UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO

EL DELITO DE FRAUDE MEDIANTE EL USO DE LA INTELIGENCIA ARTIFICIAL A LAS EMPRESAS DE SERVICIOS DE LA CIUDAD DE PUCALLPA, 2024.

Tesis para optar el título profesional de

ABOGADO

ROGER ALBERTO TUANAMA TIRADO

GIULIANA JENNEL ENCISO HUANIO

Pucallpa, Perú

2025

UNIVERSIDAD NACIONAL DE UCAYALI
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

ACTA DE EXAMEN PARA OPTAR EL TITULO DE ABOGADO

En la ciudad de Pucallpa, siendo las 11:00 am del día Viernes 18 de julio del año 2025, en el auditorio de la Facultad de Derecho y Ciencias Politicas de la Universidad Nacional de Ucayali, cito en el Tercer Piso de la Facultad de Derecho y Ciencias Politicas, se dio inicio a la correspondiente a la sustentación y/o defensa de la tesis denominada "EL DELITO DE FRAUDE MEDIANTE EL USO DE LA INTELIGENCIA ARTIFICIAL A LAS EMPRESAS DE SERVICIOS DE LA CIUDAD DE PUCALLPA, 2024", presentado por los bachilleres en Derecho y Ciencias Politicas: ROGER ALBERTO TUANAMA TIRADO y GIULIANA JENNEL ENCISO HUANIO.

En cumplimiento del Reglamento de Grados y Titulos, el Secretario Académico de la Facultad procedió a presentar a los Miembros del Jurado integrados por los docentes: Dr. LIZANDRO LEVEAU PEZO (Presidente), Dr. JUAN ARQUIMEDES NUÑEZ TERREROS (Miembro) y Dr. SANTOS WILFREDO ANTICOCA HONORES (Miembro), designados con Memorando Múltiple Nº 115/2025-UNU/FDyCP/GyT de fecha 16 de Julio del 2025; luego del cual el señor presidente instó al Secretario Académico a presentar a los bachilleres examinados.

Acto seguido el Presidente del Jurado invitó a los bachilleres a iniciar la exposición, del informe final de tesis; a cuyo término los miembros del jurado formularon las preguntas y objeciones respectivas, la misma que fueron absueltas de forma satisfactoria por los ponentes.

Continuando con el desarrollo de la sustentación y de conformidad con el Reglamento de Grados y Títulos, el presidente invitó a los bachilleres examinados y al público asistente a abandonar la Sala para su correspondiente deliberación en forma reservada.

Seguidamente el Jurado emitió la calificación general, de cuyo resultado se establece que los bachilleres ROGER ALBERTO TUANAMA TIRADO y GIULIANA JENNEL ENCISO HUANIO; fueron APROBADOS POR UNANIMIDAD.

Reiniciando el acto Público se procede a la Juramentación de honor y las felicitaciones por los miembros del Jurado, procediéndose a la lectura de la presente acta, dando por concluido el acto de sustentación siendo la 12:00 am. Del mismo día, lo suscribieron en señal de conformidad; de lo que doy fe.

Dr. LIZANDRO LEVEAU PEZO
PRESIDENTE

Dr. JUAN ARQUIMEDES NUÑEZ TERREROS
MIEMBRO

Dr. SANTOS WILFREDO ANTICOCA HONORES
MIEMBRO

Dr. RUBEN ADOLFO CERNA LEVEAU
SECRETARIO ACADÉMICO (e)

ACTA DE APROBACIÓN

La presente tesis fue aprobada por los miembros del Jurado Evaluador de la Facultad de Derecho y Ciencias Políticas de la Universidad Nacional de Ucayali, como requisito para optar el título profesional de Abogado.

DR. LIZANDRO LEVEAU PEZO

Presidente

DR. JUAN ARQUIMEDES NUÑEZ TERREROS

Miembro

DR. SANTOS WILFREDO ANTICONA HONORES

Miembro

DRA. GLORIA GONZALES SANTOS

Asesor

BACH. ROGER ALBERTO TUANAMA TIRADO

Tesista 1

BACH. GIULIANA JENNÉL ENCISO HUANIO

Tesista 2

UNIVERSIDAD NACIONAL DE UCAYALI

DIRECCIÓN DE PRODUCCIÓN INTELECTUAL

CONSTANCIA

ORIGINALIDAD DE TRABAJO DE INVESTIGACIÓN

Nº V/308-2025.

La Dirección de Producción Intelectual de la Universidad Nacional de Ucayali, hace constar por la presente, que el trabajo académico de investigación, titulado:

"EL DELITO DE FRAUDE MEDIANTE EL USO DE LA INTELIGENCIA ARTIFICIAL A LAS EMPRESAS DE SERVICIOS DE LA CIUDAD DE PUCALLPA, 2024"

Autor(es)	:	**TUANAMA TIRADO, ROGER ALBERTO**
		ENCISO HUANIO, GIULIANA JENNEL
Facultad	:	**DERECHO Y CIENCIAS POLÍTICAS**
Escuela	:	**DERECHO**
Asesor(a)	:	**Dra. GONZALES SANTOS, GLORIA**

Presenta un **porcentaje de similitud de 8%,** verificado en el Sistema Antiplagio COMPILATIO,

De acuerdo a los criterios de porcentaje establecidos en el articulo 9 de la DIRECTIVA DE USO DEL SISTEMA ANTIPLAGIO, el cual indica que todo trabajo de investigación no debe superar el 10%. **En tal sentido, se declara, que el presente trabajo de investigación: SI Contiene un porcentaje aceptable de similitud,** procediéndose a emitir la presente Constancia de Originalidad de Trabajo de Investigación (COTI) a solicitud del asesor.

En señal de conformidad se firma y sella el presente documento.

Fecha: 10/06/2025

Mg. JOSÉ MANUEL CÁRDENAS BERNAOLA
Director de Producción Intelectual

UNIVERSIDAD NACIONAL DE UCAYALI

DIRECCIÓN DE PRODUCCIÓN INTELECTUAL

AUTORIZACIÓN DE PUBLICACIÓN

Repositorio de la Universidad Nacional de Ucayali

Yo, Roger Alberto Tuanama Tirado

Autor de la tesis titulada: El Delito de fraude mediante el uso de la Inteligencia Artificial a las empresas de servicios de la Ciudad de Pucallpa, 2024.

Sustentada el año: 2025

Asesor(a): Gloria Gonzalez Santos

Facultad: Derecho y Ciencias Políticas

Escuela Profesional: Derecho

Autorizo la publicación:

PARCIAL [ ] TOTAL [X]

De mi trabajo de Investigación en el Repositorio Institucional de la Universidad Nacional de Ucayali (www.repositorio.unu.edu.pe), bajo los siguientes términos:

Primero: Otorgo a la Universidad Nacional de Ucayali licencia no exclusiva para reproducir, distribuir, comunicar, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público en general mi tesis (incluido el resumen) a través del Repositorio Institucional de la UNU, en formato digital sin modificar su contenido, en el Perú y en el extranjero; por el tiempo y las veces que considere necesario y libre de remuneraciones.

Segundo: Declaro que la tesis es una creación de mi autoría y exclusiva titularidad, por tanto me encuentro facultado a conceder la presente autorización, garantizando que la tesis no infringe derechos de autor de terceras personas, caso contrario, me hago único(a) responsable de investigaciones y observaciones futuras, de acuerdo a lo establecido en el estatuto de la Universidad Nacional de Ucayali, la Superintendencia Nacional de Educación Superior Universitaria y el Ministerio de Educación.

En señal de conformidad firmo la presente autorización.

Fecha: 30/07/25

Email: rgtuanama17@gmail.com Firma:

Teléfono: 903458380 DNI: 62969475

www.repositorio.unu.edu.pe
repositorio@unu.edu.pe

UNIVERSIDAD NACIONAL DE UCAYALI

DIRECCIÓN DE PRODUCCIÓN INTELECTUAL

AUTORIZACIÓN DE PUBLICACIÓN

Repositorio de la Universidad Nacional de Ucayali

Yo, Giuliana Jennél Enciso Huanio

Autor de la tesis titulada: El Delito de fraude mediante el uso de la Inteligencia Artificial a las empresas de servicios de la Ciudad de Pucallpa, 2024.

Sustentada el año 2025

Asesor(a): Gloria Gonzales Santos

Facultad: Derecho y Ciencias Políticas

Escuela Profesional: Derecho

Autorizo la publicación:

PARCIAL [ ] TOTAL [X]

De mi trabajo de investigación en el Repositorio Institucional de la Universidad Nacional de Ucayali (www.repositorio.unu.edu.pe), bajo los siguientes términos:

Primero: Otorgo a la Universidad Nacional de Ucayali licencia no exclusiva para reproducir, distribuir, comunicar, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público en general mi tesis (incluido el resumen) a través del Repositorio Institucional de la UNU, en formato digital sin modificar su contenido, en el Perú y en el extranjero; por el tiempo y las veces que considere necesario y libre de remuneraciones.

Segundo: Declaro que la tesis es una creación de mi autoría y exclusiva titularidad, por tanto me encuentro facultado a conceder la presente autorización, garantizando que la tesis no infringe derechos de autor de terceras personas, caso contrario, me hago único(a) responsable de investigaciones y observaciones futuras, de acuerdo a lo establecido en el estatuto de la Universidad Nacional de Ucayali, la Superintendencia Nacional de Educación Superior Universitaria y el Ministerio de Educación.

En señal de conformidad firmo la presente autorización.

Fecha: 30/07/25

Email: gjulianaenciso07@gmail Firma:

Teléfono: 986293696 DNI: 75375023

DEDICATORIA

A Dios, por ser guía constante y fuente de sabiduría en los momentos más difíciles del camino académico.

A nuestros padres, por su esfuerzo incondicional, amor inquebrantable y apoyo constante, pilares fundamentales en nuestra formación profesional y personal.

A nuestros seres queridos, quienes, con su paciencia y comprensión, nos impulsaron a seguir adelante pese a las adversidades.

Y finalmente, a todos aquellos que creen en el poder de la educación como medio para transformar la realidad y construir un futuro más justo y seguro.

AGRADECIMIENTO

Agradecemos, en primer lugar, a Dios, por concedernos la salud, la fuerza y la perseverancia necesarias para culminar con éxito esta etapa tan significativa de nuestras vidas.

Expresamos nuestro profundo agradecimiento a la Universidad Nacional de Ucayali, en especial a la Facultad de Derecho y Ciencias Políticas, por brindarnos una formación académica sólida y comprometida con la excelencia.

A nuestros asesores, docentes y jurado evaluador, por sus enseñanzas, observaciones constructivas y orientación profesional a lo largo del proceso investigativo.

A las empresas de servicios de la ciudad de Pucallpa que colaboraron con esta investigación, por su disposición y apertura para compartir información valiosa.

A nuestras familias, por su amor, comprensión y apoyo constante durante cada paso de este recorrido académico. Sin ustedes, esta meta no hubiese sido posible.

Y finalmente, a todos nuestros compañeros y compañeras de estudio, por compartir este trayecto con entrega, fraternidad y compromiso con el saber.

INDICE GENERAL

DEDICATORIA ii

AGRADECIMIENTO iii

RESUMEN vii

ABSTRACT x

INTRODUCCION xi

CAPITULO I 14

PLANTEAMIENTO DEL PROBLEMA 14

1.1. Descripción del problema 14

1.2. Formulación del Problema 17

1.2.1. Problema General 17

1.2.2. Problemas Específicos 17

1.3. Formulación de objetivos 17

1.3.1. Objetivo General 17

1.3.2. Objetivos Específicos 18

1.4. Hipótesis 18

1.4.1. Hipótesis General 18

1.4.2. Hipótesis Específicas 18

1.5. Variables 19

1.5.1. Variable 1: Inteligencia artificial 19

1.5.2. Variable 2: Delito de fraude 19

1.6. Operacionalización de Variables 19

1.7. Justificación de la investigación 21

1.7.1. Justificación Teórica 21

1.7.2. Justificación Práctica 22

1.7.3. Importancia 22

CAPITULO II 23

MARCO TEÓRICO 23

2.1. Antecedentes jurídicos del problema 23

2.1.1. Antecedentes Internacionales 23

2.1.2. Antecedentes Nacionales 25

2.1.3. Antecedentes Locales 27

2.2. Bases Teóricas 27

2.3. Marco Legal 54

2.4. Definición de términos básicos 55

CAPITULO III 59

METODOLOGÍA DE LA INVESTIGACIÓN 59

3.1. Método de Investigación 59

3.1.2. Nivel de Investigación 59

3.1.3. Diseño de Investigación 60

3.2. Población y Muestra 60

3.3. Técnica e Instrumento de Recolección de Datos 62

3.4. Procedimiento de Recolección de Datos 63

3.5. Tratamiento de datos 64

CAPITULO IV 65

RESULTADOS 65

4.1. Resultados de la Investigación 65

CAPITULO V 92

CONCLUSIONES Y RECOMENDACIONES 92

REFERENCIAS BIBLIOGRÁFICAS 95

ÍNDICE DE TABLAS

Tabla 1 Variable inteligencia artificial 65

Tabla 2 Baremos de la dimensión detección de patrones anómalos 67

Tabla 3 Baremos de la dimensión seguridad en las transacciones 68

Tabla 4 baremos de la dimensión eficiencia operativa 70

Tabla 5 baremos de la variable delito de fraude 72

Tabla 6 Baremos de la dimensión cumplimiento normativo 74

Tabla 7 baremos de la dimensión gravedad del fraude 75

Tabla 8 baremos de la dimensión eficiencia en la investigación y respuesta 77

Tabla 9 Porcentaje de respuestas con respecto a la dimensión 1.1: Detección de patrones anómalos 79

Tabla 10 Porcentaje de respuestas con respecto a la dimensión 1.2: Seguridad en las transacciones 81

Tabla 11 Porcentaje de respuestas con respecto a la dimensión 1.3: Eficiencia operativa 84

Tabla 12 Porcentaje de respuestas con respecto a la variable 1: Inteligencia artificial 87

ÍNDICE DE FIGURAS

Figura 1 Gráfico de barras de la Variable 1: Inteligencia artificial 66

Figura 2 Gráfico de barras de la Dimensión 1.1: Detección de patrones anómalos 67

Figura 3 Gráfico de barras de la Dimensión 1.2: Seguridad en las Transacciones 69

Figura 4 de barras de la Dimensión 1.3: Eficiencia operativa 70

Figura 5 barras de la Variable 2: Delito de fraude 72

Figura 6 Gráfico de barras de la Dimensión 2.1: Cumplimiento normativo ... 74

Figura 7 Barras de la Dimensión 2.2: Gravedad del fraude 75

Figura 8 Gráfico de barras de la Dimensión 2.3: Eficiencia en la investigación y respuesta 77

RESUMEN

La investigación realizada planteó como objetivo general determinar de qué manera se comete el delito de fraude mediante el uso inteligencia artificial a las empresas de servicios de la ciudad de Pucallpa, 2024. La metodología empleada incluyó el uso de un método investigativo hipotético deductivo, con un estudio de tipo aplicado, con diseño no experimental de corte transversal. En la muestra se incluyeron a 95 empresas de servicios formalizadas, las cuales fueron elegidas aleatoriamente. Como instrumento de recolección de datos se utilizó un cuestionario el cual consta de 36 preguntas. Los datos recolectados a partir de la aplicación del cuestionario fueron clasificados en hojas Ms Excel, siendo después procesados en el programa SPSS versión 25, generándose tablas y gráficos que permitieron una mejor comprensión de los resultados. Los resultados revelaron una proporción muestral de $\overline{p}$ = 0.721 (> 0.05). Además, el valor del estadístico de prueba z fue de 4,308 (>1,645), lo que permitió rechazar la hipótesis nula. En consecuencia, se concluyó que el delito de fraude mediante el uso inteligencia artificial se cometió en perjuicio del 50% de las empresas de servicios de la ciudad de Pucallpa, 2024.

Palabras clave: Delito de fraude/ Inteligencia artificial / Empresas

ABSTRACT

The general objective of the research carried out was to determine how the crime of fraud is committed through the use of artificial intelligence in service companies in the city of Pucallpa, 2024. The methodology used included the use of a hypothetical deductive investigative method, with a applied study, with a non-experimental cross-sectional design. The sample included 95 formalized service companies, which were chosen randomly. A questionnaire was used as a data collection instrument, which consists of 36 questions. The data collected from the application of the questionnaire were classified in MS Excel sheets, and then processed in the SPSS version 25 program, generating tables and graphs that allowed a better understanding of the results. The results revealed a sample proportion of $\bar{p} = 0.721$ (> 0.05). Furthermore, the value of the z test statistic was 4,308 (>1.645), which allowed us to reject the null hypothesis. Consequently, it was concluded that the crime of fraud through the use of artificial intelligence was committed to the detriment of 50% of the service companies in the city of Pucallpa, 2024.

