles informáticos



Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

Con relación a la tabla 12 y figura 7, se evidenció que el 63.77% de los especialistas encuestados se encuentran totalmente de acuerdo que el control interno debería implementar controles informáticos previamente aprobados por la gerencia de Tecnología de la Información (TI), de igual forma, el 36.23% opina encontrarse de acuerdo con lo previamente mencionado.

En base a los datos obtenidos en nuestra encuesta se puede deducir que el control interno debería implementar controles informáticos previamente aprobados por la gerencia de Tecnología de la Información, con esto se asegurarán que los controles puestos sean más efectivos y eficientes según sea el tipo de riesgo que afronten.

5.2.4. Ante la pregunta ¿Está usted de acuerdo que una auditoría interna debería basar su estrategia bajo el cumplimiento de las Normas de Auditoría de Información Financiera (NIAS) por sobre las Normas de Información Financiera (NIIF)?

Tabla 13: Normas de Información Financiera (NIIF)

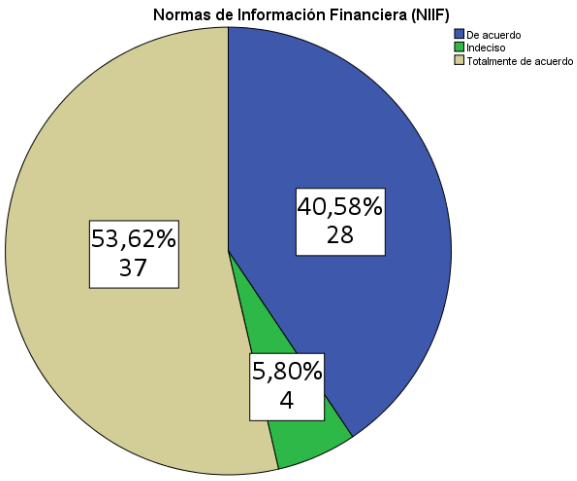
Normas de Información Financiera (NIIF)

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	De acuerdo	28	40,6	40,6	40,6
	Indeciso	4	5,8	5,8	46,4
	Totalmente de acuerdo	37	53,6	53,6	100,0
	Total	69	100,0	100,0	

Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

Figura 8: Normas de Información Financiera (NIIF)



Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

En relación a la tabla 13 y figura 8, se identificó que el 53.62% se encuentra totalmente de acuerdo con que una auditoría interna debería basar su estrategia bajo el cumplimiento de las Normas de Auditoría de Información Financiera (NIAS) por sobre las Normas de Información Financiera (NIIF), el 40.58% se encuentra de acuerdo, mientras que el 5.80% indica estar indeciso con esta decisión.

Tomando en cuenta los datos recolectados de la encuesta se puede deducir que las auditorías internas deberían basar su estrategia bajo el cumplimiento de las NIAS por sobre el de las NIIF, ya que las NIAS se encuentran más orientadas a la auditoría como tal.

5.2.5. Ante la pregunta ¿Está usted de acuerdo que las Normas de Auditoría y de Información Financiera (NIAS) están debidamente actualizadas en respuesta a los casos de fraude cibernético hallados en auditorías internas?

Tabla 14: Normas frente a casos de fraude cibernético

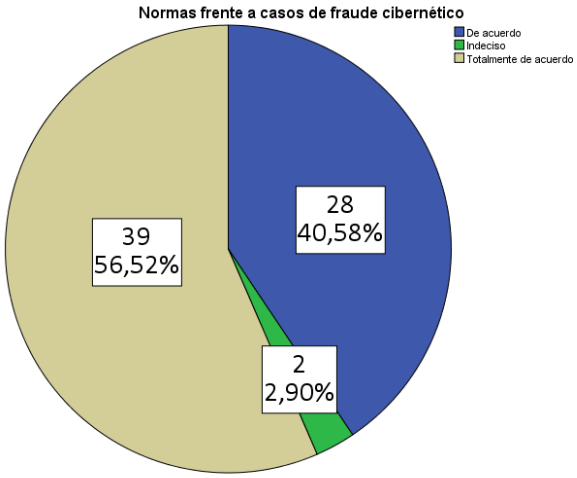
Normas frente a casos de fraude cibernético

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	De acuerdo	28	40,6	40,6	40,6
	Indeciso	2	2,9	2,9	43,5
	Totalmente de acuerdo	39	56,5	56,5	100,0
	Total	69	100,0	100,0	

Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

Figura 9: Normas frente a casos de fraude cibernético



Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

En relación a la tabla 14 y figura 9, nos muestran que el 56.52% de los especialistas encuestados se encuentran totalmente de acuerdo con que las Normas de Auditoría y de Información Financiera (NIAS) estén debidamente actualizadas en respuesta a los casos de fraude cibernético hallados en auditorías internas. el 40.58% de los encuestados mencionan estar de acuerdo, mientras que el 2.90% se mantienen indecisos en relación a su respuesta.

Con estos resultados se puede evidenciar que las NIAS deberían ir actualizando en respuesta a los casos de fraude cibernético hallados en las auditorías internas, de esta forma se podría tener como antecedentes dichos fraudes e ir modificando las NIAS para reducir el riesgo de fraude en las empresas.

5.2.6. Ante la pregunta ¿Está usted de acuerdo que la vulneración de controles por parte de la Gerencia es considerada como el riesgo más significativo en una auditoría interna?

Tabla 15: Riesgo significativo

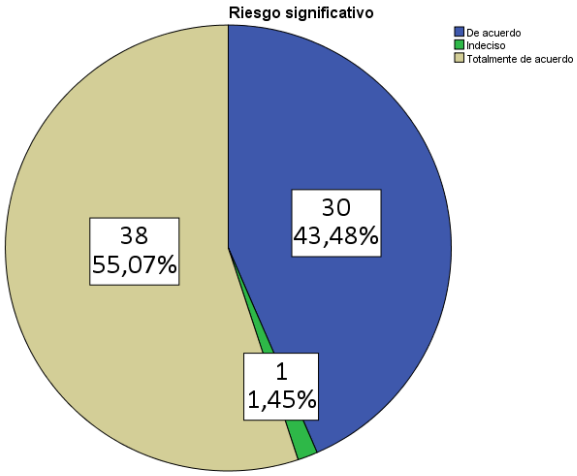
Riesgo significativo

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	De acuerdo	30	43,5	43,5	43,5
	Indeciso	1	1,4	1,4	44,9
	Totalmente de acuerdo	38	55,1	55,1	100,0
	Total	69	100,0	100,0	

Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

Figura 10: Riesgo significativo



Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

Con relación a la tabla 15 y figura 10, se reunió las siguientes respuestas de los especialistas encuestados, el 55.07% se encuentran totalmente de acuerdo con que la vulneración de controles por parte de la Gerencia es considerada como el riesgo más significativo en una auditoría interna, el 43.48% se encuentra de acuerdo y tan solo el 1.45% de los encuestados se encuentran indecisos con dicha premisa.

Tomando en cuenta los resultados obtenidos en la encuesta se puede inferir que la vulneración de controles por parte de la gerencia es considerada como el riesgo más significativo en una auditoría interna, ya que al poseer altos cargos existe menos gente que verifique el cumplimiento de los controles impuestos por la compañía.

5.2.7. Ante la pregunta ¿Está usted de acuerdo que el área de TI debe de contar con personal externo especializado en controles informáticos para un soporte neutral a fin de evitar la vulneración de controles por parte de la gerencia?

Tabla 16: Especialista externo dentro del área de TI

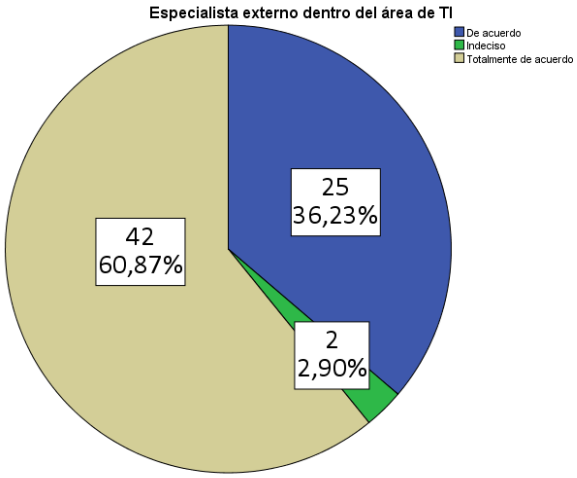
Especialista externo dentro del área de TI

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	De acuerdo	25	36,2	36,2	36,2
	Indeciso	2	2,9	2,9	39,1
	Totalmente de acuerdo	42	60,9	60,9	100,0
	Total	69	100,0	100,0	

Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

Figura 11: Especialista externo dentro del área de TI



Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

En relación a la tabla 16 y figura 11, se encontró que el 60.87% de los especialistas encuestados están totalmente de acuerdo con que el área de TI debe de contar con personal externo especializado en controles informáticos para un soporte neutral a fin de evitar la vulneración de controles por parte de la gerencia, el 36.23% se encuentra de acuerdo y el 2.90% de los encuestados mencionan estar indecisos con respecto a su respuesta.

Considerando la información recolectada de las respuestas de la encuesta se puede deducir que el área de TI debería contar con un especialista externo para un soporte neutral a fin de evitar la vulneración de controles por parte de la gerencia, de esta manera poder obtener un análisis más imparcial en referencia a la vulneración de controles en las empresas.

Variable Dependiente (X): Fraude informático

5.2.8. Ante la pregunta ¿Está usted de acuerdo que las empresas banca digitales deben contar con una matriz de riesgos específicamente ante casos de fraude informático?

Tabla 17: Riesgo significativo

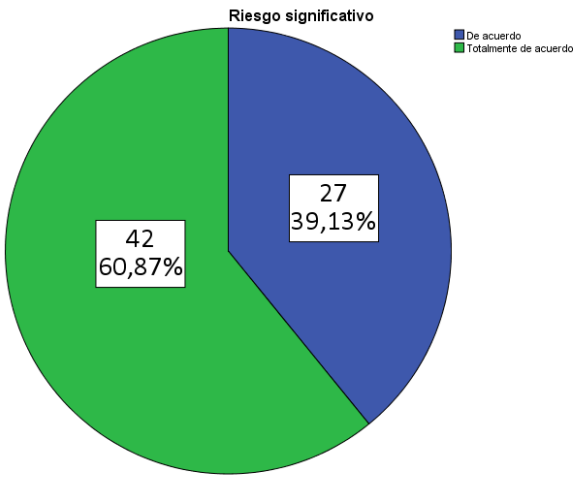
Riesgo significativo

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	De acuerdo	27	39,1	39,1	39,1
	Totalmente de acuerdo	42	60,9	60,9	100,0
	Total	69	100,0	100,0	

Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

Figura 12: Riesgo significativo



Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

Con respecto a la tabla 17 y figura 12, se recolectó la información de que el 60.87% de los especialistas encuestados se encuentran totalmente de acuerdo con que las empresas bancas digitales deben contar con una matriz de riesgos específicamente ante casos de fraude informático, mientras que el 39.13% restante decidió por la opción de acuerdo con respecta a dicha pregunta.

Considerando las respuestas brindadas por nuestros especialistas encuestados, se puede deducir que las empresas de bancas digitales deberían contar con una matriz de riesgos específicamente ante casos de fraude informático, ya que el funcionamiento operacional de dichas empresas es precisamente digital y de esta forma podría ayudar a reducir considerablemente los niveles de fraude.

5.2.9. Ante la pregunta ¿Está usted de acuerdo que la gestión de recursos tecnológicos es importante para que los equipos de TI cumplan las expectativas eficientemente?

Tabla 18: Gestión de recursos tecnológicos

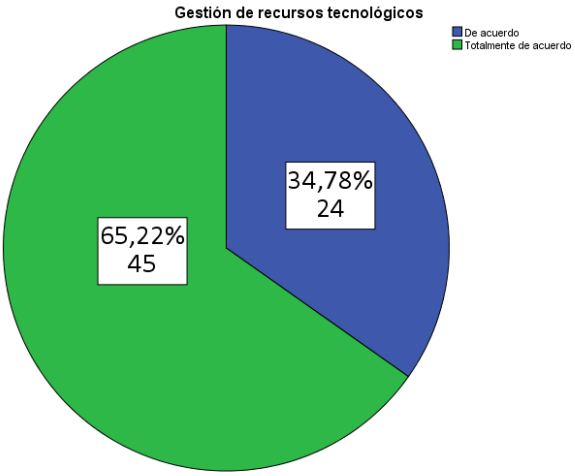
Gestión de recursos tecnológicos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	De acuerdo	24	34,8	34,8	34,8
	Totalmente de acuerdo	45	65,2	65,2	100,0
	Total	69	100,0	100,0	

Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

Figura 13: Gestión de recursos tecnológicos



Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

Con respecto a la tabla 18 y figura 13, se recolectó la información de que el 65.22% de los especialistas encuestados se encuentran totalmente de acuerdo con que la gestión de recursos tecnológicos es importante para que los equipos de TI cumplan las expectativas eficientemente, mientras que el 34.78% restante decidió por la opción de acuerdo con respecta a dicha pregunta.