Keywords: Fraud crime / Artificial intelligence / Companies

INTRODUCCION

El crecimiento exponencial de la inteligencia artificial en el entorno empresarial ha brindado beneficios significativos, como la optimización de procesos, la personalización de servicios y la mejora de la eficiencia operativa. Sin embargo, al mismo tiempo, ha abierto nuevas puertas para la perpetración de fraudes. El creciente fenómeno del fraude impulsado por la inteligencia artificial en las empresas de servicios nace debido a la complejidad de los algoritmos y sistemas inteligentes utilizados, puesto que estos sistemas, diseñados para optimizar procesos y ofrecer soluciones avanzadas, lamentablemente también proporcionan un terreno fértil para individuos malintencionados que buscan aprovecharse de su sofisticación en beneficio propio.

Morán (2021) menciona que la naturaleza misma de los algoritmos de inteligencia artificial, como las redes neuronales profundas o los algoritmos de aprendizaje automático, a menudo involucra una cantidad significativa de capas y conexiones complejas, estas estructuras opacas pueden ser explotadas por actores malintencionados para camuflar sus actividades fraudulentas, dificultando enormemente su detección por parte de los sistemas de seguridad convencionales.

Además, la capacidad de los sistemas inteligentes para adaptarse y aprender de los datos puede ser utilizada en su contra en manos de los estafadores, puesto que, los algoritmos de IA pueden ser entrenados para identificar patrones sutiles en los datos y ajustar sus comportamientos en consecuencia, esto significa que los estafadores pueden utilizar técnicas de evasión sofisticadas, como eludir los controles de seguridad al aprender y adaptarse a las defensas implementadas en tiempo real.

Otro factor crucial es la velocidad y la escala a la que operan los sistemas de IA, con el procesamiento de grandes cantidades de datos en tiempo real los estafadores pueden aprovecharse de esta capacidad para realizar actividades fraudulentas de manera rápida y masiva, abrumando los sistemas de detección tradicionales que no están preparados para manejar tales volúmenes de información.

En el Perú, la creciente prevalencia del fraude impulsado por la IA en las empresas de servicios se debe a la combinación de la complejidad inherente de los algoritmos y sistemas inteligentes a través de su capacidad para adaptarse a los algoritmos de las empresas y cometer delitos de fraude a través de ella. Además, la IA puede ser empleada para generar ataques más personalizados y dirigidos, lo que aumenta la efectividad de las técnicas de ingeniería social y el phishing. Por ejemplo, los algoritmos de aprendizaje automático pueden analizar grandes cantidades de datos para identificar patrones de comportamiento de los usuarios y crear mensajes de phishing altamente convincentes y específicos. Por ejemplo, los algoritmos de aprendizaje automático pueden examinar el historial de navegación en línea, las interacciones en redes sociales, los correos electrónicos anteriores y otros datos disponibles para comprender mejor los intereses, las preferencias y las relaciones sociales de un individuo. Con esta información detallada, los atacantes pueden crear correos electrónicos, mensajes de texto o incluso llamadas telefónicas que se ajusten perfectamente al contexto y las preocupaciones del objetivo, aumentando significativamente la probabilidad de que caigan en la trampa.

Moreno, et. al (2023) señala que otro aspecto importante es la capacidad de la inteligencia artificial para adaptarse y evolucionar sus tácticas en función de la retroalimentación recibida, los algoritmos de aprendizaje automático pueden

analizar continuamente los resultados de los ataques pasados y ajustar sus estrategias en consecuencia para maximizar el éxito futuro. Esto significa que los ataques de phishing impulsados por IA no solo son altamente efectivos desde el principio, sino que también tienden a volverse aún más sofisticados y difíciles de detectar con el tiempo. En la ciudad de Pucallpa, el mayor reto que afrontan los empresarios ante los delitos de fraude a través de inteligencia artificial es la falta de regulación y supervisión específica sobre el uso de la inteligencia artificial en el ámbito empresarial. A medida que la tecnología avanza a un ritmo vertiginoso, las leyes y políticas a menudo no pueden mantenerse al día con los nuevos desafíos y riesgos que surgen, esto deja a las empresas de servicios en una posición vulnerable, con la responsabilidad de desarrollar sus propias estrategias de seguridad y protección de datos.

Generando consecuencias devastadoras tanto para las empresas como para los clientes, además de las pérdidas financieras, el fraude puede dañar la reputación de la empresa, socavar la confianza del cliente y provocar litigios costosos, por otro lado, en sectores sensibles como la salud o las finanzas, el fraude puede tener consecuencias aún más graves, como el acceso no autorizado a información confidencial o la manipulación de datos críticos.

Es por ello que el fraude mediante el uso de la inteligencia artificial representa un desafío significativo para las empresas de servicios en la actualidad y para hacer frente a este problema, es crucial que las empresas comprendan los riesgos asociados con la IA, implementen medidas de seguridad adecuadas y se mantengan al tanto de las tendencias y desarrollos en este campo en constante evolución.

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción del problema

A nivel internacional, las empresas de servicios, que abarcan una amplia gama de sectores como finanzas, telecomunicaciones, salud, entre otros, están adoptando cada vez más tecnologías de la inteligencia artificial (IA) para mejorar la eficiencia operativa, la toma de decisiones y la experiencia del cliente, sin embargo, esta adopción de tecnología también conlleva nuevos riesgos, ya que los delincuentes aprovechan las vulnerabilidades en los sistemas de IA para perpetrar fraudes preferidos y difíciles de detectar. En ese sentido, según el Centro de Operaciones de Seguridad (SOC), los casos de fraude digital aumentan un 74%, impulsados por el uso indebido de tecnologías avanzadas como inteligencia artificial para crear deepfakes, phishing y falsificación de voz. Ante ese panorama, Castello (2021) menciona que, los delincuentes utilizan algoritmos de IA para crear correos electrónicos, mensajes de texto o llamadas telefónicas personalizadas que engañan a los empleados de las empresas de servicios para revelar información confidencial o realizar transferencias de fondos. Siendo así que, debido a la complejidad y la naturaleza dinámica de estos ataques de fraude mediante IA hace que las empresas presenten desafíos significativos al momento de optar por un sistema de inteligencia artificial.

En el Perú, según el Comercio durante lo que va del año 2024, se han detectado 50 casos de estafas utilizando IA lo cual se espera que aumente considerablemente en los próximos años a medida que las nuevas tendencias de hacking se vuelvan más accesibles en el país. Además, los sistemas tecnológicos más vulnerables a las estafas con IA son los medios de comunicación entre pares, como el correo electrónico, los audios o llamadas, o incluso las videollamadas. Los modelos generativos de IA como Midjourney, GPT o Gemini pueden crear audios,

textos o imágenes realistas que se pueden utilizar para engañar a las personas. Por su parte, el panorama para las empresas que incorporan inteligencia artificial es desafiante, ya que muchas de ellas enfrentan dificultades para establecer defensas efectivas contra las amenazas derivadas de su uso, la complejidad de estas tecnologías y su rápida evolución a menudo superan la experiencia y los recursos disponibles en el ámbito empresarial local. Por ello, esta situación se ve agravada por la falta de regulaciones específicas y políticas de seguridad cibernética diseñadas para abordar los riesgos únicos asociados con la inteligencia artificial en el contexto peruano. Moreno, et.al (2023) establece que, en un entorno donde la adopción de tecnologías de IA está en aumento, y las empresas enfrentan una carrera constante para mantenerse al día con las últimas tendencias y desarrollar capacidades de defensa cibernética adecuadas, la falta de orientación regulatoria específica deja a muchas organizaciones sin un marco claro para abordar estas preocupaciones de seguridad. Esta brecha regulatoria permite que los delincuentes aprovechen las lagunas en la protección cibernética y perpetren ataques cada vez más beneficiosos mediante el uso de inteligencia artificial. Además, la falta de políticas adaptadas a la realidad peruana dificulta la implementación de medidas proactivas de seguridad cibernética, siendo así que las empresas se encuentran navegando en un terreno incierto, donde la ausencia de directrices claras dificulta la identificación y mitigación de riesgos específicos relacionados con la inteligencia artificial, creando un entorno propicio para la explotación por parte de actores maliciosos, quienes pueden aprovecharse de las vulnerabilidades sin una supervisión y control adecuados. En consecuencia, las empresas peruanas que emplean inteligencia artificial se encuentran en una situación vulnerable, enfrentando amenazas que evolucionan rápidamente y careciendo del respaldo regulatorio y de políticas necesarias para proteger sus activos y datos de manera efectiva.

En el contexto de la ciudad de Pucallpa, el avance tecnológico ha generado

nuevas formas de cometer delitos, y uno de los más preocupantes es el fraude mediante el uso de inteligencia artificial (IA) dirigido a empresas de servicios, esta problemática plantea desafíos significativos para la seguridad económica y la confianza en las transacciones comerciales dentro de la comunidad empresarial de la ciudad, debido a que el delito de fraude mediante el uso de inteligencia artificial a las empresas de servicios en Pucallpa es una amenaza creciente y compleja que ha surgido como resultado de la adopción generalizada de tecnologías de IA en las operaciones empresariales. Siendo así que, a medida que las empresas incorporan sistemas automatizados y algoritmos inteligentes para optimizar sus procesos, también aumentan los riesgos asociados con el mal uso de estas tecnologías con fines fraudulentos, sobre todo la falta de comprensión sobre cómo se puede utilizar la inteligencia artificial para cometer fraude y la insuficiente preparación en términos de seguridad cibernética de muchas empresas de servicios en Pucallpa las deja vulnerables a diversas formas de ataques perpetrados por actores malintencionados. Sin embargo, este problema se agrava debido a la falta de marcos regulatorios específicos y medidas de seguridad cibernética adecuadas adaptadas a la realidad local, asimismo como la ausencia de protocolos de detección temprana y sistemas de prevención efectivos deja a las empresas de servicios expuestas a sufrir pérdidas financieras significativas, daños en su reputación y la confianza de sus clientes. Además, en los últimos meses la presencia de la IA se ha incrementado en todos los campos tanto profesionales como comerciales, y no podía estar ajena en los actos delincuenciales que aprovechan esta nueva tecnología para estafas, extorciones, fraudes, entre otros, por lo cual, es crucial desarrollar estrategias efectivas de prevención y mitigación que fortalezcan la ciberseguridad de las empresas de servicios en Pucallpa y promuevan un entorno comercial más seguro y confiable en la ciudad.

1.2. Formulación del Problema

1.2.1. Problema General

¿De qué manera se comete el delito de fraude mediante el uso inteligencia artificial a las empresas de servicios de la ciudad de Pucallpa, 2024?

1.2.2. Problemas Específicos

- ¿De qué manera se vienen ejecutando patrones anómalos mediante el uso de inteligencia artificial a las empresas de servicios de la ciudad de Pucallpa, 2024?
- ¿De qué forma vulneran la seguridad en las transacciones mediante el uso inteligencia artificial a las empresas de servicios de la ciudad de Pucallpa, 2024?
- ¿Cómo afectan la eficiencia operativa mediante el uso inteligencia artificial dentro de las empresas de servicios de la ciudad de Pucallpa, 2024?

1.3. Formulación de objetivos

1.3.1. Objetivo General

Determinar de qué manera se comete el delito de fraude mediante el uso inteligencia artificial a las empresas de servicios de la ciudad de Pucallpa, 2024.

1.3.2. Objetivos Específicos

- Establecer de qué manera se vienen ejecutando patrones anómalos mediante el uso de inteligencia artificial a las empresas de servicios de la ciudad de Pucallpa, 2024.
- Precisar en qué forma vulneran la seguridad en las transacciones mediante el uso inteligencia artificial a las empresas de servicios de la ciudad de Pucallpa, 2024.
- Caracterizar cómo afectan la eficiencia operativa mediante el uso inteligencia artificial a las empresas de servicios de la ciudad de Pucallpa, 2024.

1.4. Hipótesis

1.4.1. Hipótesis General

El delito de fraude mediante el uso inteligencia artificial se cometió en perjuicio en más del 50% de las empresas de servicios de la ciudad de Pucallpa, 2024.

1.4.2. Hipótesis Específicas

- Los patrones anómalos mediante el uso de inteligencia artificial se vienen ejecutando en más del 50% de las empresas de servicios de la ciudad de Pucallpa, 2024.
- La vulneración de la seguridad en las transacciones mediante el uso inteligencia artificial se está produciendo en más del 50% de las empresas de servicios de la ciudad de Pucallpa, 2024.
- La eficiencia operativa es afectada mediante el uso inteligencia artificial en más del 50% de las empresas de servicios de la ciudad de Pucallpa, 2024.

1.5. Variables

1.5.1. Variable 1: Inteligencia artificial

Definición conceptual:

“La inteligencia artificial se refiere a la capacidad de las máquinas para realizar tareas que normalmente requieren inteligencia humana, estas tareas incluyen el aprendizaje, el razonamiento, la percepción visual, el reconocimiento del lenguaje natural, la toma de decisiones y la resolución de problemas” (Rouhiainen, 2018).

1.5.2. Variable 2: Delito de fraude

Definición conceptual:

“El delito de fraude se refiere a cualquier acción o conducta engañosa, astuta o fraudulenta realizada con la intención de obtener beneficios económicos o

financieros de manera ilícita o injusta, esta conducta implica el uso de engaños, mentiras, falsificaciones u otros medios deshonestos para inducir a otra persona o entidad a actuar de una manera que resulte en pérdida económica para ellos o en beneficio injusto para el perpetrador del fraude". (Lobo, Gil y Aguirre, 2023).

1.6. Operacionalización de Variables

1.6.1. Variable 1: Inteligencia artificial

Definición operacional:

"La inteligencia artificial es un campo de la informática que busca desarrollar sistemas capaces de emular y ejecutar funciones cognitivas humanas de manera autónoma, esta disciplina se apoya en un conjunto diverso de técnicas, algoritmos y modelos computacionales con el objetivo de capacitar a las máquinas para realizar tareas que van más allá de las capacidades tradicionales de la programación convencional" (López, 2019).

Dimensión 1.1: Detección de patrones anómalos

Indicadores:

- Identificación de transacciones inusuales
- Reconocimiento de comportamientos atípicos
- Alertas de Fraude

Dimensión 1.2: Seguridad en las transacciones

Indicadores:

- Autenticación Robusta
- Protección contra Ataques
- Seguridad en la Comunicación

Dimensión 1.3: Eficiencia Operativa

Indicadores:

- Recursos utilizados por transacción detectada
- Costo Operativo

- Disponibilidad

1.6.2. Variable 2: Delito de fraude

Definición operacional:

"El delito de fraude se refiere al uso indebido de cualquier medio, sea un sistema informático, redes o dispositivos electrónicos para realizar actividades fraudulentas, esto puede incluir el acceso no autorizado a información confidencial, la manipulación de datos, el robo de identidad en línea y la distribución de software malicioso" (Moreno, et. al, 2023).

Dimensión 2.1: Cumplimiento normativo

Indicadores:

- Transacciones que cumplen con la normativa
- Actualización normativa
- Auditorias exitosas

Dimensión 2.2: Gravedad del fraude

Indicadores:

- Monto promedio de fraude
- Casos de fraude
- Impacto en las partes afectadas

Dimensión 2.3: Eficiencia en la investigación y Respuesta

Indicadores:

- Repuesta a incidentes
- Resolución de casos
- Colaboración interinstitucional

1.7. Justificación de la investigación

1.7.1. Justificación Teórica

La justificación teórica de esta investigación respecto al delito de fraude

informático mediante el uso de inteligencia artificial a empresas de servicios se fundamentó en la vulnerabilidad inherente de los sistemas de inteligencia artificial respecto a la falta de conocimientos sobre el tema, aumentando la complejidad del delito en el contexto digital debido a la falta de información de los empresarios que empleaban inteligencia artificial en sus empresas, desconociendo totalmente su aplicación y la seguridad que debían emplear. Esto generó un impacto económico negativo y reputacional para las empresas, ya que se vieron expuestas a fraudes informativos. Además de ello, se recalca la necesidad de regulación y protección adecuadas en este tipo de casos.

1.7.2. Justificación Práctica

La justificación práctica de esta investigación radicó en el conocimiento de casos relacionados con el delito de fraude mediante el uso de IA en empresas de servicios, basados en la evidencia de la investigación documentada, asimismo, mediante un futuro desarrollo de herramientas y técnicas especializadas, se abarco los desafíos de detección y prevención sobre los fraudes informáticos, disminuyendo el impacto significativo en las empresas y la sociedad en general.

1.7.3. Importancia

La importancia de esta investigación radicó en el impacto social que genera, debido a que la rápida evolución de la tecnología de IA plantea desafíos significativos para las empresas que emplean el uso de la IA y desconocen la manera de protegerse ante casos de fraudes informáticos. Si bien existen leyes y regulaciones ante estos casos estas pueden no ser suficientes para abordar adecuadamente estos nuevos tipos de delitos, lo que se requiero un enfoque proactivo y colaborativo entre los gobiernos, las empresas y otros actores relevantes, por ello debido al aumento de los casos de fraude mediante el uso de IA se destacó la necesidad de implementar medidas regulatorias efectivas y

estrategias de prevención para proteger a las empresas de servicios y a los consumidores. Por ello abordar esta problemática de manera efectiva fue crucial para proteger los intereses de las empresas, los consumidores y la sociedad en su conjunto.