Considerando las respuestas obtenidas por parte de nuestros especialistas se puede inferir que los recursos tecnológicos son parte fundamental para el adecuado desempeño del departamento de TI, ya que sin los equipos tecnológicos debidamente actualizados se dificultaría en gran parte la labor de identificar algún tipo de fraude informático.

5.2.10. Ante la pregunta ¿Está usted de acuerdo que revisar si existen cambios en los patrones de gastos en la compañía favorece en la detección del fraude?

Tabla 19: Cambios en los patrones de gastos

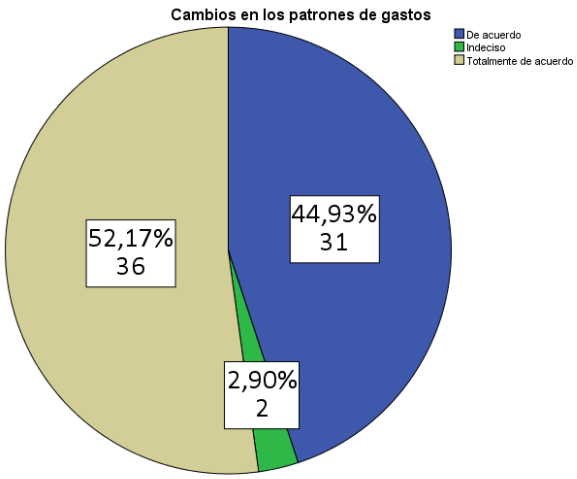
Cambios en los patrones de gastos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	De acuerdo	31	44,9	44,9	44,9
	Indeciso	2	2,9	2,9	47,8
	Totalmente de acuerdo	36	52,2	52,2	100,0
	Total	69	100,0	100,0	

Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

Figura 14: Cambios en los patrones de gastos



Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

En relación a la tabla 19 y figura 14, se encontró que el 52.17% de los especialistas encuestados están totalmente de acuerdo con que revisar si existen cambios en los patrones de gastos en la compañía favorece en la detección del fraude, el 44.93% se encuentra de acuerdo y el 2.90% de los encuestados mencionan estar indecisos con respecto a su respuesta.

Tomando en consideración las respuestas brindadas por parte de nuestros especialistas, se puede deducir que revisar de manera frecuente los cambios en los patrones de gastos en las compañías favorecen a la detección de fraude, esto se debe a que la mayoría de empresas tienen una cantidad de gasto regularmente constante, sin embargo, el hecho de encontrar un gasto desmedido o desproporcionado puede generar suspicacia y este hecho podría favorecer a la detección de fraude.

5.2.11. Ante la pregunta ¿Está usted de acuerdo que los programas de prevención de fraude facilitan a los auditores internos a mitigar los niveles de riesgo dentro de la compañía?

Tabla 20: Programa de prevención de fraude

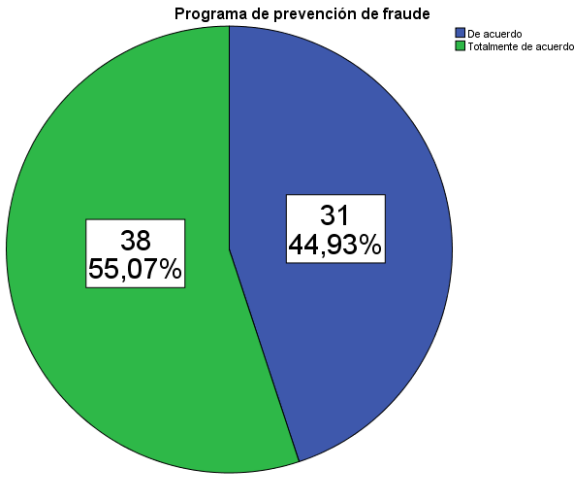
Programa de prevención de fraude

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	De acuerdo	31	44,9	44,9	44,9
	Totalmente de acuerdo	38	55,1	55,1	100,0
	Total	69	100,0	100,0	

Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

Figura 15: Programa de prevención de fraude



Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

Con relación a la tabla 20 y figura 15, se reunió las siguientes respuestas de los especialistas encuestados, el 55.07% se encuentran totalmente de acuerdo con los programas de prevención de fraude facilitan a los auditores internos a mitigar los niveles de riesgo dentro de la compañía y el 44.93% de los encuestados se encuentra de acuerdo con dicha premisa.

Tomando en consideración dichas respuestas, se puede inferir que los programas de prevención de fraude facilitan a los auditores internos a mitigar los niveles de riesgo dentro de la compañía, esto se debe a que dichos programas no solo orientan y brindan capacitaciones a los trabajadores de la compañía, sino también implementan una serie de controles los cuales logran reducir de manera considerable los niveles de riesgo de fraude.

5.2.12. Ante la pregunta ¿Está usted de acuerdo que medir la eficiencia de los controles internos de la compañía brinda soporte para definir los niveles de confianza en controles?

Tabla 21: Nivel de confianza en los controles

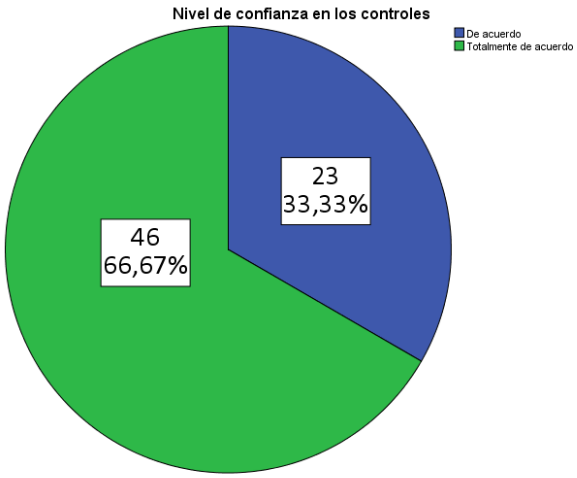
Nivel de confianza en los controles

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	De acuerdo	23	33,3	33,3	33,3
	Totalmente de acuerdo	46	66,7	66,7	100,0
	Total	69	100,0	100,0	

Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

Figura 16: Nivel de confianza en los controles



Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

Con relación a la tabla 21 y figura 16, se observó que el 66.67% de encuestados indicaron que están totalmente de acuerdo con que medir la eficiencia de los controles internos de la compañía brinda soporte para definir los niveles de confianza en controles, de igual forma el 33.33% manifestaron que se encuentran de acuerdo con lo mencionado en la pregunta.

Considerando las respuestas recibidas por parte de nuestros encuestados, se logra inferir que el medir la eficiencia de los controles internos logra proporcionar el nivel de confianza que se le puede otorgar en dichos controles, esto se debe a que la empresa debe estar en constante revisión, no solo del cumplimiento de los controles internos planteados, sino también verificar si los controles siguen siendo funcionales para mitigar el nivel de riesgo que puede poseer la compañía.

5.2.13. Ante la pregunta ¿Está usted de acuerdo que las amenazas digitales son mitigadas por el departamento de TI cuando existe un nivel elevado de ciberseguridad en la compañía?

Tabla 22: Amenazas digitales

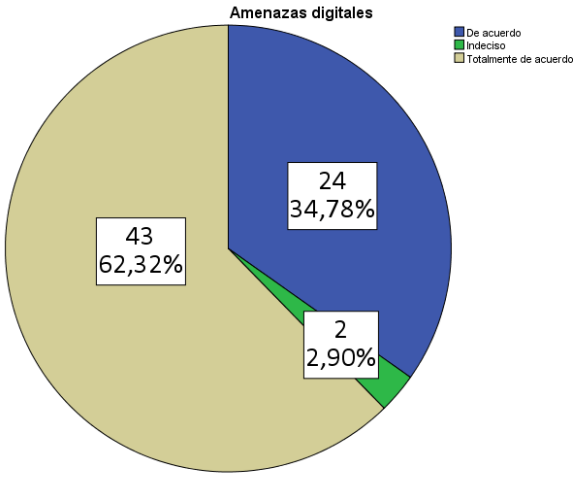
Amenazas digitales

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	De acuerdo	24	34,8	34,8	34,8
	Indeciso	2	2,9	2,9	37,7
	Totalmente de acuerdo	43	62,3	62,3	100,0
	Total	69	100,0	100,0	

Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

Figura 17: Amenazas digitales



Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

Con respecto a la tabla 22 y figura 17, se recolectó la información de que el 62.32% de los especialistas encuestados se encuentran totalmente de acuerdo con que las amenazas digitales son mitigadas por el departamento de TI cuando existe un nivel elevado de ciberseguridad en la compañía, mientras que el 34.78% decidió por la opción de acuerdo, por último, tenemos el 2.90% de los encuestados que se encuentran indecisos con respecto su respuesta.

5.2.14. Ante la pregunta ¿Está usted de acuerdo que poseer una adecuada infraestructura tecnológica es necesario para el funcionamiento y soporte de los sistemas de información de la compañía?

Tabla 23: Infraestructura tecnológica

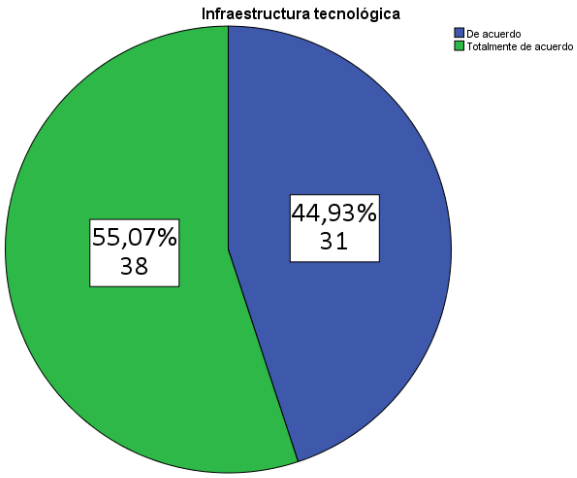
Infraestructura tecnológica

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	De acuerdo	31	44,9	44,9	44,9
	Totalmente de acuerdo	38	55,1	55,1	100,0
	Total	69	100,0	100,0	

Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

Figura 18: Infraestructura tecnológica



Fuente: Encuesta realizada a especialistas en el área de Information Technology.

Elaboración propia.

Con relación a la tabla 23 y figura 18, se reunió las siguientes respuestas de los especialistas encuestados, el 55.07% se encuentran totalmente de acuerdo con que poseer una adecuada infraestructura tecnológica es necesario para el funcionamiento

y soporte de los sistemas de información de la compañía, el 44.93% de los encuestados se encuentra de acuerdo con dicha premisa.

Considerando las respuestas recolectadas en la encuesta se puede deducir que el contar con una adecuada infraestructura tecnológica es necesario para el funcionamiento y soporte de los sistemas de información en la compañía, esto se debe a que en la actualidad los hackers tienen más a la mano todo tipo de sistemas malignos, y si la infraestructura tecnológica de la empresa no es del todo segura será muy sencillo introducirse en dichos sistemas y sacar información o dinero, produciendo así perjuicios en la compañía.

5.3. Contrastación de Hipótesis

En la presente tesis titulada : “La auditoría interna y su incidencia en el fraude informático en la banca digital en Lima Metropolitana en el año 2022”, para realizar la evaluación y contrastación las hipótesis propuestas en nuestra investigación, se aplicó la distribución de Chi Cuadrado de Pearson por medio del programa estadístico SPSS versión 25, consideramos que la herramienta Chi Cuadrado es el mejor método para evaluar cada una de las teorías de nuestro trabajo de investigación, para esta evaluación se utilizarán los resultados obtenidos en la encuesta, en la que en cada una de las preguntas se propusieron 5 opciones a elegir ordenadas de forma jerárquica y ascendente, las cuales van desde el totalmente en desacuerdo hasta el totalmente de acuerdo.

En nuestra investigación, se efectuó el procedimiento general de una prueba de hipótesis y se optó por utilizar el método tradicional, en donde se realizó una comparativa del valor de la probabilidad(**p**) y el valor de la significancia **α = 0,05.**

En donde la hipótesis nula se verá reflejada como H0 y la hipótesis alternativa es H1 la cual afirma que si existe asociación de dependencia entre variables.

5.3.1 Hipótesis específica(a)

Paso 1: Planteamos la hipótesis nula y su alternativa

Hipótesis nula (H_0)

El control interno **no** incide en la disminución de la malversación de fondos en la banca digital.

Hipótesis alternante (H_1)

El control interno **si** incide en la disminución de la malversación de fondos en la banca digital.

Paso 2: Elegimos el nivel de significancia α **= 0.05** y el estadístico de prueba Chi Cuadrado:

$$\chi^2_{(calculado)} = \sum_{i=1}^{r}\sum_{j=1}^{c}\frac{(o_{ij} - e_{ij})^2}{e_{ij}}$$

Donde:

o_{ij} = Es el valor observado de la fila “i” y la columna “j”.

e_{ij} = Es el valor esperado de la fila “i” y la columna “j”.

r= 5 número de filas.

c= 5 número de columnas en la Tabla de contingencia.

En la presente tesis, se ha determinado que la tabla cruzada se conformara por las opciones de respuestas de dos indicadores, la cual contara con la composición de 5 filas y 5 columnas, formando así 25 celdas en total, de igual forma tenemos que considerar que un indicador cuenta con 5 opciones de respuestas, las cuales se encuentran ordenadas de forma ascendente según su jerarquía y escala de Likert.

Paso 3: Cálculo del estadístico de prueba Chi Cuadrado calculado.

Los datos planteados en la tabla 22 hacen referencia a los resultados de la encuesta realizada, la cual tiene una muestra de 69 trabajadores enfocados en el rubro de bancas digitales, información que sera utilizada con el fin de elaborar las pruebas de hipótesis planteadas.

Tabla 24: Control interno y la malversación de fondos-Valores Observados

Control Interno (X1)	**Malversación de fondos (Y1)**					**Total**
	Totalmente en desacuerdo	**En desacuerdo**	**Indeciso**	**De acuerdo**	**Totalmente de acuerdo**	
Totalmente en desacuerdo	0	0	0	0	0	**0**
En desacuerdo	0	0	0	0	0	**0**
Indeciso	0	0	0	0	0	**0**
De acuerdo	0	0	2	34	15	**51**

Totalmente de acuerdo	0	0	0	9	9	**18**
Total	**0**	**0**	**2**	**43**	**24**	**69**

Fuente: Encuestados del área de auditoría interna, controles y TI.

En la Tabla 24 se observa que 18 personas se encuentran totalmente de acuerdo con que el control interno incide en la disminución de la malversación de fondos en la banca digital. De igual manera, 51 personas se encuentran de acuerdo con lo afirmado.

Es importante establecer una métrica que determine la intensidad de la relación existente entre variables e indicadores a la hora de calcular el valor de Chi Cuadrado de Pearson.

Es por esto que se procederá a desaparecer la fila y columna que no cuente con una respuesta en la Tabla 24, por lo que se excluyen del cálculo, ya que no hay nada que evaluar, esto reduce la tabla y se forma una distribución de Chi Cuadrado con 2 grados de libertad, ya que (2-1) *(3-1) = 2, y un nivel de significancia de α=0.05. Tomando en cuenta que el grado de libertad resultó 2, se consultó en la Tabla de Chi Cuadrado su valor teórico, el cual asciende a $\chi^2_{(2,0.05)} = 5.99$

Una vez haber indagado en la tabla del Anexo 3 acerca del valor teórico de Chi Cuadrado, se estableció el valor calculado de Chi Cuadrado. En esta etapa se tiene que considerar los resultados de la Tabla 24, y en base a estos datos se calculó los valores esperados, creando de esta manera una segunda tabla, en donde se muestra el recuento esperado aplicando la fórmula a continuación:

$$e_1 = \frac{51 \times 2}{69} = 1.48 \quad e_2 = \frac{51 \times 43}{69} = 31.78 \ldots e_6 = \frac{18 \times 24}{69} = 6.26$$

Tabla 25: Control interno y la malversación de fondos-Valores esperados

Control Interno (X1)	Malversación de fondos (Y1)					Total
	Totalmente en desacuerdo	En desacuerdo	Indeciso	De acuerdo	Totalmente de acuerdo	
Totalmente en desacuerdo	0	0	0	0	0	**0**
En desacuerdo	0	0	0	0	0	**0**
Indeciso	0	0	0	0	0	**0**
De acuerdo	0	0	1.5	31.8	17.7	**51**
Totalmente de acuerdo	0	0	0.5	11.2	6.3	**18**
Total	**0**	**0**	**2**	**43**	**24**	**69**

FUENTE: Encuestados del área de auditoría interna, controles y TI.

Una vez habiendo recaudado los valores observados y esperados, se tiene que calcular la fórmula para determinar el Chi Cuadrado calculado para finalizar contrastando la hipótesis.

Se utilizará el software SPSS versión 25 para constatar el cálculo de los datos, con esto se podrá definir la autenticidad de los datos y acelerar el proceso, de esta forma se puede obtener estos resultados:

Tabla 26. Resumen de procesamiento de casos de la hipótesis secundaria (a)

Resumen de procesamiento de casos

	Casos					
	Válido		Perdido		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
CONTROL INTERNO * MALVERSACION DE FONDOS	69	100,0%	0	0,0%	69	100,0%

Fuente: Programa SPSS versión 25

Procesamiento utilizando SPSS

Tabla 27: Tabla cruzada de la hipótesis secundaria (a)

Control interno (X1) vs Malversación de fondos (Y1)

Tabla cruzada CONTROL INTERNO*MALVERSACION DE FONDOS

			MALVERSACION DE FONDOS			
			TOTALMENTE DE ACUERDO	DE ACUERDO	INDECISO	Total
CONTROL INTERNO	TOTALMENTE DE ACUERDO	Recuento	9	9	0	18
		Recuento esperado	6,3	11,2	,5	18,0
	DE ACUERDO	Recuento	15	34	2	51
		Recuento esperado	17,7	31,8	1,5	51,0
Total		Recuento	24	43	2	69
		Recuento esperado	24,0	43,0	2,0	69,0

Tabla 28: Pruebas de Chi Cuadrado – Hipótesis específica(a)

Pruebas de Chi Cuadrado

	Valor	df	Significación asintótica (bilateral)
Chi Cuadrado de Pearson	2,920[a]	2	,232
Razón de verosimilitud	3,331	2	,189
Asociación lineal por lineal	2,863	1	,091
N de casos válidos	69		

a. 2 casillas (33,3%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,52.

Fuente: Programa SPSS versión 25

Procesamiento utilizando SPSS

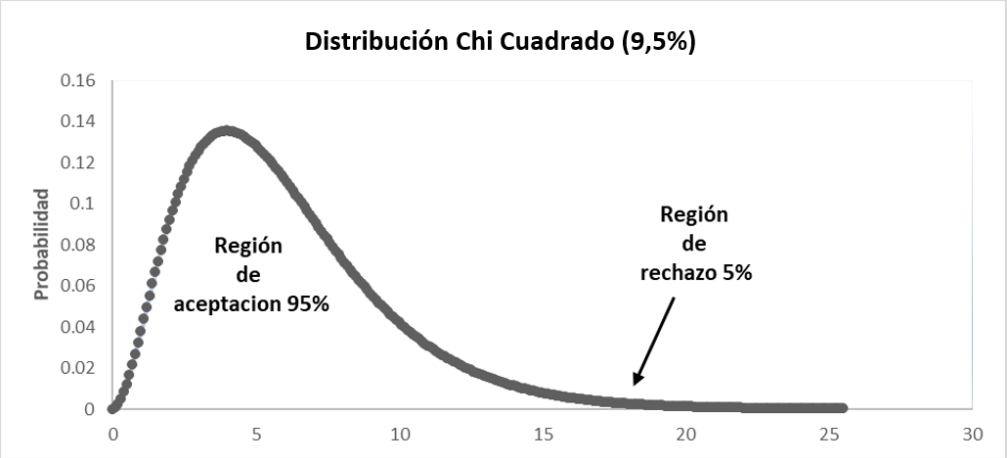
Paso 4. Decisión

Una vez realizado los cálculos necesarios, se concluyó que el valor teórico de Chi Cuadrado es inferior al valor calculado de Chi Cuadrado. Esto significa que se aceptará la hipótesis alternativa y se rechaza la nula. Se obtuvo los siguientes resultados:

$$\chi^2_{(calculado)} = 2{,}920 > \chi^2_{(2,0.05)} = 5.99$$

Esto significa que el valor calculado se ubica en la zona de rechazo.

Figura 19: Distribución Chi Cuadrado de Hipótesis secundaria (a)



Chi teórico = **5.99** Chi calculado = **2,920**

Elaboración propia extraída del SPSS

Paso 5. Conclusión e interpretación

En conclusión, si la hipótesis nula es falsa, entonces la hipótesis alternativa es verdadera, es decir, hay evidencia suficiente que apoya y sustenta que el control interno genera un grado de incidencia en relación a la disminución de malversación

de fondos en la banca digital, esto se debe a que el mantener ciertos lineamientos constantemente monitoreados mitiga en gran parte el nivel de fraude o en este caso las malversaciones de fondos.

5.3.2. Hipótesis específica(b)

Paso 1: Planteamos la hipótesis nula y su alternativa

Hipótesis nula (H_0)

El cumplimiento de las normas de auditoría y de información financiera (NIAS) **no** incide en la Gestión de riesgo de fraude en la banca digital.

Hipótesis alternante (H_1)

El cumplimiento de las normas de auditoría y de información financiera (NIAS) si incide en la Gestión de riesgo de fraude en la banca digital.

Paso 2: Elegimos el nivel de significancia α **= 0.05** y el estadístico de prueba Chi Cuadrado:

$$\chi^2_{(calculado)} = \sum_{i=1}^{r}\sum_{j=1}^{c}\frac{(o_{ij} - e_{ij})^2}{e_{ij}}$$

Donde:

o_{ij} = Es el valor observado de la fila “i” y la columna “j”

e_{ij} = Es el valor esperado de la fila “i” y la columna “j”

r= 5 número de filas

c= 5 número de columnas en la Tabla de contingencia.

En la presente tesis, se ha determinado que la tabla cruzada se conformara por las opciones de respuestas de dos indicadores, la cual contara con la composición de 5 filas y 5 columnas, formando así 25 celdas en total, de igual forma tenemos que considerar que un indicador cuenta con 5 opciones de respuestas, las cuales se encuentran ordenadas de forma ascendente según su jerarquía y escala de Likert.

Paso 3: Cálculo del estadístico de prueba Chi Cuadrado calculado.

Los datos planteados en la tabla 27 hacen referencia a los resultados de la encuesta realizada, la cual tiene una muestra de 69 trabajadores enfocados en el rubro de bancas digitales, información que sera utilizada con el fin de elaborar las pruebas de hipótesis planteadas.

Tabla 29: Cumplimiento de las NIAS y la Gestión del riesgo de fraude– Valores observados

Cumplimento de las NIAS (X2)	**Gestión del riesgo de fraude (Y2)**					**Total**
	Totalmente en desacuerdo	**En desacuerdo**	**Indeciso**	**De acuerdo**	**Totalmente de acuerdo**	
Totalmente en desacuerdo	0	0	0	0	0	**0**
En desacuerdo	0	0	0	0	0	**0**
Indeciso	0	0	1	2	2	**5**
De acuerdo	0	0	1	30	13	**44**
Totalmente de acuerdo	0	0	0	13	7	**20**

Total	**0**	**0**	**2**	**45**	**22**	**69**

Fuente: Encuestados del área de auditoría interna, controles y TI.

En la Tabla 29 se observa que 20 personas se encuentran totalmente de acuerdo con el cumplimiento de las normas de auditoría y de información financiera (NIAS) incide en la Gestión de riesgo de fraude en la banca digital. De igual manera, 44 personas se encuentran de acuerdo con lo afirmado. Mientras que, 5 personas se muestran indecisas al respecto.

Es importante establecer una métrica que determine la intensidad de la relación existente entre variables e indicadores a la hora de calcular el valor de Chi Cuadrado de Pearson.