CAPITULO II

MARCO TEÓRICO

2.1. Antecedentes jurídicos del problema

2.1.1. Antecedentes Internacionales

Moreno et al. (2023), en su estudio titulado “La inteligencia artificial como herramienta para la detección del fraude fiscal: Caso Colombia”, exploraron cómo el uso de sistemas de inteligencia artificial mejora la detección de fraudes fiscales. Aplicando una metodología documental y analítica, concluyeron que tecnologías como el sistema Aranda Query Manager (AQM) y los algoritmos de aprendizaje automático no supervisado lograron una precisión del 98%. Esta efectividad permitió a las autoridades fiscales reducir la evasión tributaria y fortalecer la sostenibilidad financiera. El estudio destaca el valor de la IA como instrumento técnico en la lucha contra delitos económicos, subrayando su potencial para optimizar la gestión pública tributaria y anticiparse a patrones fraudulentos de difícil detección por métodos tradicionales.

Alcayaga et al. (2024), en su artículo “Integración de la inteligencia artificial en la administración fiscal: un análisis comparativo y multidimensional”, analizaron el uso de modelos de IA en sistemas tributarios de países de Europa y América Latina. A través de un enfoque cualitativo, concluyeron que el aprendizaje automático ofrece altos niveles de precisión en la detección de evasión fiscal. Sin embargo, esta eficiencia depende de variables críticas como la calidad de los datos, la contextualización normativa y la infraestructura institucional. Además, advierten que el éxito de estas tecnologías requiere políticas de actualización constante que acompañen el avance tecnológico. El estudio enfatiza la importancia de alinear los marcos legales y fiscales con el progreso de la inteligencia artificial.

Mojica (2021), en su tesis “Inteligencia artificial para detectar la corrupción en la administración pública municipal de Colombia”, estudió el uso de algoritmos de aprendizaje automático para detectar actos de corrupción en gobiernos locales. El análisis comparó técnicas de aprendizaje supervisado y no supervisado, destacando que este último fue más eficaz para identificar patrones irregulares sin necesidad de datos etiquetados. Mojica argumenta que estas tecnologías permiten mejorar los sistemas de control interno, anticipando comportamientos atípicos asociados con corrupción administrativa. La tesis concluye que la inteligencia artificial, correctamente implementada, puede convertirse en una herramienta estratégica de prevención institucional, capaz de incrementar la transparencia y fortalecer la rendición de cuentas en el ámbito público municipal.

Aldea (2020), en su investigación titulada “El impacto de la inteligencia artificial en el sistema financiero”, estudió el desarrollo de la inteligencia artificial en el ámbito bursátil y financiero. A través de una revisión documental, identificó el uso de tecnologías como redes neuronales, algoritmos genéticos y sistemas expertos, especialmente en aplicaciones como el “high-frequency trading” y la seguridad cibernética. Aunque algunas instituciones ya integran estas herramientas, su implementación no está ampliamente extendida. Aldea concluye que la IA puede ofrecer una ventaja competitiva en mercados financieros altamente digitalizados, siempre que exista infraestructura tecnológica, formación profesional adecuada y legislación clara. Su estudio refuerza la urgencia de preparar marcos normativos acordes a los nuevos entornos digitales financieros.

2.1.2. Antecedentes Nacionales

Rayo (2022), en su tesis titulada “Prototipo de detección de fraudes con tarjetas de crédito basado en inteligencia artificial aplicado a un banco peruano”, planteó como objetivo diseñar una plataforma web para la detección en tiempo real de fraudes financieros mediante inteligencia artificial. Aplicando la metodología Design Thinking, el estudio evidenció que el modelo desarrollado alcanzó una precisión del 48.10% y un índice de falsos positivos de 4.35. A pesar de estas cifras, se consideró que el sistema es prometedor y podría mejorar conforme aumente el volumen de datos. El autor concluye que la implementación de IA, incluso en fases tempranas, puede ofrecer soluciones efectivas para reducir fraudes en el sector financiero, contribuyendo a la transformación digital de la banca peruana.

Villegas (2021), en su tesis “Modelo de machine learning en la detección de sitios web phishing”, desarrolló un sistema basado en aprendizaje automático para identificar sitios web fraudulentos. La investigación combinó enfoques cuantitativos y cualitativos, alcanzando una precisión promedio del 93.80% y una tasa de clasificación correcta del 91.20% para sitios falsos. Además, logró un 95.35% de precisión al identificar sitios legítimos. Estos resultados muestran que los modelos de IA pueden aplicarse eficazmente en la ciberseguridad, especialmente en la prevención de delitos informáticos como el phishing. Villegas concluye que el uso de algoritmos predictivos es una estrategia viable para combatir amenazas digitales y proteger a los usuarios en línea.

Chuco (2023), en su tesis titulada “Análisis del delito de fraude informático y hurto como delito previo, Cercado de Lima-2020”, examinó la relación jurídica entre el fraude informático y el hurto. Utilizando una metodología cualitativa de tipo descriptiva, concluyó que el fraude informático puede considerarse una modalidad

de hurto cuando implica la apropiación ilícita de bienes patrimoniales mediante el uso de sistemas informáticos. Asimismo, sostuvo que el acceso ilícito constituye un delito previo dentro del marco del fraude informático. El estudio evidenció la necesidad de una mayor precisión normativa para diferenciar estos delitos en el sistema penal peruano, con el fin de mejorar la imputación y sanción en casos relacionados con cibercriminalidad.

Parde (2018), en su tesis “Tratamiento jurídico penal informáticos contra el patrimonio, distrito judicial de Lima, 2018”, investigó la normativa penal aplicada a los delitos informáticos patrimoniales. Aplicando una metodología cualitativa con enfoque descriptivo-explicativo, concluyó que el tratamiento legal vigente es insuficiente. Sostuvo que el Código Penal agrupa inadecuadamente diversas modalidades de fraude informático bajo una misma figura, generando vacíos interpretativos que dificultan la sanción efectiva. El autor enfatiza la urgencia de reformar el marco jurídico, adaptándolo a las nuevas formas de criminalidad digital y dotando a los operadores de justicia de herramientas más específicas para enfrentar el delito informático en el contexto peruano.

Cajigas y Pérez (2023), en su tesis “La incidencia de las nuevas tecnologías en el delito de fraude informático y su aplicación en la Ley N.º 30096 en el Perú”, analizaron la adecuación normativa frente a la evolución tecnológica. Con un enfoque cualitativo y diseño descriptivo, concluyeron que la Ley N.º 30096 presenta una tipificación genérica del delito de fraude informático que no se ajusta a las actuales modalidades delictivas como el phishing o el carding. Se identificó un incremento en las denuncias por estas prácticas, lo que evidencia la necesidad de actualizar la ley para abordar con mayor precisión los delitos tecnológicos. La

investigación propone una reforma normativa que incorpore estas nuevas formas de fraude para fortalecer el sistema de persecución penal en el país.

2.1.3. Antecedentes Locales

Cataño y Panduro (2023) en su tesis titulada "*El delito informático y su incidencia en las operaciones financieras en los bancos de la provincia Coronel Portillo- Ucayali, 2022*", tuvo como objetivo determinar como el delito de información incide en las operaciones financieras en los bancos de la provincia de Coronel Portillo. La investigación fue cuantitativa, con diseño no experimental y de nivel correlacional. Como resultado se tuvo un nivel de confiabilidad del 95% con un Rho de Spearman 0.756. por lo tanto se concluyó que existe correlación positiva fuerte entre el delito informático y las operaciones financieras.

2.2. Bases Teóricas

2.2.1. Variable 1: Inteligencia artificial

La inteligencia artificial (IA) ha dejado de ser un concepto propio de la ciencia ficción para convertirse en un componente esencial de múltiples disciplinas, incluido el Derecho. Su integración en el ámbito jurídico está transformando la forma en que se gestiona la información, se analizan los casos y se toman decisiones. Ramos (2024) señala que, en el contexto societario, la IA puede suministrar datos y patrones que permiten a los administradores identificar riesgos y cumplir con el deber de diligencia, evidenciando cómo las herramientas algorítmicas ofrecen una base empírica que complementa la labor jurídica. En el sector financiero, Lado Chaviano y González Abreu (2022) demuestran que el uso de técnicas de aprendizaje automático facilita la detección automatizada de fraudes en

transacciones bancarias, destacando la importancia de procesar grandes volúmenes de datos en tiempo real para proteger los intereses de usuarios y entidades. Asimismo, la Guía sobre IA y ciberseguridad elaborada por Pérez et al. (2024) resalta que estas tecnologías permiten detectar comportamientos anómalos con mayor precisión y rapidez, reduciendo los falsos positivos y fortaleciendo la respuesta ante incidentes. En paralelo, el Banco de México (2025) subraya que la IA tiene el potencial de automatizar procesos rutinarios, disminuir costos y ampliar la capacidad de análisis de información, lo que incrementa la eficiencia operativa de las instituciones públicas y privadas. Por su parte, Benítez Palma y García Rodríguez (2024) evidencian cómo la IA generativa se aplica en la contratación pública para detectar prácticas irregulares y fortalecer la transparencia. Todos estos trabajos muestran la creciente relevancia de la IA en el Derecho y exponen tanto sus oportunidades como sus riesgos.

A partir de este contexto, los objetivos de la presente investigación son: (1) analizar cómo la IA contribuye a la detección de patrones anómalos en ámbitos jurídicos, incluyendo fraude financiero y corrupción; (2) examinar las técnicas y prácticas que garantizan la seguridad en transacciones digitales y la integridad de los datos; y (3) evaluar el impacto de la IA en la eficiencia operativa de instituciones legales, gubernamentales y financieras. Además, se plantean interrogantes sobre la regulación y la ética de la IA, como la necesidad de marcos de gobernanza que aseguren la transparencia y la rendición de cuentas (Banco de México, 2025).

La metodología general combinará un estudio bibliográfico –que revisará literatura científica y normativa relevante– y un análisis de casos. Se utilizarán métodos cualitativos para examinar textos legales, doctrinales y jurisprudencia, y se aplicarán criterios de análisis comparado para estudiar experiencias en diferentes

jurisdicciones. Asimismo, se incluirá un análisis de riesgos y beneficios, considerando la opinión de expertos y organismos regulatorios sobre la adopción de IA en el Derecho (Pérez et al., 2024). Esta aproximación permitirá no sólo describir las aplicaciones actuales de la IA, sino también proponer recomendaciones para su implementación responsable en el ámbito jurídico.

Definición de Inteligencia Artificial

La inteligencia artificial se refiere a la capacidad de los sistemas informáticos para realizar tareas que normalmente requieren inteligencia humana, como el aprendizaje, el razonamiento, la percepción y la toma de decisiones. De acuerdo con el Banco de México (2025), la IA engloba sistemas capaces de generar contenido, funcionar como asistentes de programación, optimizar procesos rutinarios y aumentar la capacidad de procesamiento y análisis de grandes volúmenes de datos. Estas tareas se logran mediante algoritmos y modelos matemáticos que permiten a las máquinas aprender a partir de los datos y mejorar su rendimiento con el tiempo, replicando o incluso superando ciertas capacidades cognitivas humanas. Desde un enfoque más jurídico, Ramos (2024) considera que la IA actúa como una herramienta tecnológica que ofrece información basada en datos, patrones y estadísticas para apoyar la toma de decisiones en el entorno societario. Este enfoque destaca la IA como un mecanismo de soporte que facilita la identificación de riesgos y anomalías en la gestión empresarial.

La IA abarca diferentes subcampos, como el aprendizaje automático (machine learning), la visión por computador, el procesamiento de lenguaje natural y los sistemas expertos. El aprendizaje automático permite que los sistemas aprendan patrones a partir de ejemplos y tomen decisiones sin ser programados

explícitamente. Lado Chaviano y González Abreu (2022) utilizan esta capacidad para detectar fraudes en transacciones bancarias en tiempo real, demostrando que la IA puede identificar anomalías y prevenir delitos financieros. La visión por computador, por su parte, se aplica para el reconocimiento facial y la verificación biométrica; Pérez, Lázaro, Rodríguez, Galán y Ureña (2024) señalan que los algoritmos pueden detectar manipulaciones como deepfakes y generar alertas de actividad sospechosa. El procesamiento de lenguaje natural se emplea para analizar textos legales, identificar cláusulas de riesgo y extraer información de contratos. Finalmente, los sistemas expertos son programas basados en reglas que reproducen el razonamiento humano en ámbitos específicos, como la asistencia en juicios o la evaluación de casos.

La inteligencia artificial es un conjunto de tecnologías que permiten a las máquinas ejecutar funciones que antes solo podía realizar el ser humano. Su relevancia en el Derecho radica en su capacidad para procesar y analizar grandes volúmenes de datos con rapidez y precisión, transformando la práctica jurídica y empresarial. Al definir la IA de esta manera, se establece la base sobre la cual se desarrollan las siguientes secciones de esta investigación, que exploran su evolución, beneficios y riesgos.

Evolución de la IA en el ámbito jurídico y societario

La aplicación de la inteligencia artificial en el ámbito jurídico ha seguido una evolución marcada por avances tecnológicos y cambios en las necesidades institucionales. Los primeros sistemas utilizados en el derecho fueron los llamados sistemas expertos, basados en reglas codificadas por juristas y programadores para emular la capacidad de asesoría jurídica. Con el desarrollo del aprendizaje

automático y el aumento de la capacidad computacional, la IA ha trascendido estos sistemas, permitiendo procesar datos en volúmenes y velocidades imposibles para el ser humano. Ramos (2024) destaca que esta transición ha permitido que la IA actúe como un mecanismo de soporte en la gobernanza empresarial, facilitando la detección de riesgos y la optimización de la toma de decisiones en consejos de administración.

La evolución de la IA jurídica no se limita a la asesoría corporativa. En el ámbito público, la IA se ha utilizado para identificar patrones de fraude y corrupción. Benítez Palma y García Rodríguez (2024) explican que herramientas agrupadas bajo el acrónimo AI-ACT (Artificial Intelligence – Anti Corruption Tools) se han implementado para analizar datos de contratación pública y detectar irregularidades de colusión. Estas herramientas permiten examinar licitaciones y contratos con un nivel de detalle que sería inviable sin asistencia tecnológica, evidenciando un salto cualitativo en la lucha contra la corrupción. La misma tendencia se observa en los sistemas judiciales, donde algoritmos de IA ayudan a clasificar expedientes, predecir tiempos procesales y analizar jurisprudencia para asistir a jueces y abogados.

En el sector financiero, la evolución ha sido igualmente significativa. Lado Chaviano y González Abreu (2022) documentan cómo las instituciones bancarias han adoptado modelos de aprendizaje automático para detectar fraudes en transacciones en tiempo real, aprovechando la IA para analizar millones de operaciones y diferenciar patrones normales de comportamientos sospechosos. Asimismo, el Banco de México (2025) subraya que los bancos centrales están utilizando la IA para optimizar procesos internos, generar contenidos y realizar análisis económicos más complejos.

Esta evolución ha estado acompañada por avances en la regulación y en la conciencia pública sobre los riesgos y beneficios de la IA. Pérez et al. (2024) destacan la necesidad de desarrollar marcos de gestión de riesgos y de ciberseguridad que acompañen la implementación de soluciones de IA en ámbitos críticos. La literatura reciente también subraya la importancia de la transparencia y la rendición de cuentas en los algoritmos aplicados al Derecho. En consecuencia, la evolución de la IA jurídica y societaria ha sido un proceso dinámico en el que la tecnología se adapta para satisfacer las exigencias de un entorno legal cada vez más complejo, al tiempo que surgen debates sobre ética, legalidad y responsabilidad.

Beneficios y riesgos de la IA en la práctica legal

La adopción de la inteligencia artificial en la práctica legal genera numerosos beneficios que impactan tanto en la eficiencia como en la calidad de los servicios jurídicos. Uno de los principales beneficios es la capacidad de la IA para procesar grandes volúmenes de datos, permitiendo identificar patrones y comportamientos anómalos de manera más precisa y rápida que los métodos tradicionales. Pérez et al. (2024) señalan que los algoritmos de aprendizaje automático reducen los falsos positivos y negativos en los sistemas de seguridad, mejorando la detección de amenazas y la respuesta ante incidentes. En la gestión corporativa, Ramos (2024) destaca que la IA proporciona información detallada que ayuda a los administradores a cumplir con sus deberes fiduciarios y a detectar conductas irregulares.