Es por esto que se procederá a desaparecer la fila y columna que no cuente con una respuesta en la Tabla 29, por lo que se excluyen del cálculo, ya que no hay nada que evaluar, esto reduce la tabla y se forma una distribución de Chi Cuadrado con 4 grados de libertad, ya que (3-1) *(3-1) = 4, y un nivel de significancia de α=0.05. Tomando en cuenta que el grado de libertad resultó 4, se consultó en la Tabla de Chi Cuadrado su valor teórico, el cual asciende a $\chi^2_{(4,0.05)} = 9.49$

Una vez haber indagado en la tabla del Anexo 3 acerca del valor teórico de Chi Cuadrado, se estableció el valor calculado de Chi Cuadrado. En esta etapa se tiene que considerar los resultados de la Tabla 29, y en base a estos datos se calculó los valores esperados, creando de esta manera una segunda tabla, en donde se muestra el recuento esperado aplicando la fórmula a continuación:

$$e_1 = \frac{5\times2}{69} = 0.15 \quad e_2 = \frac{5\times45}{69} = 3.26 \ldots e_9 = \frac{20\times22}{69} = 6.38$$

Tabla 30: Cumplimiento de las NIAS y la Gestión del riesgo de fraude-Valores esperados

Cumplimiento de las NIAS (X2)	Gestión del riesgo de fraude (Y2)					Total
	Totalmente en desacuerdo	En desacuerdo	Indeciso	De acuerdo	Totalmente de acuerdo	
Totalmente en desacuerdo	0	0	0	0	0	**0**
En desacuerdo	0	0	0	0	0	**0**
Indeciso	0	0	0.1	3.3	1.6	**5**
De acuerdo	0	0	1.3	28.7	14	**44**
Totalmente de acuerdo	0	0	0.6	13	6.4	**20**
Total	**0**	**0**	**2**	**45**	**22**	**69**

Fuente: Encuestados del área de auditoría interna, controles y TI.

Una vez habiendo recaudado los valores observados y esperados, se tiene que calcular la fórmula para determinar el Chi Cuadrado calculado para finalizar contrastando la hipótesis.

$$\chi^2_{(calculado)} = \sum_{i=1}^{4}\sum_{j=1}^{4}\frac{(o_{ij}-e_{ij})^2}{e_{ij}} = \frac{(1-0.1)^2}{0.1} + \frac{(1-3.3)^2}{3.3} + \ldots + \frac{(7-6.4)^2}{6.4} = \mathbf{6.471}$$

Se utilizará el software SPSS versión 25 para constatar el cálculo de los datos, con esto se podrá definir la autenticidad de los datos y acelerar el proceso, de esta forma se puede obtener estos resultados:

Tabla 31: Resumen de procesamiento de casos de la Hipótesis secundaria (b)

Resumen de procesamiento de casos

	Casos					
	Válido		Perdido		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
CUMPLIMIENTO DE LAS NIAS * GESTION DE RIESGO DE FRAUDE	69	100,0%	0	0,0%	69	100,0%

FUENTE: Programa SPSS versión 25

Procesamiento utilizando SPSS

Tabla 32: Tabla Cruzada de la Hipótesis secundaria (b)

Cumplimiento de las NIAS (X2) vs Gestión de riesgo de fraude (Y2)

Tabla cruzada CUMPLIMIENTO DE LAS NIAS*GESTION DE RIESGO DE FRAUDE

			GESTION DE RIESGO DE FRAUDE			
			TOTALMENTE DE ACUERDO	DE ACUERDO	INDECISO	Total
CUMPLIMIENTO DE LAS NIAS	TOTALMENTE DE ACUERDO	Recuento	7	13	0	20
		Recuento esperado	6,4	13,0	,6	20,0
	DE ACUERDO	Recuento	13	30	1	44
		Recuento esperado	14,0	28,7	1,3	44,0
	INDECISO	Recuento	2	2	1	5
		Recuento esperado	1,6	3,3	,1	5,0
Total		Recuento	22	45	2	69
		Recuento esperado	22,0	45,0	2,0	69,0

Tabla 33: Pruebas de Chi Cuadrado – Hipótesis específica (b)

Pruebas de Chi Cuadrado

	Valor	df	Significación asintótica (bilateral)
Chi Cuadrado de Pearson	6,471[a]	4	,167
Razón de verosimilitud	4,233	4	,375
Asociación lineal por lineal	,469	1	,493
N de casos válidos	69		

a. 5 casillas (55,6%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,14.

Fuente: Programa SPSS versión 25

Procesamiento utilizando SPSS

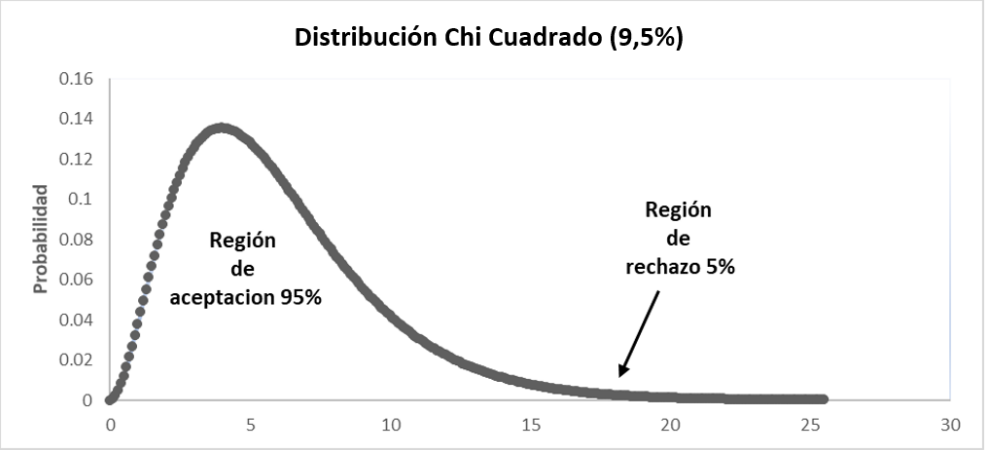
Paso 4. Decisión

Una vez realizado los cálculos necesarios, se concluyó que el valor teórico de Chi Cuadrado es inferior al valor calculado de Chi Cuadrado. Esto significa que se aceptará la hipótesis alternativa y se rechaza la nula. Se obtuvo los siguientes resultados:

$$\chi^2_{(calculado)} = 6.471 > \chi^2_{(4,0.05)} = 9.49$$

Esto significa que el valor calculado se ubica en la zona de rechazo.

Figura 20: Distribución Chi Cuadrado de Hipótesis secundaria (b)



Chi teórico = **9.49** Chi calculado = **6.471**

Elaboración propia extraída del SPSS

Paso 5. Conclusión e interpretación

En conclusión, si la hipótesis nula es falsa, entonces la hipótesis alternativa es verdadera, es decir, existe sustento y evidencia que indica que el cumplimiento de las normas de auditoría y de información (NIAS), incide en la gestión de riesgo de fraude en la banca digital, esto se debe a que estas normas brindan ciertos parámetros, los cuales se encargan de controlar y establecer criterios concretos, de esta manera es mucho más difícil que pueda existir un alto índice de fraude.

5.3.3. Hipótesis específica(c)

Paso 1: Planteamos la hipótesis nula y su alternativa

Hipótesis nula (H_0)

La vulneración de controles por parte de la Gerencia **no** incide en la aplicación de la ciberseguridad en las empresas en la banca digital.

Hipótesis alternante (H_1)

La vulneración de controles por parte de la Gerencia sí incide en la aplicación de la ciberseguridad en las empresas en la banca digital.

Paso 2: Elegimos el nivel de significancia α **= 0.05** y el estadístico de prueba Chi Cuadrado:

$$\chi^2_{(calculado)} = \sum_{i=1}^{r}\sum_{j=1}^{c}\frac{(o_{ij} - e_{ij})^2}{e_{ij}}$$

Donde:

o_{ij} = Es el valor observado de la fila “i” y la columna “j”

e_{ij} = Es el valor esperado de la fila “i” y la columna “j”

r= 5 número de filas

c = 5 número de columnas en la Tabla de contingencia.

En la presente tesis, se ha determinado que la tabla cruzada se conformara por las opciones de respuestas de dos indicadores, la cual contara con la composición de 5 filas y 5 columnas, formando así 25 celdas en total, de igual forma tenemos que considerar que un indicador cuenta con 5 opciones de respuestas, las cuales se encuentran ordenadas de forma ascendente según su jerarquía y escala de Likert.

Paso 3: Cálculo del estadístico de prueba Chi Cuadrado calculado.

Los datos planteados en la tabla 32 hacen referencia a los resultados de la encuesta realizada, la cual tiene una muestra de 69 trabajadores enfocados en el rubro de

bancas digitales, información que sera utilizada con el fin de elaborar las pruebas de hipótesis planteadas.

Tabla 34: Vulneración de Controles y la aplicación de la Ciberseguridad– Valores observados

Vulneración de Controles (X3)	Aplicación de la Ciberseguridad (Y3)					Total
	Totalmente en desacuerdo	En desacuerdo	Indeciso	De acuerdo	Totalmente de acuerdo	
Totalmente en desacuerdo	0	0	0	0	0	**0**
En desacuerdo	0	0	0	0	0	**0**
Indeciso	0	0	0	2	0	**2**
De acuerdo	0	0	0	25	19	**44**
Totalmente de acuerdo	0	0	0	11	12	**23**
Total	**0**	**0**	**0**	**38**	**31**	**69**

Fuente: Encuestados del área de auditoría interna, controles y TI.

En la Tabla 34 se observa que 23 personas se encuentran totalmente de acuerdo con que la vulneración de controles por parte de la Gerencia incide en la aplicación de la ciberseguridad en las empresas en la banca digital. De igual manera, 44 personas se encuentran de acuerdo con lo afirmado. Mientras que, 2 personas se muestran indecisas al respecto.

Es importante establecer una métrica que determine la intensidad de la relación existente entre variables e indicadores a la hora de calcular el valor de Chi Cuadrado de Pearson.

Es por esto que se procederá a desaparecer la fila y columna que no cuente con una respuesta en la Tabla 34, por lo que se excluyen del cálculo, ya que no hay nada que evaluar, esto reduce la tabla y se forma una distribución de Chi Cuadrado con 2 grados de libertad, ya que (3-1) *(2-1) = 2, y un nivel de significancia de α=0.05. Tomando en cuenta que el grado de libertad resultó 2, se consultó en la Tabla de Chi Cuadrado su valor $\chi^2_{(2,0.05)} = 5.99$ teórico, el cual asciende a

Una vez haber indagado en la tabla del Anexo 3 acerca del valor teórico de Chi Cuadrado, se estableció el valor calculado de Chi Cuadrado. En esta etapa se tiene que considerar los resultados de la Tabla 34, y en base a estos datos se calculó los valores esperados, creando de esta manera una segunda tabla, en donde se muestra el recuento esperado aplicando la fórmula a continuación:

$$e_1 = \frac{2\times38}{69} = 1.10 \quad e_2 = \frac{2\times31}{69} = 0.90 \ldots e_6 = \frac{23\times31}{69} = 10.33$$

Tabla 35: Vulneración de Controles y la aplicación de la Ciberseguridad- Valores esperados

Vulneración de Controles (X3)	Aplicación de la Ciberseguridad (Y3)					Total
	Totalmente en desacuerdo	En desacuerdo	Indeciso	De acuerdo	Totalmente de acuerdo	
Totalmente en desacuerdo	0	0	0	0	0	**0**

En desacuerdo	0	0	0	0	0	**0**
Indeciso	0	0	0	1.1	0.9	**2**
De acuerdo	0	0	0	24.2	19.8	**44**
Totalmente de acuerdo	0	0	0	12.7	10.3	**23**
Total	**0**	**0**	**0**	**38**	**31**	**69**

Fuente: Encuestados del área de auditoría interna, controles y TI.