Otro beneficio significativo es la automatización de procesos. El Banco de México (2025) indica que la IA puede optimizar la ejecución de tareas rutinarias, reducir

costos y ampliar la capacidad de análisis, aumentando la eficiencia operativa en instituciones financieras y regulatorias. Esta automatización no solo agiliza trámites, sino que libera a los profesionales del Derecho para enfocarse en actividades de mayor valor añadido, como la estrategia y la argumentación jurídica. Además, la IA contribuye a la transparencia y a la lucha contra la corrupción. Benítez Palma y García Rodríguez (2024) demuestran que la combinación de datos de contratación pública y algoritmos de IA permite identificar irregularidades y mejorar la supervisión en licitaciones.

Sin embargo, el uso de IA en la práctica legal no está exento de riesgos. Uno de los principales desafíos es la opacidad de algunos modelos, que pueden generar decisiones difíciles de explicar. El Banco de México (2025) advierte que la falta de transparencia puede conducir a conclusiones erróneas y crear riesgos reputacionales. También existe el riesgo de sesgos en los algoritmos, que podrían perpetuar o amplificar desigualdades, especialmente si los datos de entrenamiento reflejan discriminaciones históricas. La Guía del ISMS Forum subraya la importancia de la supervisión humana y el uso de conjuntos de datos diversos para mitigar estos sesgos (Pérez et al., 2024). Otro riesgo es la externalización de la responsabilidad: en el ámbito público, depender de proveedores externos de IA podría llevar a que las instituciones deleguen la lucha contra la corrupción, lo que plantea dilemas éticos y legales (Benítez Palma & García Rodríguez, 2024).

Adicionalmente, la adopción de IA incrementa los riesgos de ciberseguridad. Los sistemas que procesan datos sensibles están expuestos a vulnerabilidades que pueden ser explotadas por actores maliciosos. Por ello, es crucial implementar medidas de protección y marcos de gobernanza que aseguren la confidencialidad, integridad y disponibilidad de la información (Pérez et al., 2024). Finalmente, la

integración de la IA exige inversiones en infraestructura tecnológica y formación del personal, lo que puede ser un reto para organizaciones con recursos limitados.

En conclusión, la IA ofrece oportunidades significativas para transformar la práctica legal, pero su implementación debe ir acompañada de mecanismos de supervisión, transparencia y gestión de riesgos. Solo así se podrá aprovechar su potencial para mejorar la justicia y la eficiencia sin comprometer la ética ni los derechos fundamentales.

Dimensión Detección de patrones anómalos

Fundamentos de la detección de anomalías y su relevancia jurídica

La detección de patrones anómalos se basa en identificar observaciones que se desvían significativamente del comportamiento esperado en un conjunto de datos. Estas desviaciones pueden indicar errores, fraudes o actividades irregulares que requieren atención inmediata. En el ámbito jurídico, esta capacidad resulta esencial para prevenir delitos financieros, evaluar riesgos regulatorios y garantizar la transparencia de las transacciones. Pérez, Lázaro, Rodríguez, Galán y Ureña (2024) subrayan que los algoritmos de IA están diseñados para analizar grandes volúmenes de datos en tiempo real, aprender patrones de comportamiento normal y generar alertas cuando se detectan anomalías. Este enfoque permite adelantarse a posibles irregularidades y mejorar la efectividad de los mecanismos de cumplimiento normativo. La relevancia jurídica radica en que estas herramientas apoyan la labor de jueces, auditores y reguladores al proporcionar evidencia objetiva basada en datos y minimizar la discrecionalidad humana.

Aplicaciones en el derecho societario y la gobernanza empresarial

En el contexto de la gobernanza empresarial, la inteligencia artificial se utiliza para analizar registros contables, transacciones y comunicaciones internas con el fin de detectar comportamientos sospechosos o indicios de mala praxis. Ramos (2024) señala que las herramientas de IA ayudan a los administradores a cumplir con su deber de diligencia, proporcionando datos y estadísticas que facilitan la identificación temprana de riesgos y la toma de decisiones informadas. Estas tecnologías permiten establecer indicadores de alerta que advierten sobre posibles fraudes, conflictos de interés o incumplimientos de políticas internas. Además, la IA mejora los procesos de auditoría interna al automatizar el análisis de datos financieros, reduciendo la posibilidad de que se escapen anomalías significativas. La implementación de estas soluciones refuerza la confianza de los accionistas y contribuye a una cultura de cumplimiento y transparencia dentro de las organizaciones.

Casos de uso en fraude y corrupción en contratación pública

La IA también se aplica en la lucha contra la corrupción y el fraude en la contratación pública. Benítez Palma y García Rodríguez (2024) analizan cómo las herramientas anticorrupción basadas en IA permiten detectar colusión entre licitadores y prácticas irregulares. Al combinar bases de datos públicas con técnicas estadísticas avanzadas, la IA puede revelar patrones que sugieren acuerdos ilegales, sobreprecios o distribución anómala de contratos. Este tipo de análisis resulta invaluable para las agencias anticorrupción y organismos de control, ya que automatiza la vigilancia y permite actuar con rapidez ante posibles irregularidades. Los autores destacan que la combinación de información abundante, mayor

capacidad de cómputo y métodos analíticos sofisticados crea un entorno propicio para combatir la corrupción, incluso en países donde el acceso a datos era limitado. La IA, por tanto, se convierte en una aliada estratégica para mejorar la transparencia y la eficiencia en el gasto público.

Modelos y algoritmos

Para detectar anomalías se emplean tanto algoritmos de aprendizaje supervisado como no supervisado. Entre los supervisados destacan el bosque aleatorio (random forest), los árboles de decisión y los modelos de regresión logística, que se entrenan con datos etiquetados para distinguir entre comportamientos normales y fraudulentos. Lado Chaviano y González Abreu (2022) comparan diversos modelos supervisados en la detección de fraude bancario y concluyen que la elección del algoritmo depende del equilibrio entre precisión y eficiencia computacional. Por otro lado, en ausencia de etiquetas, los algoritmos no supervisados como el aislamiento forest, k-means o los modelos de densidad identifican puntos atípicos mediante el análisis de la distribución de los datos. La metodología KDD (Knowledge Discovery in Databases) guía la selección, limpieza y transformación de los datos antes de aplicar estos modelos, asegurando que la información sea adecuada para el análisis. Un análisis comparativo de rendimiento permite elegir el modelo más eficaz según la tasa de detección y los falsos positivos.

Desafíos y limitaciones

A pesar de sus beneficios, la detección de anomalías enfrenta varios desafíos. Uno de los principales es la gestión de falsos positivos y falsos negativos: un exceso de alertas erróneas puede saturar a los analistas y disminuir la confianza en el sistema,

mientras que una detección insuficiente puede permitir que las anomalías pasen desapercibidas. Pérez et al. (2024) subrayan la necesidad de entrenar los modelos con conjuntos de datos exhaustivos y diversos para reducir estos errores. Otro desafío es la calidad de los datos; los algoritmos requieren información precisa y actualizada para aprender patrones fiables, por lo que es imprescindible contar con procesos de limpieza y normalización de datos. La supervisión humana sigue siendo crucial, ya que los expertos jurídicos deben validar las alertas y contextualizar los hallazgos. Finalmente, aspectos éticos como la privacidad y el sesgo algorítmico deben ser gestionados mediante políticas claras y marcos de responsabilidad, garantizando que las herramientas de IA respeten los derechos fundamentales y no perpetúen discriminaciones.

Dimensión Seguridad en las transacciones

Fundamentos de la seguridad en transacciones digitales

La seguridad en las transacciones digitales se sustenta en principios de confidencialidad, integridad y disponibilidad, así como en normativas que regulan el tratamiento de los datos personales y financieros. Las regulaciones como el Reglamento General de Protección de Datos (RGPD) en la Unión Europea y la Ley de Protección de Datos Personales en las jurisdicciones latinoamericanas establecen obligaciones para las entidades que manejan información sensible, imponiendo medidas técnicas y organizativas para proteger los datos frente a accesos no autorizados. Además, las leyes de servicios de pago y las directivas de seguridad de redes y sistemas de información exigen que las transacciones electrónicas se procesen de forma segura y que se implementen controles de autenticación reforzada. En este contexto normativo, la inteligencia artificial se

integra como una herramienta de apoyo que permite cumplir con los requisitos de protección de datos al detectar y prevenir incidentes de seguridad con mayor rapidez y precisión.

Detección de fraudes en transacciones bancarias

El crecimiento de las operaciones digitales en el sector financiero ha incrementado el riesgo de fraudes electrónicos. Lado Chaviano y González Abreu (2022) desarrollan un método de detección automatizada de anomalías en transacciones bancarias mediante tecnologías de procesamiento distribuido. Su propuesta aborda desafíos como el enorme volumen de operaciones diarias, la desproporción entre transacciones legítimas y fraudulentas y la necesidad de respuestas en tiempo real. Los autores aplican algoritmos de aprendizaje automático que analizan patrones de comportamiento y diferencias sutiles entre transacciones normales y sospechosas, permitiendo generar alertas inmediatas para bloquear o investigar operaciones irregulares. Esta aproximación se alinea con las políticas de “conozca a su cliente” y de prevención de lavado de activos, que requieren vigilancia continua y análisis de riesgos basados en datos.

Inteligencia artificial en la ciberseguridad y protección de datos

La IA ha impulsado avances significativos en la ciberseguridad. En el ámbito biométrico, los algoritmos de visión por computador pueden detectar deepfakes y manipulaciones en huellas digitales o reconocimiento facial, generando alertas ante posibles intentos de suplantación. Pérez, Lázaro, Rodríguez, Galán y Ureña (2024) explican que estos algoritmos analizan grandes volúmenes de datos biométricos para identificar patrones inusuales y detectar ataques de falsificación. Además, los

sistemas de IA aprenden el comportamiento normal de redes y usuarios; mediante técnicas de aprendizaje automático supervisado y no supervisado pueden reconocer desviaciones que podrían indicar ataques de phishing, malware o accesos no autorizados. Estas capacidades complementan las medidas tradicionales de seguridad, como los cortafuegos y el cifrado, proporcionando una capa adicional de protección adaptativa. Al mismo tiempo, es necesario implementar medidas de privacidad desde el diseño (privacy by design) para garantizar que los sistemas de IA no vulneren la confidencialidad de los datos personales.

Supervisión, auditoría y responsabilidad

La supervisión y la auditoría son elementos esenciales para garantizar que la inteligencia artificial se utilice de forma ética y legal en la seguridad de las transacciones. Benítez Palma y García Rodríguez (2024) señalan que la IA permite mejorar la transparencia al monitorizar en tiempo real las operaciones y detectar prácticas irregulares. No obstante, advierten que es crucial mantener la responsabilidad institucional y no delegar totalmente la función de control en proveedores externos de IA. Las instituciones financieras y las agencias reguladoras deben establecer marcos de gobernanza que incluyan auditorías periódicas de los algoritmos, explicabilidad de los modelos y procedimientos para la revisión humana de las alertas generadas. Asimismo, deben adoptarse políticas claras sobre la asignación de responsabilidades en caso de fallos o decisiones erróneas derivadas del uso de sistemas automatizados. La rendición de cuentas y la trazabilidad de las decisiones son imprescindibles para mantener la confianza de los usuarios y cumplir con las obligaciones legales.

Dimensión Eficiencia operativa

Inteligencia artificial como herramienta de optimización

La inteligencia artificial ha demostrado ser una aliada estratégica para optimizar procesos en ámbitos financieros y regulatorios. Su capacidad para automatizar tareas rutinarias permite liberar recursos humanos y reducir costos operativos. El Banco de México (2025) explica que las herramientas de IA pueden generar reportes, elaborar resúmenes y asistir en la programación, optimizando y automatizando la ejecución de procesos, lo que se traduce en mayor eficiencia operativa y una mejor utilización del tiempo y los recursos. Además, la IA amplía significativamente la capacidad de análisis de grandes volúmenes de datos, permitiendo identificar patrones complejos y tendencias que resultarían invisibles con métodos manuales. En contextos regulatorios, esta capacidad es fundamental para evaluar riesgos sistémicos, vigilar el cumplimiento normativo y diseñar estrategias preventivas basadas en evidencia.

Inteligencia artificial en organismos reguladores y bancarios

Los organismos reguladores y los bancos centrales han adoptado la inteligencia artificial para fortalecer sus funciones operativas y analíticas. Uno de los casos de uso más importantes es la generación de alertas tempranas sobre riesgos y vulnerabilidades en el sistema financiero. Según el Banco de México (2025), la IA complementa y potencia las herramientas existentes para la detección temprana de riesgos mediante el seguimiento de tendencias en distintos canales y la construcción de mecanismos de alerta en tiempo real. Estas alertas permiten a las autoridades actuar de manera proactiva ante posibles crisis y asegurar la estabilidad financiera. Otro uso innovador es la generación de datos sintéticos para

entrenar modelos sin exponer información confidencial. El mismo informe señala que los bancos centrales y otros organismos emplean datos sintéticos para ampliar los conjuntos de entrenamiento y proteger la privacidad, permitiendo desarrollar modelos robustos sin comprometer la seguridad de los datos sensibles.

Aplicaciones en la gestión judicial y administrativa

En el ámbito judicial y administrativo, la inteligencia artificial se está utilizando para automatizar tareas repetitivas y agilizar la gestión de expedientes. Aunque la literatura específica es aún incipiente, las aplicaciones más destacadas incluyen la clasificación automática de documentos, la asignación de turnos judiciales y la generación de borradores de resoluciones. Estas herramientas reducen los tiempos procesales y mejoran la calidad del servicio al permitir que jueces y abogados se concentren en aspectos sustantivos del análisis jurídico. Ramos (2024) destaca que la IA puede proporcionar información detallada y especializada que ayuda a los operadores jurídicos a tomar decisiones más asertivas y eficientes, lo que repercute en una mejora de la administración de justicia y un aumento de la confianza pública en el sistema.

Riesgos operativos y sostenibilidad

A pesar de los beneficios operativos, la adopción de IA plantea desafíos significativos en términos de infraestructura tecnológica y sostenibilidad. El Banco de México (2025) advierte que la integración de nuevas tecnologías requiere inversiones en infraestructura de tecnologías de la información y comunicaciones, así como en la capacitación del personal para asegurar un uso adecuado de las herramientas. Además, los modelos de IA pueden ser opacos, lo que genera

riesgos reputacionales si las decisiones automatizadas resultan erróneas o difíciles de explicar. Pérez, Lázaro, Rodríguez, Galán y Ureña (2024) subrayan la importancia de la transparencia y la supervisión humana para mitigar estos riesgos y garantizar que las soluciones de IA operen bajo principios éticos y legales. Asimismo, el consumo energético y los requisitos computacionales de algunos modelos pueden ser elevados, planteando desafíos de sostenibilidad y eficiencia energética. Para abordar estos riesgos, las organizaciones deben implementar marcos de gobernanza claros, evaluar la eficiencia energética de sus soluciones y fomentar una cultura de capacitación continua que permita a los empleados adaptarse a la rápida evolución tecnológica.

Implicaciones éticas y legales

La adopción de inteligencia artificial en el ámbito jurídico y financiero plantea importantes retos éticos y legales que deben abordarse para garantizar un uso responsable de la tecnología. En primer lugar, los principios de una IA responsable exigen que las soluciones desarrolladas se alineen con valores éticos y normas legales. El Banco de México (2025) señala que todas las herramientas que integran IA deben operar bajo principios legales, morales y éticos para evitar efectos negativos sobre la protección del consumidor y la estabilidad financiera. Esto implica, por ejemplo, que los modelos de IA no solo persigan la eficiencia, sino que también respeten los derechos fundamentales y eviten daños a las personas o grupos afectados por sus decisiones. La “alineación de valores” descrita en el informe se refiere a que la IA debe ajustarse a las preferencias y principios humanos, evitando conductas que puedan considerarse inmorales o ilegales.

En segundo lugar, la gobernanza de algoritmos es esencial para asegurar la transparencia y la explicabilidad de las decisiones automatizadas. Pérez, Lázaro, Rodríguez, Galán y Ureña (2024) recomiendan implementar marcos de gestión de riesgos y auditorías periódicas para evaluar el comportamiento de los modelos y garantizar que operen conforme a las normas y expectativas sociales. La gobernanza incluye establecer quién es responsable de las decisiones tomadas por los sistemas de IA y cómo se puede revisar y corregir su funcionamiento en caso de errores. La transparencia implica documentar el diseño y el entrenamiento de los modelos, así como informar a los usuarios sobre su funcionamiento. La explicabilidad, por su parte, busca que las decisiones generadas por la IA puedan ser comprendidas y justificadas ante las partes interesadas, algo fundamental en procesos judiciales y administrativos donde la rendición de cuentas es vital.

La implementación de IA debe proteger los derechos fundamentales y abordar los riesgos de sesgo y discriminación. Ramos (2024) subraya que, aunque la IA ofrece herramientas valiosas para la toma de decisiones, su uso debe estar sujeto a controles que eviten vulneraciones de derechos. Los algoritmos pueden heredar o amplificar sesgos presentes en los datos de entrenamiento, lo que puede conducir a decisiones discriminatorias, especialmente en ámbitos sensibles como el acceso al crédito o la justicia. Para mitigar estos riesgos, es imprescindible utilizar conjuntos de datos representativos y aplicar técnicas de mitigación de sesgos, así como mantener la supervisión humana en los procesos críticos. También es necesario garantizar que la recolección y el tratamiento de datos cumplan con las leyes de protección de datos y privacidad, asegurando que la información personal se utilice de manera legítima y con el consentimiento adecuado. En conjunto, estos principios éticos y legales son fundamentales para consolidar la confianza en el uso de la IA

y promover una adopción responsable que beneficie a la sociedad sin comprometer los derechos individuales.

Propuesta de implementación en el sistema jurídico peruano

La incorporación de la inteligencia artificial en el sistema jurídico peruano requiere una estrategia integral que combine reformas normativas, políticas públicas y medidas institucionales. En primer lugar, el marco legal debe adaptarse para reconocer formalmente el uso de herramientas de IA y establecer límites y responsabilidades claras. Ramos (2024) subraya la importancia de que los administradores cumplan con su deber de diligencia cuando utilizan tecnologías de IA; esto implica que las leyes societarias y regulatorias deberían establecer obligaciones específicas para la supervisión y el control de los sistemas automatizados. Asimismo, es necesario modificar normativas de protección de datos y privacidad para asegurar que los modelos de IA respeten la confidencialidad de la información y cuenten con mecanismos de consentimiento informado y de evaluación de impacto en la privacidad.

En términos de políticas públicas, se recomienda desarrollar lineamientos nacionales sobre IA que incluyan principios de transparencia, explicabilidad y responsabilidad. El Banco de México (2025) enfatiza la necesidad de contar con marcos de gestión de riesgos y gobernanza para el uso de IA; inspirándose en estas directrices, el Perú podría establecer estándares para la elaboración, implementación y supervisión de algoritmos en sectores clave como justicia, finanzas y salud. Estos estándares deberían incluir auditorías periódicas, certificación de sistemas de IA y formación especializada para funcionarios públicos y operadores jurídicos. También es fundamental promover la investigación y el

desarrollo de soluciones locales que se ajusten al contexto socioeconómico del país y eviten la dependencia excesiva de proveedores extranjeros.

Para la adopción en entidades públicas y privadas, es vital considerar la capacidad institucional y la preparación tecnológica. Las instituciones deben evaluar su infraestructura y dotarse de recursos tecnológicos y humanos adecuados. Según Pérez, Lázaro, Rodríguez, Galán y Ureña (2024), la capacitación del personal y la supervisión humana son esenciales para garantizar un uso seguro y eficaz de la IA. En las entidades públicas, la implementación debe ser gradual y priorizar áreas donde la IA pueda aportar mayor valor, como la gestión de expedientes judiciales o la detección de fraudes en licitaciones. En el sector privado, las empresas deben integrar la IA en sus sistemas de gobernanza y cumplimiento, asegurando que la automatización no comprometa la ética ni los derechos de los usuarios. En todos los casos, se recomienda adoptar políticas de "IA responsable", implementando salvaguardias contra sesgos y estableciendo canales de consulta y revisión para las decisiones automatizadas. De esta manera, el sistema jurídico peruano y otras jurisdicciones podrán aprovechar los beneficios de la inteligencia artificial mientras protegen los principios fundamentales de justicia y equidad.

2.2.2. Variable 2: Delito de fraude.

Según Mayer y Oliver (2020) el delito fraude "Implica cualquier actividad que viole la seguridad cibernética, ya sea a través de la intrusión en sistemas informáticos, la interceptación de comunicaciones electrónicas o el robo de información personal o financiera" (p.160).

Según Díaz, Angulo y Barboza (2018) el delito de fraude se refiere "A cualquier actividad fraudulenta que se lleva a cabo utilizando medios informáticos

o electrónicos. Este tipo de fraude implica el uso indebido de la tecnología de la información y las comunicaciones para cometer delitos con el fin de obtener beneficios financieros, obtener información confidencial, dañar sistemas informáticos o causar perjuicio a individuos u organizaciones" (p.12).

Delito de fraude

El **fraude digital** constituye una forma de engaño ejecutada mediante herramientas tecnológicas con el fin de obtener beneficios económicos ilícitos, comprometiendo la seguridad de personas naturales, jurídicas y del propio Estado. En el entorno global, organismos como la ONU y el Consejo de Europa han desarrollado tratados como el *Convenio de Budapest sobre Ciberdelincuencia*, que se ha convertido en el principal instrumento internacional para combatir este tipo de delitos (Council of Europe, 2024). En el Perú, este fenómeno se encuentra tipificado en el Título X del Código Penal, referido a los delitos informáticos, incorporado mediante la Ley N.º 30096 y actualizado por la Ley N.º 31815 (Congreso de la República del Perú, 2023).

La **inteligencia artificial (IA)**, entendida como el conjunto de sistemas informáticos capaces de imitar procesos cognitivos humanos, está presente en sectores como el financiero, logístico y judicial. Sin embargo, su uso delictivo ha incrementado el riesgo de fraudes altamente sofisticados, como el uso de *deepfakes* para suplantar identidades, generar documentos apócrifos y realizar estafas automatizadas a gran escala (Papasavva et al., 2024). En Perú, si bien la IA aún no cuenta con una regulación específica, el Proyecto de Ley N.º 8133/2023-CR propone un marco normativo orientado a la ética, transparencia y responsabilidad civil en el uso de sistemas automatizados (PCM, 2024).

El **derecho comparado** evidencia un esfuerzo creciente por tipificar y sancionar los fraudes cometidos mediante IA. La Unión Europea, con el Reglamento (UE) 2024/1689 sobre Inteligencia Artificial, establece categorías de riesgo y prohíbe expresamente sistemas de IA utilizados para manipular o estafar (European Union, 2024). En Estados Unidos, algunos estados han penalizado el uso de voz sintética y deepfakes con fines delictivos (Shapiro, 2025).

Respecto a los **elementos típicos del fraude con IA**, se identifican tres fases: recolección de datos, suplantación automatizada y ejecución de la estafa. Estas fases complican la trazabilidad del delito y desafían los métodos tradicionales de investigación. Desde la **criminología**, se ha adaptado el "triángulo del fraude" de Cressey, integrando la automatización como una nueva variable que potencia la oportunidad y reduce el riesgo percibido del delito (Mazars, 2025).

El fraude mediante IA representa un desafío para el derecho penal moderno. Tanto en el campo internacional como en el derecho peruano, se observa un proceso de adaptación normativa que exige enfoques multidisciplinarios, regulación ética y cooperación interinstitucional para responder eficazmente a este nuevo tipo de criminalidad.

DIMENSIÓN CUMPLIMIENTO NORMATIVO

La **dimensión de cumplimiento normativo** frente al fraude mediante inteligencia artificial (IA) implica revisar el marco legal vigente y su adecuación a los desafíos tecnológicos. En el Perú, el Código Penal (Decreto Legislativo 635) y la Ley N.º 30096 sobre delitos informáticos constituyen los pilares normativos para sancionar conductas ilícitas cometidas mediante medios digitales. En 2025, se promulgó la Ley N.º 32314, que incorpora como agravante penal el uso de IA para

perpetrar delitos como estafa, suplantación, difamación o delitos sexuales, permitiendo al juez incrementar la pena hasta en un tercio del máximo previsto. Esta modificación refuerza el compromiso del Estado con la protección penal frente al uso indebido de tecnologías avanzadas (Perú, 2025; LP Derecho, 2025).

En el ámbito internacional, el **Convenio de Budapest** constituye el principal instrumento jurídico supranacional para combatir los ciberdelitos, promoviendo la cooperación entre países y la armonización legislativa. Además, organismos como la ONU, la OEA y la OCDE han desarrollado principios rectores para la gobernanza de la IA, recomendando a los Estados regular su uso de forma ética, transparente y proporcional. Estas directrices buscan evitar que la tecnología se convierta en un medio para violar derechos fundamentales.

En cuanto a la **regulación de la IA**, los principios de legalidad penal exigen normas claras, precisas y predecibles. En el Perú, el Proyecto de Ley N.º 7033/2023-CR busca establecer un marco normativo específico sobre inteligencia artificial, reconociendo doce aplicaciones sensibles de esta tecnología, entre ellas, el uso en bases de datos biométricos, la manipulación de emociones o la discriminación algorítmica.

Pese a estos avances, existen importantes **vacíos legales**. Hasta antes de la Ley N.º 32314, el uso de IA para cometer fraudes no estaba expresamente regulado. Muchas conductas se sancionaban de manera indirecta, sin tomar en cuenta el medio tecnológico empleado ni su capacidad de multiplicar el daño. Asimismo, persiste la necesidad de establecer criterios técnicos para determinar cuándo un sistema de IA ha sido utilizado de manera dolosa o negligente.

Respecto a la **responsabilidad penal**, la ley peruana ya contempla sanciones para personas naturales y jurídicas. Los desarrolladores o proveedores de sistemas IA

que faciliten la comisión de delitos pueden ser responsables penalmente si se acredita su participación dolosa o culposa.

Finalmente, las **propuestas normativas emergentes** apuntan a consolidar un régimen legal especializado. Entre ellas destacan los reglamentos derivados de la Ley N.º 32314 y nuevas iniciativas inspiradas en el modelo europeo, que clasifican los usos de IA por niveles de riesgo y establecen límites estrictos para aplicaciones peligrosas o invasivas.

DIMENSIÓN GRAVEDAD DEL FRAUDE

La **gravedad del fraude mediante inteligencia artificial (IA)** se evidencia por la diversidad, magnitud y sofisticación de los mecanismos utilizados para engañar a personas, empresas y entidades públicas. En cuanto a las **tipologías de fraude**, destacan los *deepfakes*, el *phishing* automatizado, la suplantación de identidad con voz clonada, las estafas masivas generadas por bots y los videos sintéticos utilizados para solicitar transferencias, acceder a cuentas o manipular información corporativa (Kurshan et al., 2024; Secureworld, 2025). Estas formas de fraude explotan la capacidad de la IA para imitar patrones humanos con alta fidelidad, superando los filtros tradicionales de seguridad.

El **impacto económico** es contundente. Solo durante el primer trimestre de 2025, los fraudes habilitados por IA causaron pérdidas globales por más de 200 millones de dólares, y se estima que la cifra anual superará los 900 millones (Security Magazine, 2025). En Estados Unidos, Deloitte (2025) reporta que las pérdidas por fraudes con IA podrían alcanzar los 40.000 millones de dólares para el año 2027. En Asia, especialmente en India, los fraudes cibernéticos han crecido en un 206 %

entre 2023 y 2024, alcanzando pérdidas de más de 22.800 millones de rupias (Times of India, 2025).

Las **repercusiones sociales y psicológicas** en las víctimas son graves y muchas veces invisibilizadas. Deepfakes empleados para difamación, chantaje o acoso provocan cuadros de ansiedad, depresión e incluso afectación de la vida profesional y familiar. En el Perú, se ha documentado el uso de videos falsos para engañar a ciudadanos con campañas de estafa en redes sociales, así como la manipulación de voces femeninas de periodistas para difundir fraudes financieros (Women Press Freedom, 2024). A nivel escolar, también se han registrado casos de *deepfake bullying* con graves consecuencias emocionales (Alexander, 2025).

En cuanto a la **casuística internacional**, destaca el caso de Hong Kong donde una empleada transfirió 25 millones de dólares tras ser engañada con una videollamada deepfake del CEO de su empresa (Deloitte, 2025). En Perú, informes recientes revelan que bandas criminales utilizan IA para suplantar la voz de familiares y exigir depósitos de dinero a través de WhatsApp y Telegram (InsightCrime, 2024).

Los **sectores más vulnerables** ante este tipo de fraude son el financiero, salud y servicios públicos. Las instituciones bancarias enfrentan una oleada de ataques con voz clonada que comprometen los sistemas de autenticación, y los hospitales comienzan a experimentar intentos de manipulación de registros clínicos y accesos administrativos mediante IA (MarketWatch, 2024; Deloitte, 2025).

Finalmente, los **estudios estadísticos** muestran un crecimiento acelerado. Discover Global Network (2024) indica que el 26 % de los ciudadanos globales han sido víctimas de algún tipo de fraude digital entre 2022 y 2023. En EE. UU., el FBI reportó más de 880.000 denuncias por fraude en 2023, con pérdidas por encima de los 12.500 millones de dólares. Este crecimiento, estimado en más del 3.000 %,

plantea retos urgentes para la prevención, persecución penal y reparación de daños.

DIMENSIÓN EFICIENCIA EN LA INVESTIGACIÓN Y RESPUESTA

La **eficiencia investigativa** frente al fraude mediante inteligencia artificial (IA) en el Perú involucra una evaluación integral de las capacidades institucionales, limitaciones procesales y el aprovechamiento tecnológico. En primer lugar, el **Ministerio Público** y la **Policía Nacional del Perú (PNP)** han desarrollado algunas herramientas especializadas para la detección de ciberfraudes. Destacan los avances en la División de Investigación de Delitos de Alta Tecnología (Divindat-PNP) y en el uso de agentes digitales encubiertos. Asimismo, el Ministerio Público ha implementado técnicas de preservación de evidencias digitales, como el uso de algoritmos hash, para garantizar la autenticidad de los datos recopilados (ILO, 2024).

No obstante, persisten importantes **obstáculos procesales**. La falta de trazabilidad en redes anónimas, la dispersión jurisdiccional cuando el ciberdelito involucra múltiples países, y los tiempos excesivos en la obtención de autorizaciones judiciales para acceder a información bancaria o digital, limitan la capacidad reactiva del sistema penal (Defensoría del Pueblo, 2023). A esto se suma la falta de uniformidad en el tratamiento de pruebas digitales, que requiere criterios técnicos y jurídicos claros.

En cuanto a la **coordinación interinstitucional e internacional**, se reconoce el papel de organismos como INTERPOL y Europol, que promueven la cooperación transfronteriza a través de redes de intercambio de información y capacitación especializada. Perú ha participado en operaciones regionales coordinadas contra

el cibercrimen, lo cual demuestra el valor estratégico de estas alianzas (Europol EC3, s.f.; INTERPOL, s.f.).

El **uso de IA en la investigación forense** también se ha expandido. Herramientas basadas en inteligencia artificial permiten analizar grandes volúmenes de datos en tiempo real, detectar patrones sospechosos en movimientos financieros y facilitar la identificación de conexiones entre dispositivos, correos y usuarios. Deloitte (2024) destaca que los sistemas de IA generativa han reducido hasta en un 90 % el tiempo de revisión documental en auditorías forenses, optimizando la respuesta a fraudes complejos.

Las **buenas prácticas en investigación digital** incluyen el respeto a la cadena de custodia, el uso de software forense certificado y la participación de peritos informáticos capacitados en ciberseguridad e IA. En este sentido, el modelo del Ministerio Público peruano promueve la colaboración entre fiscales, peritos digitales y auditores forenses (Benites Ocampo, 2023).

Finalmente, entre las **propuestas para mejorar la eficacia investigativa** en el Perú se sugiere: ampliar la capacitación técnica del personal especializado; equipar a las unidades policiales con herramientas de análisis digital; fortalecer los protocolos de actuación conjunta entre PNP y Ministerio Público; y actualizar los marcos legales para facilitar el acceso a registros electrónicos bajo supervisión judicial. Estas medidas son esenciales para una respuesta penal efectiva frente al creciente uso de IA en el fraude digital.

ANÁLISIS CRÍTICO Y PROPUESTA DE MEJORA

La **evaluación del estado actual** de la lucha contra el fraude mediante inteligencia artificial (IA) en el Perú revela avances normativos importantes, como la

promulgación de la Ley N.º 32314 que incorpora el uso de IA como agravante en la comisión de delitos. Sin embargo, su aplicación práctica aún enfrenta retos operativos y técnicos. La limitada especialización de agentes fiscales y policiales, así como la escasa infraestructura tecnológica, debilitan la eficacia en la detección, prevención y sanción de estos delitos (Allende & Brea, 2025; Nearshore Americas, 2024).

En relación con los **riesgos éticos y jurídicos** del uso de IA por parte del propio Estado, surgen preocupaciones sobre la transparencia y equidad en los procesos judiciales que utilizan sistemas automatizados. El uso de IA generativa en decisiones judiciales podría vulnerar principios fundamentales como la presunción de inocencia y el debido proceso, al no garantizar la trazabilidad ni la interpretación humana de sus resultados (Data & Policy Journal, 2025).