Una vez habiendo recaudado los valores observados y esperados, se tiene que calcular la fórmula para determinar el Chi Cuadrado calculado para finalizar contrastando la hipótesis.:

$$\chi^2_{(calculado)} = \sum_{i=1}^{4}\sum_{j=1}^{4}\frac{(o_{ij}-e_{ij})^2}{e_{ij}} = \frac{(2-1.1)^2}{1.1} + \frac{(0-0.9)^2}{0.9} + \ldots + \frac{(12-10.3)^2}{10.3} = \mathbf{2.174}$$

Se utilizará el software SPSS versión 25 para constatar el cálculo de los datos, con esto se podrá definir la autenticidad de los datos y acelerar el proceso, de esta forma se puede obtener estos resultados:

Tabla 36: Resumen de procesamiento de casos de la Hipótesis secundaria (c)

Resumen de procesamiento de casos

	Casos					
	Válido		Perdido		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
VULNERACION DE CONTROLES POR PARTE DE LA GERENCIA * APLICACION DE LA CIBERSEGURIDAD EN LAS EMPRESAS DE BANCA DIGITAL	69	100,0%	0	0,0%	69	100,0%

Fuente: Programa SPSS versión 25

Procesamiento utilizando SPSS

Tabla 37: Tabla Cruzada de la Hipótesis secundaria (c)

Vulneración de Controles por parte de la Gerencia (X3) vs Aplicación de la Ciberseguridad (Y3)

Tabla cruzada VULNERACION DE CONTROLES POR PARTE DE LA GERENCIA*APLICACION DE LA CIBERSEGURIDAD EN LAS EMPRESAS DE BANCA DIGITAL

			APLICACION DE LA CIBERSEGURIDAD EN LAS EMPRESAS DE BANCA DIGITAL		
			TOTALMENTE DE ACUERDO	DE ACUERDO	Total
VULNERACION DE CONTROLES POR PARTE DE LA GERENCIA	TOTALMENTE DE ACUERDO	Recuento	12	11	23
		Recuento esperado	10,3	12,7	23,0
	DE ACUERDO	Recuento	19	25	44
		Recuento esperado	19,8	24,2	44,0
	INDECISO	Recuento	0	2	2
		Recuento esperado	,9	1,1	2,0
Total		Recuento	31	38	69
		Recuento esperado	31,0	38,0	69,0

Fuente: Programa SPSS versión 25

Tabla 38: Pruebas de Chi Cuadrado – Hipótesis específica (c)

Pruebas de Chi Cuadrado

	Valor	df	Significación asintótica (bilateral)
Chi Cuadrado de Pearson	2,174[a]	2	,337
Razón de verosimilitud	2,925	2	,232
Asociación lineal por lineal	1,408	1	,235
N de casos válidos	69		

a. 2 casillas (33,3%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,90.

Fuente: Programa SPSS versión 25

Procesamiento utilizando SPSS

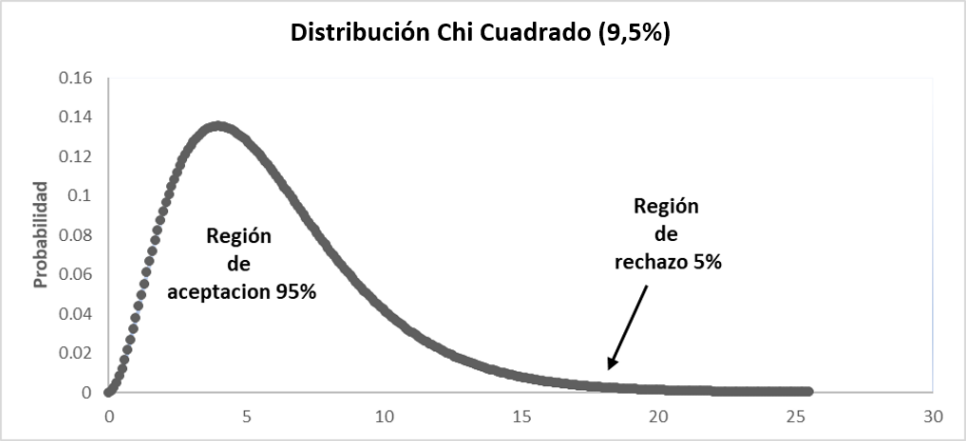
Paso 4. Decisión

Una vez realizado los cálculos necesarios, se concluyó que el valor teórico de Chi Cuadrado es inferior al valor calculado de Chi Cuadrado. Esto significa que se aceptará la hipótesis alternativa y se rechaza la nula. Se obtuvo los siguientes resultados:

$$\chi^2_{(calculado)} = 2.174 > \chi^2_{(2,0.05)} = 5.99$$

Esto significa que el valor calculado se ubica en la zona de rechazo.

Figura 21. Distribución Chi Cuadrado de Hipótesis secundaria (c)



Chi teórico = **5.99** Chi calculado = **2.174**

Elaboración propia extraída del SPSS

Paso 5. Conclusión e interpretación

En conclusión, si la hipótesis nula es falsa, entonces la hipótesis alternativa es verdadera, es decir, existe sustento y evidencia que indica que la vulneración de controles por parte de la gerencia incide en la aplicación de la ciberseguridad en las empresas en la banca digital, esto se debe a que las empresas en la actualidad buscan

protegerse de todos los riesgos que pueda, ya sean externos o internos, esto incluye a los altos mandos de la organización.

5.3.4. Hipótesis General

Paso 1: Planteamos la hipótesis nula y su alternativa

Hipótesis nula (H_0)

La auditoría interna **no** incide favorablemente en la detección del fraude informático en sector banca digital en Lima Metropolitana, año 2022.

Hipótesis alternante (H_1)

La auditoría interna **si** incide favorablemente en la detección del fraude informático en sector banca digital en Lima Metropolitana, año 2022

Paso 2: Elegimos el nivel de significancia α **= 0.05** y el estadístico de prueba Chi Cuadrado:

$$\chi^2_{(calculado)} = \sum_{i=1}^{r}\sum_{j=1}^{c}\frac{(o_{ij} - e_{ij})^2}{e_{ij}}$$

Donde:

o_{ij} = Es el valor observado de la fila “i” y la columna “j”

e_{ij} = Es el valor esperado de la fila “i” y la columna “j”

r= 5 número de filas

c= 5 número de columnas en la Tabla de contingencia.

En la presente tesis, se ha determinado que la tabla cruzada se conformara por las opciones de respuestas de dos indicadores, la cual contara con la composición de 5 filas y 5 columnas, formando así 25 celdas en total, de igual forma tenemos que considerar que un indicador cuenta con 5 opciones de respuestas, las cuales se encuentran ordenadas de forma ascendente según su jerarquía y escala de Likert.

Paso 3: Cálculo del estadístico de prueba Chi Cuadrado calculado.

Los datos planteados en la tabla 39 hacen referencia a los resultados de la encuesta realizada, la cual tiene una muestra de 69 trabajadores enfocados en el rubro de bancas digitales, información que será utilizada con el fin de elaborar las pruebas de hipótesis planteadas.

Tabla 39: La auditoría interna y el fraude cibernético – valores observados

La auditoría interna (X)	Fraude Cibernético (Y)					Total
	Totalmente en desacuerdo	En desacuerdo	Indeciso	De acuerdo	Totalmente de acuerdo	
Totalmente en desacuerdo	0	0	0	0	0	**0**
En desacuerdo	0	0	0	0	0	**0**
Indeciso	0	0	0	0	0	**0**
De acuerdo	0	0	0	9	0	**9**
Totalmente de acuerdo	0	0	0	23	37	**60**

Total	**0**	**0**	**0**	**32**	**37**	**69**

Fuente: Encuestados del área de auditoría interna, controles y TI.

En la Tabla 39 se observa que 60 personas se encuentran totalmente de acuerdo con que la auditoría interna incide favorablemente en la detección del fraude informático en sector banca digital en Lima Metropolitana, año 2022.La auditoría interna si incide favorablemente en la detección del fraude informático en sector banca digital en Lima Metropolitana, año 2022. De igual manera, 9 personas se encuentran de acuerdo con lo afirmado.

Es importante establecer una métrica que determine la intensidad de la relación existente entre variables e indicadores a la hora de calcular el valor de Chi Cuadrado de Pearson.

Es por esto que se procederá a desaparecer la fila y columna que no cuente con una respuesta en la Tabla 39, por lo que se excluyen del cálculo, ya que no hay nada que evaluar, esto reduce la tabla y se forma una distribución de Chi Cuadrado con 1 grados de libertad, ya que (2-1) *(2-1) = 1, y un nivel de significancia de α=0.05. Tomando en cuenta que el grado de libertad resultó 1, se consultó en la Tabla de Chi Cuadrado su valor teórico, el cual asciende a $\chi^2_{(1,0.05)} = 3.84$

Una vez haber indagado en la tabla del Anexo 3 acerca del valor teórico de Chi Cuadrado, se estableció el valor calculado de Chi Cuadrado. En esta etapa se tiene que considerar los resultados de la Tabla 39, y en base a estos datos se calculó los valores esperados, creando de esta manera una segunda tabla, en donde se muestra el recuento esperado aplicando la fórmula a continuación:

$$e_1 = \frac{9\times32}{69} = 4.17 \quad e_2 = \frac{9\times37}{69} = 4.83\ldots\ e_4 = \frac{60\times37}{69} = 32.17$$

Tabla 40: La auditoría interna y el fraude cibernético-Valores esperados

La Auditoría interna (X)	Fraude Cibernético (Y)					Total
	Totalmente en desacuerdo	En desacuerdo	Indeciso	De acuerdo	Totalmente de acuerdo	
Totalmente en desacuerdo	0	0	0	0	0	**0**
En desacuerdo	0	0	0	0	0	**0**
Indeciso	0	0	0	0	0	**0**
De acuerdo	0	0	0	4.2	4.8	**9**
Totalmente de acuerdo	0	0	0	27.8	32.2	**60**
Total	**0**	**0**	**0**	**32**	**37**	**69**

Fuente: Encuestados del área de auditoría interna, controles y TI.

Una vez habiendo recaudado los valores observados y esperados, se tiene que calcular la fórmula para determinar el Chi Cuadrado calculado para finalizar contrastando la hipótesis.:

$$\chi^2_{(calculado)} = \sum_{i=1}^{4}\sum_{j=1}^{4}\frac{(o_{ij}-e_{ij})^2}{e_{ij}} = \frac{(9-4.2)^2}{4.2} + \frac{(0-4.8)^2}{4.8} + \ldots + \frac{(37-32.2)}{32.2} = \mathbf{11.967}$$

Se utilizará el software SPSS versión 25 para constatar el cálculo de los datos, con esto se podrá definir la autenticidad de los datos y acelerar el proceso, de esta forma se puede obtener estos resultados:

Tabla 41. Resumen de procesamiento de casos de la Hipótesis General

Resumen de procesamiento de casos

	Casos					
	Válido		Perdido		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
AUDITORIA INTERNA * FRAUDE INFORMATICO	69	100,0%	0	0,0%	69	100,0%

Fuente: Programa SPSS versión 25

Procesamiento utilizando SPSS

Tabla 42: Tabla Cruzada de la Hipótesis General

Auditoría Interna (X) vs Fraude Informático (Y)

Tabla cruzada AUDITORIA INTERNA*FRAUDE INFORMATICO

			FRAUDE INFORMATICO		
			TOTALMENTE DE ACUERDO	DE ACUERDO	Total
AUDITORIA INTERNA	TOTALMENTE DE ACUERDO	Recuento	37	23	60
		Recuento esperado	32,2	27,8	60,0
	DE ACUERDO	Recuento	0	9	9
		Recuento esperado	4,8	4,2	9,0
Total		Recuento	37	32	69
		Recuento esperado	37,0	32,0	69,0

Fuente: Programa SPSS versión 25

Tabla 43: Pruebas de Chi Cuadrado – Hipótesis General

Pruebas de Chi Cuadrado

	Valor	df	Significación asintótica (bilateral)	Significación exacta (bilateral)	Significación exacta (unilateral)
Chi Cuadrado de Pearson	11,967[a]	1	,001		
Corrección de continuidad[b]	9,616	1	,002		
Razón de verosimilitud	15,411	1	,000		
Prueba exacta de Fisher				,000	,000
Asociación lineal por lineal	11,794	1	,001		
N de casos válidos	69				

a. 2 casillas (50,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es 4,17.

b. Sólo se ha calculado para una tabla 2x2

Fuente: Programa SPSS versión 25

Procesamiento utilizando SPSS

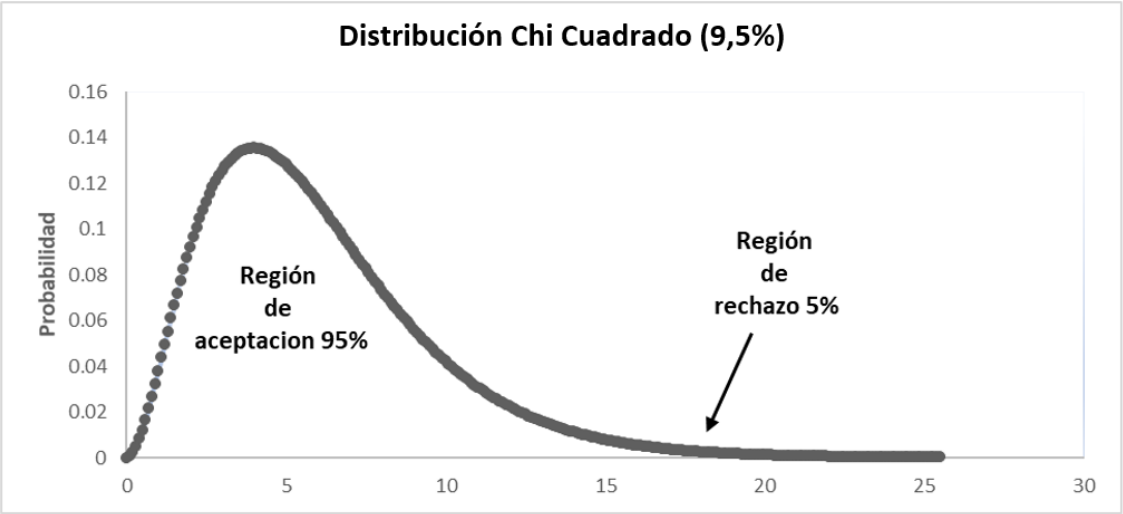
Paso 4. Decisión

Una vez realizado los cálculos necesarios, se concluyó que el valor teórico de Chi Cuadrado es inferior al valor calculado de Chi Cuadrado. Esto significa que se aceptará la hipótesis alternativa y se rechaza la nula. Se obtuvo los siguientes resultados:

$$\chi^2_{(calculado)} = 11.967 > \chi^2_{(1,0.05)} = 3.84$$

Esto significa que el valor calculado se ubica en la zona de rechazo.