Una **propuesta de reforma legal y política pública** exige consolidar los marcos normativos existentes con directrices técnicas claras. En el caso peruano, es necesario complementar la Ley N.º 31814 sobre promoción de la IA con regulaciones específicas que clasifiquen los usos por niveles de riesgo, exijan auditorías obligatorias, establezcan estándares de explicabilidad y asignen responsabilidad ante fallos tecnológicos (Data Guidance, 2024).

Respecto a las **estrategias de prevención y formación ciudadana**, se requiere implementar campañas nacionales de alfabetización digital. Estas deberían enfocarse en enseñar a la población a identificar fraudes por voz clonada, correos automatizados, y contenido manipulado. Asimismo, debe incentivarse la adopción de autenticación multifactorial y métodos biométricos por parte de empresas e instituciones, especialmente en el sector financiero (Feedzai, 2025).

El **rol de la empresa privada y la autorregulación tecnológica** es esencial. Se espera que las compañías adopten estándares éticos de desarrollo y uso de IA, compartan información sobre incidentes de fraude y prioricen tecnologías como el aprendizaje federado y la inteligencia explicable para proteger la privacidad de los usuarios y facilitar auditorías externas (Awosika et al., 2023).

Finalmente, se propone un **modelo integral de respuesta penal y cibernética** basado en: la creación de unidades especializadas multidisciplinarias; el uso de IA defensiva para el monitoreo de fraudes en tiempo real; la cooperación internacional activa con organismos como INTERPOL y Europol; y la exigencia de transparencia y control sobre el uso estatal de tecnologías avanzadas en la persecución penal (Kurshan et al., 2024; Ververica, 2025).

2.3. Marco Legal

En el Perú, el delito de fraude mediante el uso de inteligencia artificial puede ser abordado bajo las disposiciones generales de la legislación relacionada con el fraude y los delitos informáticos.

La ley N° 30096, “Ley de delitos informáticos”, la cual tiene como objetivo prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia. Esta ley modifica el Código Penal y el Código Procesal Penal, debido a que esta introdujo disposiciones relacionadas con los delitos informáticos, las cuales ser aplicadas en casos de fraude que involucren el uso de sistemas de inteligencia artificial tal como se especifica en el **artículo 8 .- fraude informático** el cual menciona que “El que

deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa", especificación en la cual se aplica una pena privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.

Sin embargo, es importante tener en cuenta que la legislación puede no ser específica sobre el uso de inteligencia artificial en el fraude, ya que la tecnología evoluciona más rápido que la ley. Por lo tanto, en muchos casos, la interpretación de la ley por parte de los tribunales puede ser crucial para determinar si una actividad que involucra inteligencia artificial constituye fraude bajo la ley peruana.

2.4. Definición de términos básicos

Actualización normativa: "Es un proceso mediante el cual se realizan cambios, ajustes o revisiones en las leyes, regulaciones o normativas existentes" (Barrera, 2020, p.736).

Alertas de Fraude: "Son notificaciones automáticas o mensajes emitidos por sistemas de seguridad o plataformas financieras que advierten a los usuarios sobre posibles actividades fraudulentas o sospechosas en sus cuentas o transacciones" (Alzate y Giraldo, 2023, p.12).

Auditorías exitosas: "Se refiere a un proceso de revisión y evaluación de los registros financieros, operativos o de cumplimiento de una organización que se

lleva a cabo de manera efectiva, eficiente y con resultados satisfactorios" (Imbaquingo et al, 2020, p. 428).

Autenticación Robusta: "Se refiere a un proceso de verificación de identidad que utiliza múltiples factores de autenticación para garantizar un nivel más alto de seguridad" (Cerna, Quincho y De los Santos, 2023).

Casos de fraude: "Se refiere a una situación en la que una persona, grupo de personas o entidad comete un acto fraudulento con el objetivo de obtener ganancias ilegales, causar daño o engañar a otros" (Mayer y Oliver, 2020).

Colaboración interinstitucional: "Se refiere a la cooperación y coordinación entre diferentes instituciones, organizaciones o entidades para abordar problemas o desafíos comunes, lograr objetivos compartidos o llevar a cabo iniciativas conjuntas" (Ruiz y Masera, 2021).

Costo operativo: "Se refiere a los gastos necesarios para mantener en funcionamiento las actividades y operaciones de una empresa o entidad durante un período de tiempo específico" (Berrones, 2021).

Disponibilidad del sistema: "Se refiere a la capacidad de un sistema informático, una aplicación o una red para estar operativo y accesible cuando se necesite, es decir, que esté disponible para su uso por parte de los usuarios autorizados en cualquier momento que lo requieran" (Chávez, Jiménez y Pushung, 2020, p. 250).

Identificación de transacciones inusuales: "Se refiere al proceso de detectar y analizar aquellas transacciones que presentan características o patrones

que difieren significativamente de las transacciones normales o habituales dentro de una organización o sistema financiero" (León, 2019, p.19).

Impacto en las partes afectadas: "Se refiere a las consecuencias o repercusiones que tienen las acciones, decisiones o eventos en las personas, grupos, organizaciones o comunidades que están directa o indirectamente involucradas o afectadas por ellos" (Hohl, 2020).

Monto promedio de fraude: "Se refiere al valor medio de las pérdidas causadas por actividades fraudulentas dentro de un período de tiempo específico, generalmente expresado en términos monetarios" (De la Torre, 2018, p. 59).

Protección contra Ataques: "Se refiere al conjunto de medidas y prácticas diseñadas para prevenir, detectar, mitigar y responder a los diversos tipos de ataques cibernéticos, amenazas de seguridad y actividades maliciosas dirigidas contra sistemas informáticos, redes, dispositivos y datos" (Cando y Medina, 2021, p. 25).

Reconocimiento de Comportamientos Atípicos: "Se refiere al proceso de identificar y analizar acciones, patrones o actividades que se desvían significativamente de lo que se considera normal, típico o esperado en un entorno específico" (Alcalá y Ochoa, 2022, p. 13).

Recursos utilizados por transacción detectada: "Se refieren a los activos o elementos que están involucrados o afectados durante el proceso de realizar dicha transacción" (Pavón, et al., 2019, p. 865).

Resolución de casos: “Se refiere al proceso de investigar, analizar y resolver situaciones específicas o incidentes que requieren atención y acción por parte de una organización o entidad” (Estrada y Alfaro, 2015, p. 208).

Respuesta a incidentes: “Se refiere al proceso organizado y coordinado de detectar, analizar, mitigar y recuperarse de eventos no deseados o incidentes de seguridad que afectan la integridad, confidencialidad o disponibilidad de los sistemas informáticos, redes, datos o recursos de una organización” (Chamorro, et al., 2021, p. 223).

Seguridad en la Comunicación: “Se refiere a las medidas y prácticas diseñadas para proteger la confidencialidad, integridad y autenticidad de la información transmitida entre diferentes partes a través de diversos medios de comunicación, como redes de datos, internet, correo electrónico, mensajería instantánea, llamadas telefónicas, entre otros” (Pacheco, 2022, p. 216).

Transacciones que cumplen con la normativa: “Son aquellas que se realizan de acuerdo con las leyes, regulaciones y políticas aplicables a una determinada industria, país o jurisdicción” (Corti, 2016, p. 145).

CAPITULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Tipo de investigación

La investigación es de tipo básica, ya que se orienta a la comprensión teórica de los fenómenos sin buscar una aplicación inmediata. Su propósito es generar conocimientos nuevos, ampliar marcos conceptuales existentes y fortalecer el saber científico dentro del área de estudio. Este enfoque permite profundizar en principios, leyes o teorías fundamentales, siendo clave para el avance del conocimiento en disciplinas como el Derecho, sin necesidad de resolver problemas prácticos inmediatos (Hernández et al., 2021).

3.2. Método de Investigación

Según López y Ramos (2021) el método hipotético deductivo, “implica desglosar un objeto de estudio en partes más pequeñas para comprenderlo mejor planteando respuestas tentativas a modo de hipótesis. Este proceso permite una exploración detallada de cada aspecto” (p. 27).

En este estudio, se utilizó el método hipotético deductivo para abordar de manera exhaustiva y sistemática las variables seleccionadas. Esta decisión se fundamentó en la necesidad de plantear hipótesis de trabajo que fueron contrastadas. Además, se facilitó una comprensión más profunda y completa del conjunto general de la investigación.

3.2.1. Nivel de Investigación

Según Ramos (2020), la investigación descriptiva “es esencial en la investigación científica, ya que se dedica a describir detallada y sistemáticamente fenómenos, situaciones o grupos. Además, su enfoque radica en recolectar datos y observaciones precisas sobre un tema específico sin influir en el entorno

estudiado. Y, su objetivo principal es ofrecer una representación objetiva y precisa de la realidad, con el fin de identificar patrones, tendencias o características fundamentales" (p.24).

Se utilizó un enfoque descriptivo en la investigación, ya que se enfocó específicamente en el delito de fraude mediante el uso de la inteligencia artificial a las empresas de servicios de la ciudad de Pucallpa, 2024, por lo que se basó en técnicas y métodos descriptivos, como análisis de datos estadísticos basados en los resultados del instrumento de investigación.

3.2.2. Diseño de Investigación

Según Galarza (2021) manifiesta que: "el diseño de investigación no experimental implica observar, recopilar y analizar datos sin intervenir en el entorno o manipular variables. Se centra en la recolección de información en su estado natural, sin aplicar tratamientos o condiciones controladas por el investigador" (p. 150).

Asimismo, Galarza (2021), señala que: "El estudio transversal es una investigación observacional que examina datos de variables recolectadas en un periodo específico sobre una muestra poblacional o un subconjunto definido previamente" (p. 155).

Se utilizó un diseño no experimental de tipo transversal, basado en la observación y análisis de variables sin intervención directa o manipulación deliberada. Esto facilitó el estudio de fenómenos en su entorno natural en un momento específico, sin perturbar las condiciones originales. Se realizó una observación minuciosa de los eventos y variables pertinentes, seguida de un análisis detallado.

3.3. Población y Muestra

3.3.1. Población

De acuerdo al planteamiento de Robles (2019): “la población se refiere a un conjunto total de elementos, individuos, objetos o eventos que comparten una característica específica y son el centro de atención de un estudio. Esta característica puede ser cualquier atributo común que distinga a estos elementos, como la edad, el género, la ubicación geográfica, el nivel educativo, entre otros” (p. 174).

La población de interés para la investigación estuvo compuesta por 125 empresas de servicios formalizadas de la ciudad de Pucallpa. (N=125).

3.3.2. Muestra

La definición de muestra se obtuvo de lo publicado por Robles (2019): “se trata de una muestra representativa de la población completa que se elige y examina para obtener conclusiones o inferencias sobre el conjunto más grande. En resumen, es un grupo más reducido seleccionado de manera intencional para su estudio, con el propósito de extraer conclusiones aplicables a la población en general” (p. 93).

El muestreo que se ha empleado en la presente investigación fue aleatorio simple. Por lo que para determinar el tamaño de la muestra se usó la siguiente fórmula para poblaciones finitas:

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

Donde:

N : Tamaño de la población 125

Z : Valor crítico asociado al nivel de confianza (95%): 1.96

p : Probabilidad de aceptación (50%) : 0.5

q : Probabilidad de rechazo (50%) : 0.5

d : Error de estimación (5%) : 0.05

n : Tamaño de la muestra

$$n = \frac{124 * (1.96)^2 * (0.5) * (0.5)}{124 * (0.05)^2 + (1.96)^2 * (0.5) * (0.5)}$$

$$n = \frac{125*3.8416*0.25}{124 *0.0025 + 3.8416*0.25} = 95$$

La muestra estuvo conformada por 95 empresas de servicios formalizadas, las cuales fueron elegidas aleatoriamente.

3.4. Técnica e Instrumento de Recolección de Datos

3.4.1. Técnica

Según Feria, et al. (2020): "la encuesta es un método utilizado para recolectar información y datos particulares de una muestra representativa de una población más amplia. Implica una serie de preguntas estructuradas y/o semiestructuradas diseñadas para obtener respuestas coherentes y comparables sobre opiniones, actitudes, comportamientos, características demográficas u otros aspectos pertinentes de un grupo de individuos" (p. 72).

Se empleó la técnica de la encuesta como parte integral de este estudio, dado que será crucial obtener información directa de fuentes primarias. Por lo que se centró en recopilar percepciones, opiniones y experiencias directas de las empresas de servicios, lo que mejoró el análisis y la comprensión de la presencia del delito de fraude mediante el uso de la inteligencia artificial a las empresas de servicios de la ciudad de Pucallpa, 2024.

3.4.2. Instrumento

De la definición dada por González y Sosa (2020): describen el cuestionario como una herramienta compuesta por un conjunto de preguntas meticulosamente elaboradas para recolectar la información necesaria y cumplir con los objetivos planteados en la investigación. Su objetivo principal es realizar un diagnóstico sobre las estrategias de aprendizaje empleadas por un estudiante durante su proceso de estudio con el propósito de aprender. Estas estrategias están estrechamente vinculadas con los procesos involucrados en la actividad de aprendizaje (p. 208).

Durante este estudio, se desarrollaron dos conjuntos de cuestionarios, cada uno compuesto por 18 preguntas relacionadas con una variable específica. Estas preguntas se formularon de manera que su respuesta fuera simple, presentándose en un formato cerrado con cinco opciones para elegir. Estas respuestas se asignaron a una escala ordinal, similar al enfoque utilizado en la escala de Likert. Luego, se llevó a cabo un proceso de validación de estos cuestionarios mediante la técnica de juicio de expertos para asegurar su idoneidad y pertinencia para el propósito de la investigación.

Además, se evaluó la confiabilidad de estos cuestionarios utilizando el coeficiente alfa de Cronbach, un indicador estadístico empleado para medir la consistencia interna de las preguntas. Esta evaluación fue fundamental para asegurar la fiabilidad y consistencia de los cuestionarios en la recolección de datos, lo que garantizó la solidez de los resultados obtenidos en el estudio.

3.5. Procedimiento de Recolección de Datos

Inicialmente, se procedió a ubicar el lugar de estudio, centrándose en la ciudad de Pucallpa. Esta etapa involucró la presentación formal de la solicitud para

realizar la investigación, con el objetivo de obtener acceso a la información relevante. Una vez se recibió la autorización necesaria para proceder, se dio inicio al proceso investigativo, empleando herramientas específicas para la recolección de datos.

Durante esta fase, se llevó a cabo la identificación de los participantes, seleccionados al azar entre los productores de cacao del mencionado distrito. Antes de su inclusión, se les invitó y se obtuvo su consentimiento informado para participar en el estudio. Se les proporcionó información detallada sobre el propósito académico de la investigación, asegurando que los datos recopilados se utilizaran exclusivamente para fines académicos.

Además, se garantizó a los participantes la confidencialidad de sus respuestas y se les alentó a responder con sinceridad y plena libertad a las preguntas formuladas en los cuestionarios. Este enfoque ético y transparente con los participantes fue esencial para asegurar la integridad de la investigación.

3.6. Tratamiento de datos

Los datos recolectados fueron almacenados en una hoja de cálculo y se transfirieron al programa SPSS versión 25 para su análisis estadístico. Dentro de esta herramienta, se generaron tablas de frecuencia y gráficos de barras, lo que facilitó la representación visual de los resultados obtenidos, junto con su respectiva interpretación. Además, se realizaron cálculos específicos, como los coeficientes de correlación de rangos Rho de Spearman y los valores de p (significancias bilaterales empíricas) para cada una de las hipótesis de investigación. Estos

cálculos se efectuaron para obtener estadísticas relevantes que respaldaron el análisis y la contrastación correspondiente.

CAPITULO IV

RESULTADOS

4.1. Resultados de la Investigación

4.1.1. Resultados de la evaluación de Instrumento

Se realizó un análisis inicial sobre la fiabilidad del cuestionario empleado en el estudio, centrándose en su coherencia interna. Asimismo, se llevó a cabo una encuesta a 95 empresas de servicios establecidas en la ciudad de Pucallpa. Esta encuesta se amplió con la utilización del coeficiente de Cronbach (α) como método de evaluación, con el fin de establecer la coherencia entre las preguntas del cuestionario. Los hallazgos de esta evaluación se detallan en la tabla 1.