Figura 21: Distribución Chi Cuadrado de Hipótesis General



Chi teórico = **3.84** Chi calculado = **11.967**

Elaboración propia extraída del SPSS

Paso 5. Conclusión e interpretación

En conclusión, si la hipótesis nula es falsa, entonces la hipótesis alternativa es verdadera, es decir, existe sustento y evidencia que indica que la auditoría interna incide favorablemente en la detección del fraude informático en sector banca digital en Lima Metropolitana, año 2022, esto significa que efectivamente el que una empresa lleve de manera constante la auditoría interna favorece a la disminución del fraude informático ya que esta brinda un mayor control y seguridad en los procesos de la empresa

CAPÍTULO VI: DISCUSIÓN, CONCLUSIONES Y RECOMENDACIONES

6.1. Discusión

Tras haber hecho uso de los instrumentos de recopilación de información adecuados dentro de la investigación **“LA AUDITORÍA INTERNA Y SU INCIDENCIA EN EL FRAUDE INFORMÁTICO EN LA BANCA DIGITAL EN LIMA METROPOLITANA EN EL AÑO 2022”** se pudieron identificar los siguientes hallazgos:

a. En resumen, los resultados de la encuesta respaldan la idea de la implementación de medidas específicas, como la creación de un área de auditoría interna especializada, el seguimiento de recomendaciones internas y la adaptación de normativas, son esenciales para fortalecer la seguridad y reducir el riesgo de fraude cibernético en el sector de banca digital en Lima Metropolitana. En relación con la tabla 11 y la figura 6, se observa que el 59.42% de los especialistas encuestados están de acuerdo en que tomar en

cuenta las recomendaciones de la auditoría interna beneficia a la seguridad electrónica de la empresa al detectar el fraude cibernético. Además, el 39.13% está totalmente de acuerdo, mientras que un pequeño porcentaje (1.45%) se muestra indeciso al respecto. Estos resultados sugieren que la mayoría de los encuestados perciben que considerar las recomendaciones de la auditoría interna es beneficioso para mejorar la seguridad electrónica y detectar el fraude cibernético en las empresas de banca digital.

Mengoa, V. (2021) resalta el aumento de la vulnerabilidad debido a la globalización y dependencia tecnológica, destaca la necesidad urgente de fortalecer los mecanismos de control para prevenir pérdidas económicas y reputacionales, ambas Fuentes destacan la importancia de controles internos sólidos y ética empresarial para combatir el fraude informático y corporativo. **De la Torre, M. (2018)** proporciona un antecedente importante al abordar la gestión del riesgo de fraude, ofreciendo una perspectiva adicional sobre cómo las empresas pueden enfrentar los desafíos de la ciberdelincuencia.

b. Los resultados de la encuesta destacan la necesidad imperante de fortalecer los mecanismos de control interno en empresas de banca digital. La implementación de controles informáticos previamente aprobados por la gerencia de Tecnología de la Información emerge como una estrategia crucial para asegurar la efectividad y eficiencia de los controles, adaptándose de manera específica a los diferentes tipos de riesgos a los que se enfrentan. Además, la preferencia significativa (53.62% totalmente de acuerdo y 40.58% de acuerdo) en basar la estrategia de auditoría interna en el cumplimiento de las Normas de Auditoría de Información Financiera (NIAS) en lugar de las

Normas de Información Financiera (NIIF) subraya la importancia de una orientación más centrada en la auditoría como práctica. Asimismo, la amplia aceptación (56.52% totalmente de acuerdo y 40.58% de acuerdo) de que las NIAS deben actualizarse en respuesta a los casos de fraude cibernético identificados en auditorías internas destaca la necesidad de mantener normativas actualizadas, utilizando los hallazgos como antecedentes para mejorar y reducir el riesgo de fraude en las empresas. Estos hallazgos respaldan la idea de que la adaptación constante y la especialización son fundamentales en la gestión efectiva de la ciberseguridad y la prevención del fraude en el entorno de la banca digital.

c. Los resultados de la encuesta revelan que la percepción de los especialistas sobre la vulneración de controles por parte de la gerencia se posiciona como el riesgo más significativo en una auditoría interna, con un notable 55.07% totalmente de acuerdo y un 43.48% de acuerdo. Esta conclusión sugiere que la alta jerarquía dentro de una organización puede generar un entorno propicio para la falta de verificación y cumplimiento de los controles establecidos. La escasez de supervisión debida a la presencia limitada de personal para verificar la implementación de controles es una preocupación destacada.

Además, los datos recopilados en la tabla 16 y la figura 11 refuerzan la necesidad de contar con personal externo especializado en controles informáticos en el área de Tecnología de la Información (TI). Con un 60.87% totalmente de acuerdo y un 36.23% de acuerdo, los encuestados respaldan la idea de incorporar especialistas externos para brindar un soporte neutral y evitar la vulneración de controles por parte de la gerencia. Este hallazgo sugiere que la inclusión de expertos externos puede proporcionar una perspectiva

imparcial y fortalecer los mecanismos de control, contribuyendo a la prevención de riesgos asociados con la manipulación interna de controles. En conjunto, estas conclusiones enfatizan la importancia de abordar la vulnerabilidad de controles desde diversas perspectivas, tanto desde la jerarquía interna como a través de la incorporación de especialistas externos en áreas críticas como la Tecnología de la Información.

d. La notable mayoría de especialistas, representada por un 60.87%, respalda la necesidad de que estas empresas cuenten con una matriz de riesgos diseñada específicamente para abordar casos de fraude informático. Esta conclusión subraya la relevancia de adaptar las estrategias de gestión de riesgos a la naturaleza digital de estas entidades, lo que podría contribuir significativamente a la reducción de los niveles de fraude. Asimismo, el 65.22% de los encuestados está totalmente de acuerdo en que la gestión eficiente de recursos tecnológicos es crucial para el adecuado desempeño de los equipos de Tecnología de la Información (TI). Este hallazgo destaca la importancia de contar con recursos tecnológicos actualizados para facilitar la identificación y prevención de posibles fraudes informáticos. En cuanto a la detección del fraude, la mayoría de los especialistas respalda la práctica de revisar regularmente los cambios en los patrones de gastos en la compañía. Esta estrategia se revela como una herramienta efectiva, ya que la detección de gastos inusuales o desproporcionados puede generar alertas tempranas y favorecer la identificación de posibles fraudes. En conjunto, estas conclusiones sugieren que la implementación de medidas específicas, como matrices de riesgos adaptadas, una gestión eficiente de recursos tecnológicos y la revisión constante de patrones de gastos, son importantes para fortalecer la

ciberseguridad y la detección de fraudes en el entorno de las empresas de banca digital.

e. Los resultados de la encuesta indican un respaldo significativo por parte de los especialistas hacia los programas de prevención de fraude, con un 55.07% totalmente de acuerdo y un 44.93% de acuerdo. Estos programas no solo proporcionan orientación y capacitación a los empleados, sino que también implementan controles efectivos, mitigando así los niveles de riesgo de fraude de manera considerable. Además, el 66.67% de los encuestados respalda la idea de que medir la eficiencia de los controles internos brinda soporte para definir los niveles de confianza en dichos controles, mientras que el 33.33% está de acuerdo. Este hallazgo sugiere que la constante revisión y evaluación de los controles internos son esenciales para mantener la eficacia en la gestión del riesgo. Estos resultados coinciden con la investigación de **Carbajal A. (2017)** en México, el cual revela la prevalencia de fraudes cibernéticos en empresas y destaca la importancia de medidas preventivas y éticas para mitigar los riesgos asociados con la digitalización. La presencia de trabajadores sin ética profesional se destaca como un factor común en los fraudes, subrayando la necesidad de enfoques integrales en la gestión del riesgo de fraude cibernético a nivel global.

f. Los resultados de la encuesta revelan un fuerte respaldo, con un 66.67% totalmente de acuerdo y un 33.33% de acuerdo, hacia la idea de que medir la eficiencia de los controles internos proporciona un nivel de confianza crucial en su funcionalidad. Esta conclusión sugiere que la constante revisión y evaluación de los controles internos son esenciales para mantener su eficacia y mitigar el riesgo en la compañía. Además, al considerar la tabla 22 y la figura

17, el 62.32% de los especialistas encuestados respalda la noción de que el departamento de TI puede mitigar las amenazas digitales cuando existe un alto nivel de ciberseguridad en la compañía. Estos hallazgos concuerdan con la preocupación expresada por **Gumucio J. (2021)** en su tesis sobre el fraude cibernético en entidades financieras. La gestión deficiente de la seguridad de la información podría resultar en pérdidas económicas y consecuencias legales, destacando la importancia de un enfoque seguro, transparente y responsable en el uso de herramientas y canales digitales para proteger la información de los clientes y mitigar los riesgos asociados al fraude cibernético.

g. Tras los resultados de la presente investigación podemos afirmar que con un 55.07% de totalmente de acuerdo y un 44.93% de acuerdo, hacia la idea de que poseer una adecuada infraestructura tecnológica es esencial para el funcionamiento y soporte de los sistemas de información de la compañía. Estos resultados subrayan la crítica importancia de contar con sistemas seguros frente a las crecientes amenazas cibernéticas. Además, la investigación de **Paiva, R. (2021)** destaca la relevancia de comprender los riesgos asociados a la digitalización en la banca, especialmente en términos de fraude electrónico. La interpretación de la Corte Suprema de Justicia respecto a la responsabilidad civil de las entidades bancarias en casos de fraude electrónico destaca la necesidad de examinar la responsabilidad del banco en eventos de fraude electrónico bajo los parámetros del régimen general de las obligaciones. Este enfoque, respaldado por la encuesta, subraya la importancia de políticas sólidas de ciberseguridad para garantizar el adecuado funcionamiento de los sistemas de seguridad implementados por las entidades pertinentes y prevenir pérdidas económicas y riesgos asociados al fraude cibernético.