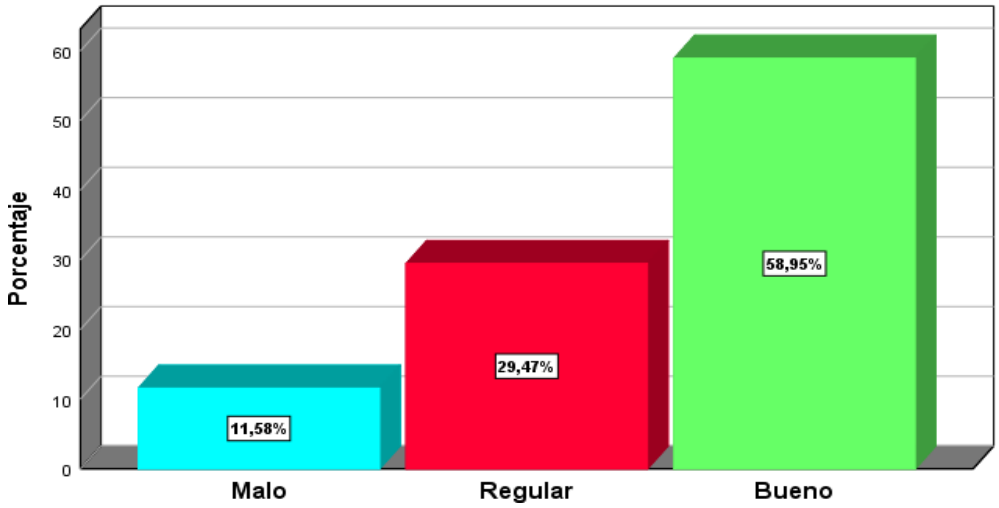
Tabla 1 Variable inteligencia artificial

Baremos de la Variable 1: Inteligencia artificial.

Baremos	Categoría	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
[51-58]	Malo	11	11,6	11,6	11,6
[59-65]	Regular	28	29,5	29,5	41,1
[66-76]	Bueno	56	58,9	58,9	100,0
	Total	95	100,0	100,0	

Fuente: Elaboración propia en base al software SPSS v.25

Figura 1 Gráfico de barras de la Variable 1: Inteligencia artificial.



Fuente: Software SPSS versión 25

Interpretación:

En el análisis de los datos sobre inteligencia artificial presentados en la tabla 2, se revelan percepciones variadas entre los encuestados. Los resultados muestran que de los encuestados, 56 expresaron que la detección de patrones anómalos, la seguridad en las transacciones y la eficiencia operativa contribuyen de manera significativa a la inteligencia artificial, representando el 58.9%. Esta perspectiva podría reflejar una necesidad de mayor claridad o énfasis en cómo estas dimensiones específicas pueden impactar en la eficacia y utilidad de la inteligencia artificial. Por otro lado, 28 encuestados, que equivalen al 29.5%, consideraron que estas tres dimensiones se sitúan en un nivel regular. Mientras que 11 encuestados, que representan el 11.6%, opinaron que estas dimensiones presentan un nivel de medición deficiente para la variable en cuestión, ya que su contribución es baja, calificándolas como malas. Esta minoría considera que la

contribución de estos aspectos es baja, calificándolos como malos. Este punto de vista puede indicar áreas de mejora o preocupaciones específicas sobre cómo se están abordando o implementando estas dimensiones en relación con la inteligencia artificial.

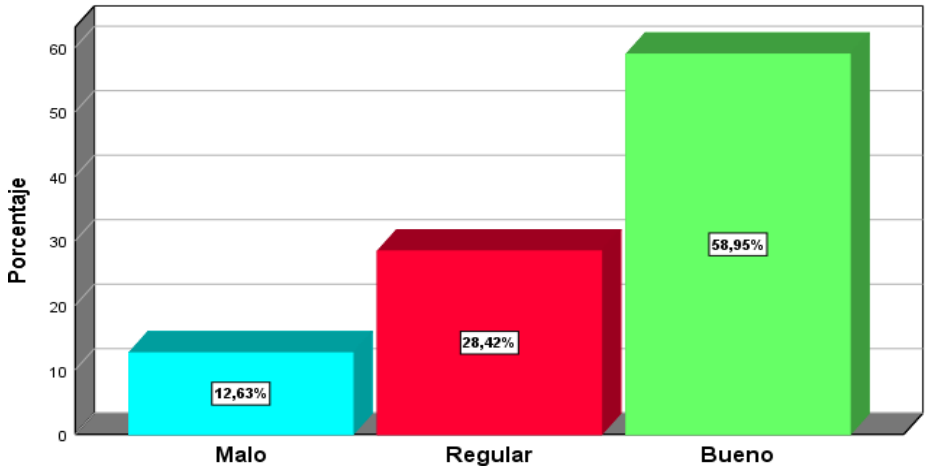
Tabla 2 Baremos de la dimensión detección de patrones anómalos

Baremos de la Dimensión 1.1: Detección de patrones anómalos.

Baremos	Categoría	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
[13-17]	Malo	12	12,6	12,6	12,6
[18-20]	Regular	27	28,4	28,4	41,1
[21-29]	Bueno	56	58,9	58,9	100,0
	Total	95	100,0	100,0	

Fuente: Elaboración propia en base al software SPSS v.25

Figura 2 Gráfico de barras de la Dimensión 1.1: Detección de patrones anómalos.



Fuente: Software SPSS versión 25

Interpretación:

En la tabla 3 podemos apreciar que, de acuerdo a la suma de los baremos, obtenemos los resultados de la primera dimensión, siendo así que 12 encuestados representando al 12,6% de ellos, porcentaje muy leve que opina que la identificación de transacciones inusuales, el reconocimiento de comportamientos atípicos y las alertas de fraude cumplen un papel malo en la detección de patrones anómalos, mientras que el 28,4% representado por 27 quienes refieren que las dimensiones mencionadas guardan una relación regular con la detección de patrones anómalos; finalmente el 58,9% representando a 56 encuestados afirma que indicadores mencionados cumplen una buena influencia en la detección de patrones anómalos.

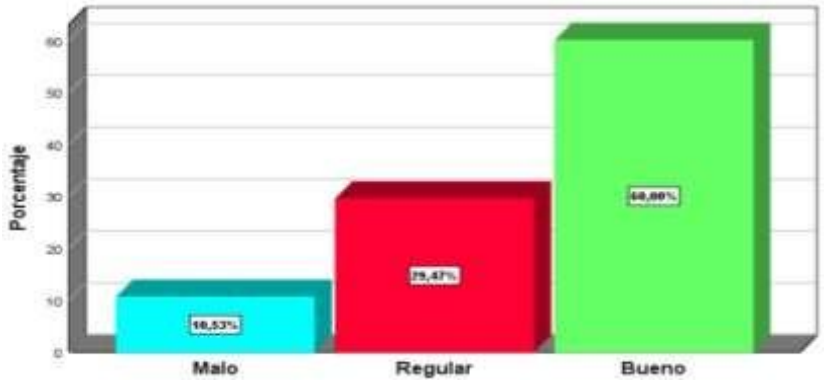
Tabla 3 Baremos de la dimensión seguridad en las transacciones

Baremos de la Dimensión 1.2: Seguridad en las Transacciones.

Baremos	Categoría	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
[16-18]	Malo	10	10,5	10,5	10,5
[19-21]	Regular	28	29,5	29,5	40,0
[22-28]	Bueno	57	60,0	60,0	100,0
	Total	95	100,0	100,0	

Fuente: Elaboración propia en base al software SPSS v.25

Figura 3 Gráfico de barras de la Dimensión 1.2: Seguridad en las Transacciones.



Fuente: Software SPSS versión 25

Interpretación:

En relación a la dimensión seguridad en las transacciones, los resultados de la encuesta se presentan en la tabla 4. Según estos resultados, 10 encuestados, que representan el 10.5%, indicaron que la autenticación robusta, la protección contra ataques y la seguridad en la comunicación fueron valorados como malo. Por otro lado, 28 encuestados, que constituyen el 29,5%, consideraron que estos indicadores otorgan a la dimensión una percepción intermedia, lo que implica una valoración regular. En contraste, 57 encuestados, con el porcentaje del 60% de los resultados, evaluaron positivamente los indicadores relacionados con la dimensión seguridad en las transacciones.

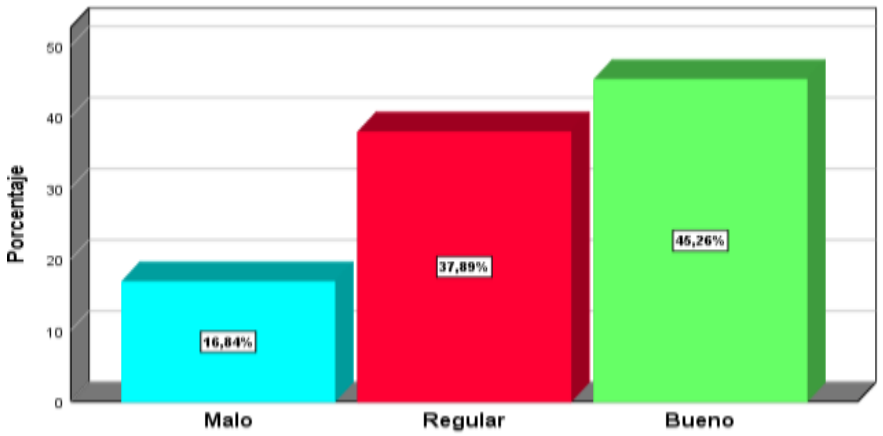
Tabla 4 baremos de la dimensión eficiencia operativa

Baremos de la Dimensión 1.3: Eficiencia operativa.

Baremos	Categoría	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
[16-19]	Malo	16	16,8	16,8	16,8
[20-22]	Regular	36	37,9	37,9	54,7
[23-27]	Bueno	43	45,3	45,3	100,0
	Total	95	100,0	100,0	

Fuente: Elaboración propia en base al software SPSS v.25

Figura 4 de barras de la Dimensión 1.3: Eficiencia operativa.



Fuente: Software SPSS versión 25

Interpretación:

En el análisis de la tercera dimensión, eficiencia operativa, se observa una variedad de percepciones entre los encuestados, como se muestra en la tabla 5. Es notable que una parte considerable, el 43 encuestados representados por el 45,3%, afirmaron que los recursos utilizados por transacción detectada, el costo operativo y la disponibilidad del sistema evidencia una valoración buena, es decir, que estos indicadores tienen una alta percepción por parte de los encuestados. Por

otro lado, tenemos que a 36 encuestados representados por el 37,9%, porcentaje de los resultados el cual afirma que los indicadores mencionados hacen que la dimensión tenga una percepción intermedia, es decir que, le atribuyen una valoración regular. Esto podría indicar áreas de mejora o posibles preocupaciones sobre cómo se están gestionando estos aspectos en los sistemas de IA. Mientras que, 16 encuestados, con un porcentaje del 16,8% señalan que los indicadores mencionados los cuales están relacionados y componen la dimensión eficiencia operativa, son valorados por ellos como malos, dado que estos contribuyen de manera baja con la primera variable inteligencia artificial. Este hallazgo subraya la necesidad de una mayor atención a la optimización de los recursos y la mejora de la eficiencia en el contexto de la implementación de la IA.

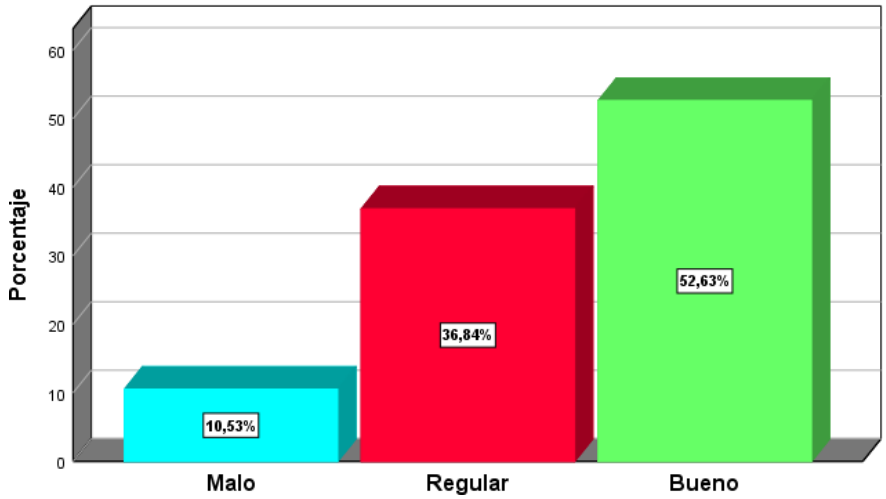
Tabla 5 baremos de la variable delito de fraude

Baremos de la Variable 2: Delito de fraude.

Baremos	Categoría	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
[47-58]	Malo	10	10,5	10,5	10,5
[59-65]	Regular	35	36,8	36,8	47,4
[66-80]	Bueno	50	52,6	52,6	100,0
	Total	95	100,0	100,0	

Fuente: Elaboración propia en base al software SPSS v.25

Figura 5 barras de la Variable 2: Delito de fraude.



Fuente: Software SPSS versión 25

Interpretación:

En la tabla 6 se presenta una interpretación detallada de la escala de calificación aplicada a la variable delito de fraude, proporcionando una visión clara de las percepciones de los encuestados en relación con las dimensiones asociadas a esta variable. Pudiendo observar que de los 50 encuestados con respecto a la segunda variable mencionan que las dimensiones el cumplimiento normativo, la gravedad del fraude, y la eficiencia en la investigación y respuesta guardan un alto

nivel de porcentaje equivalente a 52,6% asegurando así que dichas dimensiones son muy buenas y complementan a la variable delito de fraude. Esta evaluación positiva sugiere que estas dimensiones son percibidas como altamente efectivas y contribuyen de manera significativa a la comprensión y abordaje del delito de fraude, por otro lado tenemos a 35 encuestados con un 36,8% los cuales mencionan que las tres dimensiones se encuentran en un nivel regular, en cambio 10 encuestados con un porcentaje equivalente al 10,5%, porcentaje leve el cual se encuentran en un nivel de medición mala para la variable delito de fraude.

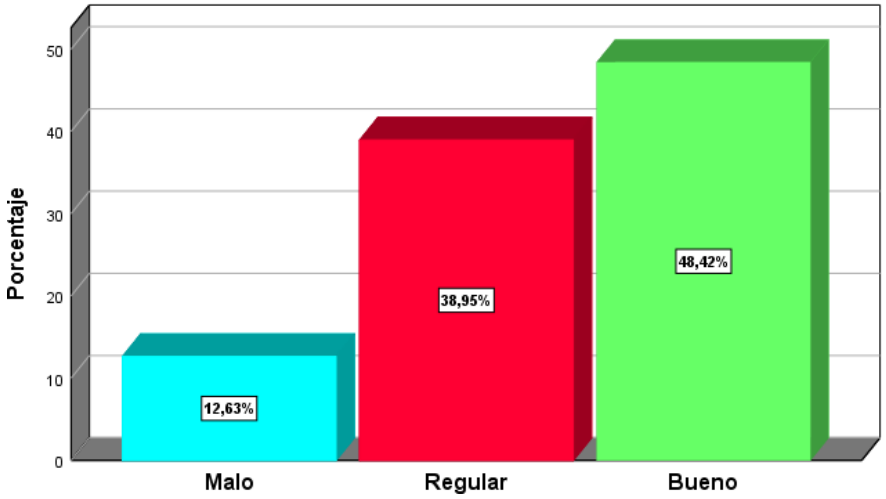
Tabla 6 Baremos de la dimensión cumplimiento normativo

Baremos de la Dimensión 2.1: Cumplimiento normativo.

Baremos	Categoría	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
[12-18]	Malo	12	12,6	12,6	12,6
[19-22]	Regular	37	38,9	38,9	51,6
[23-28]	Bueno	46	48,4	48,4	100,0
	Total	95	100,0	100,0	

Fuente: Elaboración propia en base al software SPSS v.25

Figura 6 Gráfico de barras de la Dimensión 2.1: Cumplimiento normativo.



Fuente: Software SPSS versión 25

Interpretación:

Referente a la primera dimensión cumplimiento normativo, en la tabla 7 se muestra la suma obtenida de la encuesta, 12 encuestados representados por el 12,6%, afirmaron que las transacciones que cumplen con la normativa, la actualización normativa y las auditorías exitosas evidencia una valoración mala, es decir, que estos indicadores tienen una baja percepción por parte de los encuestados. Por otro lado, tenemos que a 37 encuestados representados por el

38,9%, porcentaje de los resultados el cual afirma que los indicadores mencionados hacen que la dimensión tenga una percepción intermedia, es decir que, le atribuyen una valoración regular. Mientras que, 46 encuestados, con un porcentaje del 48,4% señalan que los indicadores mencionados los cuales están relacionados y componen la dimensión cumplimiento normativo, son valorados por ellos como bueno, dado que estos contribuyen con la segunda variable delito de fraude.