6.2.1 Conclusiones

a. Se concluye que el control interno incide favorablemente en la disminución de la malversación de fondos en la banca digital puesto que el control interno establece un marco integral que aborda los riesgos financieros y operativos. La identificación temprana de anomalías a través de mecanismos de monitoreo continuo, la segregación de funciones para prevenir la colusión y la realización de auditorías internas y externas para evaluar la efectividad de los procedimientos financieros son componentes esenciales de este sistema. Además, las políticas y procedimientos claros establecidos por el control interno van a brindar pautas específicas para realizar transacciones, reduciendo así la posibilidad de apropiación indebida. Asimismo, la incorporación de tecnología avanzada y sistemas de monitoreo en tiempo real van a fortalecer aún más la capacidad de detectar patrones sospechosos. En un entorno en donde la banca digital se encuentra en constante cambio, la actualización continua de los controles internos será una garantía como una respuesta proactiva a nuevas amenazas, consolidando así su impacto positivo en la reducción de la malversación de fondos en una organización.

b. La exigencia del Cumplimiento de las normas de auditoría y de información financiera (NIAS) incide significativamente en la Gestión de riesgo de fraude en la banca digital ya que sirve para establecer un marco regulatorio que promueva la transparencia, la integridad y la rendición de cuentas. El cumplimiento de las normas de auditoría proporciona un mecanismo organizado para evaluar la eficacia de los controles internos y garantizar la exactitud de los informes financieros, al exigir a las bancas digitales que sigan estándares estrictos, se establece una base sólida para la detección temprana y la prevención de

actividades fraudulentas en entornos digitales. Bajo este contexto, el cumplimiento normativo de las normas de auditoría no sólo garantiza la confiabilidad de la información, sino también actúa como un componente esencial en la gestión de riesgos, reduciendo la probabilidad de fraude y mejorando la resiliencia de la banca digital ante posibles amenazas.

c. Se concluye que la vulneración de controles por parte de la Gerencia incide favorablemente en la aplicación de la ciberseguridad en la banca digital ya que la alta dirección desempeña un papel crucial en la definición de políticas, la asignación de recursos y el establecimiento de una cultura organizacional que priorice la ciberseguridad. Cuando la dirección ignora o debilita los controles establecidos, se reduce la capacidad de la organización para resistir y prevenir las amenazas cibernéticas. Las decisiones de gestión que minimizan la asignación de recursos adecuados o descuidan la actualización constante de las medidas de seguridad pueden dejar a la institución financiera vulnerable ante ataques sofisticados. En resumen, la vulneración de los controles por parte de la gerencia no solo debilita la seguridad interna, sino también compromete la capacidad de la banca digital para adaptarse y defenderse contra amenazas cibernéticas que se encuentran en una constante evolución.

La auditoría interna incide significativamente en la detección del fraude informático en la banca digital, esto debido a que a través de revisiones integrales y de auditorías periódicas, se evalúa la efectividad de los mecanismos de seguridad implementados para proteger la información importante y los activos digitales. La auditoría interna no sólo identifica vulnerabilidades potenciales en los sistemas, sino que también analiza transacciones y actividades en busca de patrones inusuales o comportamiento fraudulento. Al tener un conocimiento profundo de la infraestructura tecnológica y los

procesos operativos, la auditoría interna está bien posicionada para detectar anomalías que podrían indicar intentos de fraude informático. Además, la independencia de este departamento proporciona una perspectiva imparcial y objetiva, fortaleciendo la confianza en la integridad de los informes de auditoría. En última instancia, la auditoría interna no sólo contribuye a la identificación temprana de las ciberamenazas, sino que también sugiere mejoras en los controles existentes, fortaleciendo así la postura de seguridad de la banca digital contra los riesgos de ciberfraude.

6.3. Recomendaciones

a. Las empresas de banca digital deben ser exigentes respecto a que el personal reciba la formación adecuada sobre las mejores prácticas de seguridad, incluida la creación de contraseñas seguras y la protección de la información personal. Esta formación debería resaltar la importancia de las contraseñas únicas y complejas, así como la necesidad de cambiarlas periódicamente. Además, se debe educar a los empleados sobre posibles tácticas de phishing, subrayando la importancia de la vigilancia constante y la verificación de la autenticidad de los correos electrónicos o comunicaciones sospechosas. La capacitación también debe incluir la identificación de intentos de fraude y proporcionar pautas claras sobre cómo reconocer y denunciar actividades fraudulentas. Al proveer de sólidos conocimientos de ciberseguridad a los empleados, las empresas de banca digital pueden construir una primera línea de defensa más sólida contra posibles amenazas, fortaleciendo así la integridad de sus sistemas y la confianza de los clientes en un entorno financiero cada vez más digitalizado.

b. Las empresas de banca digital deben adquirir la implementación de sistemas de monitoreo en tiempo real para salvaguardar la integridad y seguridad de las transacciones en el entorno de la banca digital. Estos sistemas van a permitir una vigilancia constante, identificando de forma proactiva patrones de actividad o transacciones inusuales que podrían indicar posibles intentos de fraude. Asimismo, mediante el uso de algoritmos avanzados y tecnologías de aprendizaje automático, estos sistemas son capaces de analizar grandes volúmenes de datos en tiempo real, detectando anomalías y comportamientos atípicos. La capacidad de responder instantáneamente a actividades sospechosas brinda a las instituciones financieras la oportunidad de tomar medidas preventivas inmediatas, ya sea mediante autenticación adicional, notificación al usuario o suspensión temporal de la transacción para una revisión adicional. De igual forma, se recomienda implementar los lineamientos establecidos por las NIAS para así obtener una mayor certeza de la efectividad de los controles y disminuir el riesgo de fraude.

c. Las empresas de banca digital deben limitar el acceso a los datos y sistemas únicamente a aquellos empleados que requieran dicha información para llevar a cabo sus responsabilidades específicas. Para lograrlo de manera efectiva, es recomendable establecer políticas de control de privilegios que aseguren que a los empleados se les asigne el nivel mínimo de acceso necesario para realizar sus tareas diarias. Al restringir los privilegios de acceso, se reduce significativamente el riesgo de exposición de datos confidenciales. Estas medidas no sólo salvaguardan la información confidencial de los clientes, sino que también minimizan la posibilidad de acceso malicioso. Además, la implementación de políticas de control de privilegios fomenta un entorno de

trabajo más seguro y transparente, al tiempo que refuerza la confianza tanto de los clientes como de los empleados en el manejo seguro de la información financiera en la era digital.

Las empresas de banca digital deben realizar auditorías periódicas a través de un examen exhaustivo de los sistemas, protocolos y procedimientos, las auditorías identifican posibles brechas de seguridad o vulnerabilidades que podrían comprometer la integridad del entorno digital. La detección temprana de cualquier debilidad ofrece la oportunidad de implementar medidas correctivas a tiempo, fortaleciendo así las defensas contra amenazas potenciales. Asimismo, la transparencia resultante de las auditorías no solo va a garantizar el cumplimiento de los estándares de seguridad, sino que también refuerza la confianza tanto de los clientes como de las partes interesadas en la capacidad de la institución para salvaguardar la información financiera en el cambiante panorama digital. En última instancia, estas evaluaciones periódicas son esenciales para mantener la resiliencia y confiabilidad de las operaciones en el espacio de la banca digital.

ANEXO Nº 01

Título: LA AUDITORÍA INTERNA Y SU INCIDENCIA EN EL FRAUDE INFORMÁTICO EN LA BANCA DIGITAL EN LIMA METROPOLITANA EN EL AÑO 2022

FORMULACIÓN DEL PROBLEMA	OBJETIVOS	FORMULACIÓN DE HIPÓTESIS	VARIABLES E INDICADORES	METODOLOGÍA
PROBLEMA GENERAL ¿De qué manera influye la auditoría interna en la detección del fraude informático financiero en la banca digital en Lima Metropolitana, año 2022?	**OBJETIVO GENERAL** Determinar si la auditoría interna incide en la detección del fraude informático financiero en la banca digital en Lima Metropolitana, año 2022	**HIPÓTESIS GENERAL** La auditoría interna incide favorablemente en la detección del fraude informático financiero en sector banca digital en Lima Metropolitana, año 2022	1.Variable independiente X. Auditoría interna Indicadores: X1 Control Interno X2 Cumplimiento de las Normas De Auditoría y de Información Financiera X3 Vulneración de Controles por parte de la Gerencia 2. Variable Dependiente	1. Tipo de investigación Investigación aplicada nivel descriptivo 2. Población La población estará conformada por 69 personas 3. Muestra La muestra está conformada por 69 personas entre hombres y mujeres que comprenden gerentes, seniors, asistentes, economistas,
PROBLEMAS ESPECÍFICOS a. ¿De qué manera el Control Interno incide en la disminución de la Malversación de Fondos en la banca digital?	**OBJETIVOS ESPECÍFICOS** a. Determinar si el Control Interno incide en la disminución de la Malversación de Fondos en la banca digital?	**HIPÓTESIS ESPECÍFICAS** a. El Control Interno incide en la disminución de la Malversación de Fondos en la banca digital.		

b. ¿En qué medida la exigencia del Cumplimiento de las normas de auditoría y de información financiera incide en la Gestión de riesgo de fraude en la banca digital?	b. Analizar si el Cumplimiento de las normas de auditoría y de información financiera incide en la Gestión de riesgo de fraude en la banca digital.	b. El Cumplimiento de las normas de auditoría y de información financiera incide en la Gestión de riesgo de fraude en la banca digital.	Y. Detección del fraude informático financiero Indicadores: Y1 Malversación de fondos Y2 Gestión de riesgo de fraude Y3 Ciberseguridad	contadores, administradores Se utilizó la fórmula del muestreo aleatorio simple. 5.Técnicas e instrumentos de recolección de datos: Métodos: descriptivo, estadístico, análisis, síntesis, entre otros.
c. ¿De qué manera la vulneración de Controles por parte de la Gerencia incide en la aplicación de la ciberseguridad en la banca digital?	c. Definir si la vulneración de Controles por parte de la Gerencia incide en a la aplicación de la Ciberseguridad en la banca digital.	c. La vulneración de Controles por parte de la Gerencia incide en a la aplicación de la Ciberseguridad en la banca digital.		

ANEXO Nº 02

ENCUESTA

Estimado(a) participante, con la presente encuesta se busca determinar el grado de influencia entre **"LA AUDITORÍA INTERNA Y SU INCIDENCIA EN EL FRAUDE INFORMÁTICO EN LA BANCA DIGITAL EN LIMA METROPOLITANA EN EL AÑO 2022."**

Para tal efecto, solicitamos a usted, se sirva contestar las preguntas del siguiente cuestionario cuya información ayudará a completar nuestra investigación.

Dentro de las alternativas brindadas, elija la que considere correcta, esta encuesta es **ANÓNIMA**.

Agradecemos su colaboración.

Se le agradece su colaboración

1. ¿Está usted de acuerdo que las empresas de banca digital deben contar con un área de auditoría interna especializada en fraude cibernético?

   a. Totalmente de acuerdo ( )
   b. De acuerdo ( )
   c. Indeciso ( )
   d. En desacuerdo ( )
   e. Totalmente en desacuerdo ( )

2. ¿Está usted de acuerdo que tomar en cuenta las recomendaciones de la auditoría interna beneficia a la seguridad electrónica de la empresa al detectar el fraude cibernético?

a. Totalmente de acuerdo ( )
b. De acuerdo ( )
c. Indeciso ( )
d. En desacuerdo ( )
e. Totalmente en desacuerdo ( )

3. ¿Está usted de acuerdo que el control interno debería implementar controles informáticos previamente aprobados por la gerencia de Tecnología de la Información (TI)?

a. Totalmente de acuerdo ( )
b. De acuerdo ( )
c. Indeciso ( )
d. En desacuerdo ( )
e. Totalmente en desacuerdo ( )

4. ¿Está usted de acuerdo que una auditoría interna debería basar su estrategia bajo el cumplimiento de las Normas de Auditoría de Información Financiera (NIAS) por sobre las Normas de Información Financiera (NIIF)?

a. Totalmente de acuerdo ( )
b. De acuerdo ( )
c. Indeciso ( )

d. En desacuerdo ( )

e. Totalmente en desacuerdo ( )

5. ¿Está usted de acuerdo que las Normas de Auditoría y de Información Financiera (NIAS) están debidamente actualizadas en respuesta a los casos de fraude cibernético hallados en auditorías internas?

a. Totalmente de acuerdo ( )

b. De acuerdo ( )

c. Indeciso ( )

d. En desacuerdo ( )

e. Totalmente en desacuerdo ( )

6. ¿Está usted de acuerdo que la vulneración de controles por parte de la Gerencia es considerada como el riesgo más significativo en una auditoría interna?

a. Totalmente de acuerdo ( )

b. De acuerdo ( )

c. Indeciso ( )

d. En desacuerdo ( )

e. Totalmente en desacuerdo ( )

7. ¿Está usted de acuerdo que el área de TI debe de contar con personal externo especializado en controles informáticos para un soporte neutral a fin de evitar la vulneración de Controles por parte de la Gerencia?

a. Totalmente de acuerdo ( )
b. De acuerdo ( )
c. Indeciso ( )
d. En desacuerdo ( )
e. Totalmente en desacuerdo ( )

8. ¿Está usted de acuerdo que las empresas banca digitales deben contar con una matriz de riesgos específicamente ante casos de fraude informático?

a. Totalmente de acuerdo ( )
b. De acuerdo ( )
c. Indeciso ( )
d. En desacuerdo ( )
e. Totalmente en desacuerdo ( )

9. ¿Está usted de acuerdo que la gestión de recursos tecnológicos es importante para que los equipos de TI cumplan las expectativas eficientemente?

a. Totalmente de acuerdo ( )
b. De acuerdo ( )
c. Indeciso ( )

d. En desacuerdo ( )

e. Totalmente en desacuerdo ( )

10. ¿Está usted de acuerdo que revisar si existen cambios en los patrones de gastos en la compañía favorece en la detección del fraude?

a. Totalmente de acuerdo ( )

b. De acuerdo ( )

c. Indeciso ( )

d. En desacuerdo ( )

e. Totalmente en desacuerdo ( )

11. ¿Está usted de acuerdo que los programas de prevención de fraude facilitan a los auditores internos a mitigar los niveles de riesgo dentro de la compañía?

a. Totalmente de acuerdo ( )

b. De acuerdo ( )

c. Indeciso ( )

d. En desacuerdo ( )

e. Totalmente en desacuerdo ( )

12. ¿Está usted de acuerdo que medir la eficiencia de los controles internos de la compañía brinda soporte para definir los niveles de confianza en controles?

a. Totalmente de acuerdo ( )
b. De acuerdo ( )
c. Indeciso ( )
d. En desacuerdo ( )
e. Totalmente en desacuerdo ( )

13. ¿Está usted de acuerdo que las amenazas digitales son mitigadas por el departamento de TI cuando existe un nivel elevado de ciberseguridad en la compañía?

a. Totalmente de acuerdo ( )
b. De acuerdo ( )
c. Indeciso ( )
d. En desacuerdo ( )
e. Totalmente en desacuerdo ( )

14. ¿Está usted de acuerdo que poseer una adecuada infraestructura tecnológica es necesario para el funcionamiento y soporte de los sistemas de información de la compañía?

a. Totalmente de acuerdo ( )
b. De acuerdo ( )

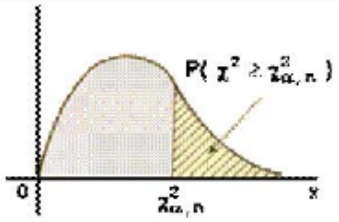
c. Indeciso ( )

d. En desacuerdo ( )

e. Totalmente en desacuerdo ( )

ANEXO N° 3

TABLA CHI CUADRADO



	Probabilidad de un valor superior				
Grados de libertad	0,1	0,05	0,025	0,01	0,005
1	2,71	3,84	5,02	6,63	7,88
2	4,61	5,99	7,38	9,21	10,60
3	6,25	7,81	9,35	11,34	12,84
4	7,78	9,49	11,14	13,28	14,86
5	9,24	11,07	12,83	15,09	16,75
6	10,64	12,59	14,45	16,81	18,55
7	12,02	14,07	16,01	18,48	20,28
8	13,36	15,51	17,53	20,09	21,95
9	14,68	16,92	19,02	21,67	23,59
10	15,99	18,31	20,48	23,21	25,19
11	17,28	19,68	21,92	24,73	26,76
12	18,55	21,03	23,34	26,22	28,30
13	19,81	22,36	24,74	27,69	29,82
14	21,06	23,68	26,12	29,14	31,32
15	22,31	25,00	27,49	30,58	32,80
16	23,54	26,30	28,85	32,00	34,27
17	24,77	27,59	30,19	33,41	35,72
18	25,99	28,87	31,53	34,81	37,16
19	27,20	30,14	32,85	36,19	38,58
20	28,41	31,41	34,17	37,57	40,00
21	29,62	32,67	35,48	38,93	41,40
22	30,81	33,92	36,78	40,29	42,80

FUENTES BIBLIOGRÁFICAS

- Acosta, M., Benavides, M. y García, N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. Universidad del Zulia. Ecuador. Recuperado de https://www.redalyc.org/journal/290/29062641023/html/#:~:text=Resumen%3A%20Los%20delitos%20inform%C3%A1ticos%2C%20son,almacenados%20en%20servidores%20o%20gadgets.
- Bermeo-Giraldo, M., Grajales-Gaviria, D., Valencia-Arias, A. y Palacios-Moya, L. (2021). Evolución de la producción científica sobre el fraude contable en las organizaciones: análisis bibliométrico. Universidad Icesi. Medellín, Colombia. Recuperado de https://www.redalyc.org/journal/212/21268838013/21268838013.pdf
- Carbajal, A. (2017). El papel de la auditoría interna y los factores pre criminógenos en el reclutamiento y selección de personal en las empresas de México, como herramienta en la detección de fraudes. Universidad Nacional Autónoma de México. Ciudad de México. Recuperado de https://repositorio.unam.mx/contenidos?c=pQ8wXB&f=650.%23.4.x_lit:Ciencias%20Sociales%20y%20Econ%C3%B3micas&d=false&q=fraude_._en_._las_._empresas&v=0&t=search_0&as=0&i=1
- Castañeda, R., Guevara, O. y Rojas, K. (2018). Valoración del riesgo de fraude interno en el subproceso de compras comerciales de supermercados peruanos S.A. de acuerdo al principio n° 2 del Fraud Risk management guide. Universidad del Pacífico. Lima, Perú. Recuperado de https://repositorio.up.edu.pe/bitstream/handle/11354/2323/Raisa_Tesis_maestria_2018.pdf?sequence=1&isAllowed=y

- Chanjan, R., Torres, D. y Gonzales, M. (2020). Claves para reconocer los principales delitos de Corrupción. Recuperado de https://repositorio.pucp.edu.pe/index/bitstream/handle/123456789/169417/claves-corrupcion.pdf?sequence=1&isAllowed=y
- De La Torre, M. (2018). Gestión del riesgo organizacional de fraude y el rol de Auditoría Interna. Pontificia Universidad Católica del Perú. Lima, Perú. Recuperado de https://www.redalyc.org/journal/2816/281658256008/281658256008.pdf
- Gumucio, J. (2021). Guía de implementación de un programa de gestión de riesgos de ciberseguridad en entidades de intermediación financiera. Universidad de Chile. Santiago de Chile, Chile. Recuperado de https://repositorio.uchile.cl/bitstream/handle/2250/180169/Guia-de-implementacion-de-un-programa-de-gestion-de-riesgos-de-ciberseguridad-en-entidades-de-intermediacion-financiera.pdf?sequence=1&isAllowed=y
- Gutierrez, J. y Necochea, P. (2020). Programa académico de Ingeniería de sistemas de información - Modelo de madurez de ciberseguridad cloud para el sector financiero. Universidad Peruana de Ciencias Aplicadas. Recuperado de https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/660408/Gutierrez_AJ.pdf?sequence=3&isAllowed=y
- Hernández, W., López, H, y Valencia, B. (2015). Equivalentes de efectivo de las empresas dedicadas al servicio de envío de encomiendas. Universidad de El Salvador. San Salvador, El Salvador. Recuperado de https://ri.ues.edu.sv/id/eprint/9604/1/Trabajo%20de%20graduacion.pdf

- Instituto Mexicano de Auditores Internos A.C. (IMAI). (septiembre de 2018). Instituto Mexicano de Auditores Internos A.C. (IMAI). Recuperado de https://www.imai.org.mx/about.php
- Jardim, D., Carneiro, A. y Silva, F. (2017). Cyber security governance and management for smart grids in brazilian energy utilities. Universidad de São Paulo. São Paulo, Brasil. Recuperado de https://www.redalyc.org/pdf/2032/203254259006.pdf
- Jiménez, D. y Namuche, J. (2019). Estado del Arte de la Auditoría Informática y su Importancia para las Empresas. Universidad Nacional de Piura. Recuperado de https://repositorio.unp.edu.pe/bitstream/handle/UNP/1971/FCC-JIM-ORT-2019.pdf?sequence=1&isAllowed=y
- KPMG (2016). Global Profiles of the fraudster: Technology enables and weak controls fuel the fraud. Recuperado de https://assets.kpmg.com/content/dam/kpmg/pdf/2016/05/profiles-of-the-fraudster.pdf
- KMPG (2022). Una triple amenaza en las Américas. Argentina. Recuperado de:https://assets.kpmg.com/content/dam/kpmg/ar/pdf/2022/triple-amenaza-en-%20las-americas-2022-kpmg-fraud-outlook-esp-ar.pdf
- Mengoa, M. (2021). Punibilidad del comportamiento del phisher-mule en el delito de fraude informático en el Perú. Universidad César Vallejo. Recuperado de : https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/62379/Mengoa_VMM-SD.pdf?sequence=1&isAllowed=y

- Newmeyer, K. (2015). Ciberespacio, Ciberseguridad y Ciberguerra. ESUP. Recuperado de https://repositorio.esup.edu.pe/bitstream/20.500.12927/113/1/pp.76-95.pdf
- Paiva, R. (2021). El paradigma objetivo en la responsabilidad de las entidades bancarias por fraude electrónico: una mirada desde las obligaciones de resultado. Universidad Nacional de Colombia. Medellín, Colombia. Recuperado de https://repositorio.unal.edu.co/bitstream/handle/unal/80691/1033768750-2021.pdf?sequence=2&isAllowed=y
- Pariona, R. (2019). El delito de malversación de fondos públicos: Consideraciones dogmáticas y político-criminales. Revista Derecho & Sociedad, N° 52. Recuperado de https://revistas.pucp.edu.pe/index.php/derechoysociedad/article/view/21221/20926
- Price waterhouse Coopers (2022). PwC's Global Economic Crime and Fraud Survey. Protecting the perimeter: The rise of external fraud. Recuperado de https://www.pwc.com/gx/en/forensics/gecsm-2022/pdf/PwC%E2%80%99s-Global-Economic-Crime-and-Fraud-Survey-2022.pdf
- Price waterhouse Coopers (2018). Fraude al descubierto Encuesta Global Crimen Económico 2018. Colombia. Recuperado de https://www.pwc.com/co/en/publications/technology/Fraude-al-descubierto.pdf
- Reátegui, R. (2019). Auditoría Financiera. Universidad Nacional De La Amazonia Peruana. Iquitos, Perú. Recuperado de https://repositorio.unapiquitos.edu.pe/bitstream/handle/20.500.12737/5696/Reyner_examen_titulo_2019.pdf?sequence=4&isAllowed=y

- Rizo, P. (2019). Importancia de la auditoría Interna para una PYME mexicana: una aproximación cualitativa desde el sector construcción. Universidad Nacional Autónoma de México. México. Recuperado de https://repositorio.unam.mx/contenidos/importancia-de-la-auditoria-interna-para-una-pyme-mexicana-una-aproximacion-cualitativa-desde-el-sector-de-la-constru-3448936?c=bw99go&d=false&q=auditor%C3%ADa_._interna&i=1&v=1&t=search_0&as=0
- Rodríguez, E. (2014). Identificación y Mejoramiento de los Procesos de Gestión del Conocimiento en el Área De Auditoría Interna de una Aseguradora Colombiana. Universidad Nacional de Colombia. Bogotá. Recuperado de https://repositorio.unal.edu.co/bitstream/handle/unal/52218/940903.2014.pdf?sequence=1&isAllowed=y
- Salinas, A. (2020). Modelo de ciberseguridad para cajas municipales en tiempos de transformación digital - Un nuevo enfoque. Universidad Privada del Norte. Recuperado de https://repositorio.upn.edu.pe/handle/11537/29733
- Superintendencia de Banca, Seguros y AFP (2022). Información Estadística Unidad de Inteligencia Financiera del Perú. Recuperado de https://www.sbs.gob.pe/Portals/5/jer/ESTADISTICAS-OPERATIVAS/2022/Bolet%C3%ADn%20estad%C3%ADstico%20dic%202022.pdf
- Torres, V. (2020). Plan de Auditoría Forense para evitar malversación de fondos en la Municipalidad Distrital de Ciudad Eten. Universidad César Vallejo. Lima, Perú. Recuperado de

https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/46225/Torres_CVE-SD.pdf?sequence=1&isAllowed=y

- Urdanégui, R. (2018). El control interno en las empresas. Revistas UPC. Lima, Perú. Recuperado de https://revistas.upc.edu.pe/index.php/rgm/article/view/911/881