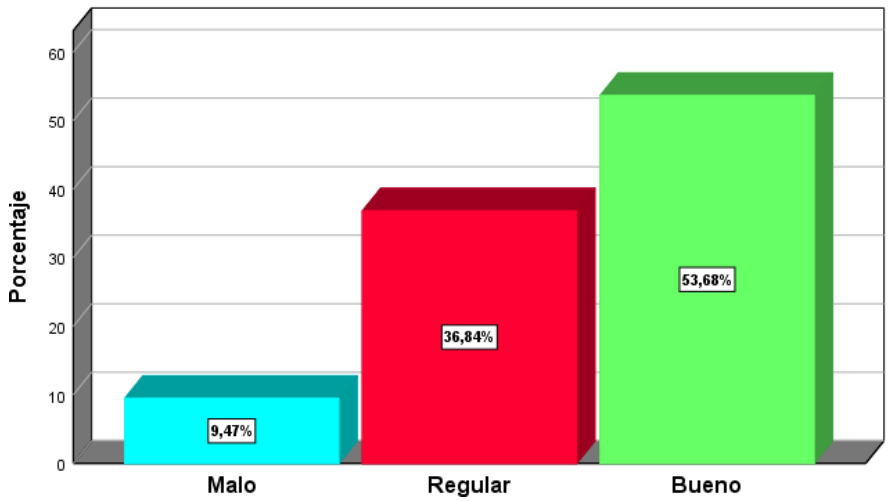
Tabla 7 baremos de la dimensión gravedad del fraude

Baremos de la Dimensión 2.2: Gravedad del fraude.

Baremos	Categoría	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
[10-17]	Malo	9	9,5	9,5	9,5
[18-21]	Regular	35	36,8	36,8	46,3
[22-28]	Bueno	51	53,7	53,7	100,0
	Total	95	100,0	100,0	

Fuente: Elaboración propia en base al software SPSS v.25

Figura 7* Barras *de la Dimensión 2.2: Gravedad del fraude.



Fuente: Software SPSS versión 25

Interpretación:

Referente a la segunda dimensión gravedad del fraude, en la tabla 8 se muestra la suma obtenida de la encuesta, 51 encuestados representados por el 53,7%, siendo el porcentaje más alto, afirmaron que el monto promedio de fraude, los casos de fraude y el impacto en las partes afectadas evidencia una valoración buena, es decir, que estos indicadores tienen una alta y positiva percepción por parte de los encuestados. Por otro lado, tenemos que a 35 encuestados representados por el 36,8% de los resultados, el cual afirma que los indicadores mencionados hacen que la dimensión tenga una percepción intermedia, es decir que, le atribuyen una valoración regular. Mientras que, 9 encuestados, con un porcentaje del 9,5% señalan que los indicadores mencionados los cuales están relacionados y componen la dimensión gravedad del fraude, son valorados por ellos como malas, dado que estos contribuyen de manera leve con la segunda variable delito de fraude. Esta evaluación crítica sugiere que hay preocupaciones sobre la relevancia o la efectividad de estos indicadores en la comprensión y prevención del delito de fraude. Este hallazgo subraya la necesidad de una revisión más detallada y posiblemente de acciones correctivas para abordar las deficiencias identificadas en esta dimensión.

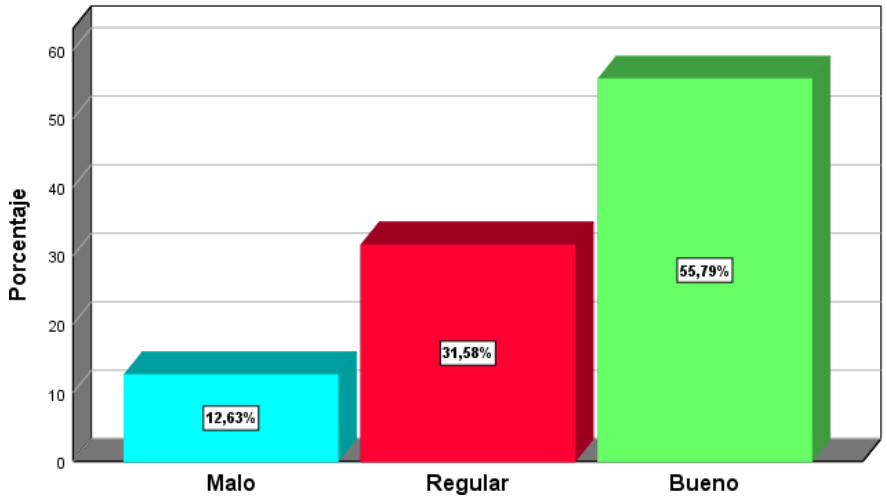
Tabla 8 baremos de la dimensión eficiencia en la investigación y respuesta

Baremos de la Dimensión 2.3: Eficiencia en la Investigación y Respuesta.

Baremos	Categoría	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
[12-19]	Malo	12	12,6	12,6	12,6
[20-21]	Regular	30	31,6	31,6	44,2
[22-27]	Bueno	53	55,8	55,8	100,0
	Total	95	100,0	100,0	

Fuente: Elaboración propia en base al software SPSS v.25

Figura 8 Gráfico de barras de la Dimensión 2.3: Eficiencia en la investigación y respuesta.



Fuente: Software SPSS versión 25

Interpretación:

Referente a la tercera dimensión eficiencia en la investigación y respuesta, en la tabla 9 se muestra la suma obtenida de la encuesta, 12 encuestados representados por el 12,6%, afirmaron que la respuesta a incidentes, la resolución de casos y la colaboración interinstitucional evidencia una valoración mala, es decir, que estos indicadores tienen una baja percepción por parte de los encuestados.

Por otro lado, tenemos que a 30 encuestados representados por el 31,6%, porcentaje el cual afirma que los indicadores mencionados hacen que la dimensión tenga una percepción intermedia, es decir que, le atribuyen una valoración regular. Mientras que, 53 encuestados, con un porcentaje del 55,8% señalan que los indicadores mencionados los cuales están relacionados y componen la dimensión eficiencia en la investigación y respuesta, son valorados por ellos como bueno, dado que estos contribuyen con la segunda variable delito de fraude. Esta evaluación crítica indica que estos encuestados perciben una deficiencia en la respuesta a incidentes, la resolución de casos y la colaboración interinstitucional en el contexto del delito de fraude.

4.2. Contraste de Hipótesis

4.2.1. Contraste de la Hipótesis especifica 1

Partiendo de la hipótesis específica 1, se plantean las hipótesis científicas nula (Ho) y alterna (Ha):

Ho: Los patrones anómalos mediante el uso de inteligencia artificial se vienen ejecutando en no más del 50% de las empresas de servicios de la ciudad de Pucallpa, 2024.

Ha: Los patrones anómalos mediante el uso de inteligencia artificial se vienen ejecutando en más del 50% de las empresas de servicios de la ciudad de Pucallpa, 2024.

A partir de esto, se debe tener en cuenta la proporción p de empresas de servicios formalizadas en la ciudad de Pucallpa. Para la proporción hipotética, se utilizó p_0 = 0,5 ya que cuando supera el 50% se considera que la mayoría de las empresas formalizadas presentan anomalías mediante el uso de inteligencia

artificial. Con esta proporción poblacional, se establecen las correspondientes hipótesis estadísticas:

$$Ho: p \leq 0{,}50 \quad ; \quad Ha: p > 0{,}50$$

La contrastación de la hipótesis se efectuó utilizando la prueba Z estándar para la proporción de la población, suponiendo que las proporciones de las muestras siguen una distribución normal. Esta suposición se basa en que el tamaño de la muestra n=95 (>30) es considerado lo suficientemente grande, lo que permite aplicar la prueba normal de una cola con valores críticos y utilizando z como el estadístico de prueba.

Tras revisar el uso de la IA en las empresas de servicios y evaluar los resultados de la aplicación del instrumento a los ítems relacionados con los indicadores asociados a la dimensión de detección de patrones anómalos, se obtuvo una proporción muestral de $\overline{p} = 0.684$, como se muestra en la tabla 46.

Tabla 9 Porcentaje de respuestas con respecto a la dimensión 1.1: Detección de patrones anómalos

Dimensión	**Indicadores**	**% Respuestas obtenidas**				
		Nunca	Casi nunca	A veces	Casi siempre	Siempre
Detección de patrones anómalos	Identificación de transacciones inusuales	4,2%	8,4%	27,4%	37,9%	22,1%
		5,3%	15,8%	27,4%	26,3%	25,3%
	Reconocimiento de Comportamientos Atípicos	6,3%	14,7%	31,6%	26,3%	21,1%
		3,2%	11,6%	29,5%	30,5%	25,3%
	Alertas de Fraude	4,2%	12,6%	28,4%	33,7%	21,1%
		5,3%	10,5%	31,6%	26,3%	26,3%
Promedio		4,8%	12,3%	29,3%	30,2%	23,5%
Acumulado		Menor a 50			Mayor a 50	
		0,317			**0,684**	

El error estándar se calculó utilizando la siguiente fórmula:

$$\sigma_p = \sqrt{\frac{p_0(1 - p_0)}{n}}$$

$$\sigma_p = \sqrt{\frac{0.5\ (1-0.5)}{95}} = 0{,}0513$$

Dado que tanto np_0 $como$ $n(1 - p_0)$ superan los valores de 5 y 0.05, respectivamente, se puede estimar con un nivel de confianza del 95% que la distribución de la media muestral $\bar{p}$ es muy similar a una distribución normal. Con estas bases, el estadístico de prueba z se determinó mediante la siguiente fórmula:

$$z = \frac{\bar{p} - p_0}{\sigma_p}$$

$$z = \frac{0{,}684 - 0{,}5}{0{,}0513} = 3{,}587$$

Considerando un nivel de significancia de □=0,05, el valor crítico está asociado a un área de 0.05 en la cola superior de una distribución normal, resultando en $z_{0.05} = 1.645$.

Se empleó la técnica del valor crítico para establecer la regla de rechazo, que consiste en rechazar la hipótesis nula (H0) cuando z > 1.645. En este caso específico, z tiene un valor de 3.587, superando el umbral crítico de 1.645. Por lo tanto, se rechaza la hipótesis nula (H0), lo que confirma que los patrones anómalos, mediante el uso de inteligencia artificial, se vienen ejecutando en más del 50% de las empresas de servicios en la ciudad de Pucallpa en 2024.

4.2.2. Contraste de la Hipótesis especifica 2

Partiendo de la hipótesis específica 2, se plantean las hipótesis científicas nula (Ho) y alterna (Ha):

Ho: La vulneración de la seguridad en las transacciones mediante el uso inteligencia artificial se está produciendo en no más del 50% de las empresas de servicios de la ciudad de Pucallpa, 2024.

Ha: La vulneración de la seguridad en las transacciones mediante el uso inteligencia artificial se está produciendo en más del 50% de las empresas de servicios de la ciudad de Pucallpa, 2024.

En base a esto, es necesario considerar la proporción p de empresas de servicios formalizadas en la ciudad de Pucallpa. Se adoptó una proporción hipotética de p_0 = 0,5, dado que al superar el 50% se considera que la mayoría de las empresas formalizadas presentan problemas de seguridad en las transacciones al utilizar inteligencia artificial. Con esta proporción poblacional, se plantean las hipótesis estadísticas correspondientes:

Ho: p ≤ 0,50 ; Ha: p > 0,50

La verificación de la hipótesis se realizó empleando la prueba Z estándar para la proporción de la población, bajo la suposición de que las proporciones de las muestras siguen una distribución normal. Esta suposición se justifica dado que el tamaño de la muestra n=95 (>30) es considerado suficientemente grande, lo que posibilita la aplicación de la prueba normal de una cola con valores críticos y utilizando z como el estadístico de prueba.

Después de analizar el uso de la IA en las empresas de servicios y evaluar los resultados obtenidos de aplicar el instrumento a los ítems vinculados con los indicadores de la dimensión de seguridad en las transacciones, se determinó una proporción muestral de $\overline{p}$ = 0.749, como se ilustra en la tabla 47.

Tabla 10 Porcentaje de respuestas con respecto a la dimensión 1.2: Seguridad en las transacciones

Dimensión	Indicadores	% Respuestas obtenidas				
		Nunca	Casi nunca	A veces	Casi siempre	Siempre
	Autenticación robusta	2,1%	15,8%	25,3%	31,6%	25,3%
		6,3%	7,4%	18,9%	43,2%	24,2%

Seguridad en las transacciones	Protección contra ataques	2,1%	5,3%	27,4%	37,9%	27,4%
		7,4%	8,4%	20,0%	28,4%	35,8%
	Seguridad en la comunicación	3,2%	8,4%	27,4%	30,5%	30,5%
		4,2%	9,5%	22,1%	30,5%	33,7%
Promedio		4%	9%	24%	34%	29%
Acumulado		Menor a 50			Mayor a 50	
		0,251			**0,749**	

El cálculo del error estándar se realizó mediante la fórmula siguiente:

$$\sigma_p = \sqrt{\frac{p_0(1 - p_0)}{n}}$$

$$\sigma_p = \sqrt{\frac{0.5\ (1-0.5)}{95}} = 0{,}0513$$

Como tanto np_0 $como$ $n(1 - p_0)$ exceden los valores de 5 y 0.05, respectivamente, se puede inferir con un nivel de confianza del 95% que la distribución de la media muestral $\bar{p}$ se asemeja bastante a una distribución normal. Basado en esto, el estadístico de prueba z se calculó utilizando la fórmula siguiente:

$$z = \frac{\bar{p} - p_0}{\sigma_p}$$

$$z = \frac{0{,}749 - 0{,}5}{0{,}0513} = 4{,}854$$

Con un nivel de significancia de □=0,05, el valor crítico corresponde a un área de 0.05 en la cola superior de una distribución normal, obteniendo un $z_{0.05}$ = 1.645.

Se utilizó la técnica del valor crítico para definir la regla de rechazo, la cual establece que se debe rechazar la hipótesis nula (H0) cuando z > 1.645. En este caso particular, z es igual a 4.854, superando el umbral crítico de 1.645. Por lo tanto, se rechaza la hipótesis nula (H0), lo que indica que la vulneración de la

seguridad en las transacciones mediante inteligencia artificial ocurre en más del 50% de las empresas de servicios en la ciudad de Pucallpa en 2024.

4.2.3. Contraste de la Hipótesis especifica 3

En base al enunciado de la hipótesis específica 3, llega a plantearse sus hipótesis científicas nula (Ho) y alterna (Ha):

Ho: La eficiencia operativa es afectada mediante el uso inteligencia artificial en no más del 50% de las empresas de servicios de la ciudad de Pucallpa, 2024.

Ha: La eficiencia operativa es afectada mediante el uso inteligencia artificial en más del 50% de las empresas de servicios de la ciudad de Pucallpa, 2024.

A partir de esto, es importante tener en cuenta la proporción p de empresas de servicios formalizadas en la ciudad de Pucallpa. Se utilizó una proporción hipotética de p_0 = 0,5, ya que superar el 50% sugiere que la mayoría de las empresas formalizadas tienen su eficiencia operativa afectada por el uso de inteligencia artificial. Con esta proporción poblacional, se establecen las hipótesis estadísticas correspondientes:

$$Ho: p \leq 0{,}50 \quad ; \quad Ha: p > 0{,}50$$

La comprobación de la hipótesis se llevó a cabo utilizando la prueba Z estándar para la proporción de la población, asumiendo que las proporciones muestrales siguen una distribución normal. Esta suposición se fundamenta en que el tamaño de la muestra, n=95 (>30), es lo suficientemente grande como para permitir la aplicación de la prueba normal de una cola, con valores críticos y utilizando z como el estadístico de prueba.

Tras examinar el uso de la IA en las empresas de servicios y revisar los resultados de la aplicación del instrumento a los ítems relacionados con los

indicadores de la dimensión de eficiencia operativa, se obtuvo una proporción muestral de $\overline{p}$ = 0.731, según se muestra en la tabla 48.

Tabla 11 Porcentaje de respuestas con respecto a la dimensión 1.3: Eficiencia operativa

Dimensión	Indicadores	% Respuestas obtenidas				
		Nunca	Casi nunca	A veces	Casi siempre	Siempre
Eficiencia operativa	Recursos utilizados por transacción detectada	3,2%	11,6%	27,4%	30,5%	27,4%
		4,2%	4,2%	31,6%	31,6%	28,4%
	Costo operativo	5,3%	10,5%	28,4%	28,4%	27,4%
		3,2%	7,4%	28,4%	37,9%	23,2%
	Disponibilidad del sistema	5,3%	5,3%	27,4%	36,8%	25,3%
		5,3%	10,5%	28,4%	27,4%	28,4%
Promedio		4%	8%	29%	32%	27%
Acumulado		Menor a 50			Mayor a 50	
		0,270			**0,731**	

El error estándar se determinó utilizando la siguiente fórmula:

$$\sigma_p = \sqrt{\frac{p_0(1 - p_0)}{n}}$$

$$\sigma_p = \sqrt{\frac{0.5\ (1-0.5)}{95}} = 0{,}0513$$

Dado que tanto $np_0\ como\ n(1 - p_0)$ superan los valores de 5 y 0.05, respectivamente, se puede concluir con un nivel de confianza del 95% que la distribución de la media muestral $\overline{p}$ es muy similar a una distribución normal. Con esta premisa, el estadístico de prueba z se determinó mediante la fórmula siguiente:

$$z = \frac{\overline{p} - p_0}{\sigma_p}$$

$$z = \frac{0{,}731 - 0{,}5}{0{,}0513} = 4{,}503$$

Para un nivel de significancia de α=0.05, el valor crítico se relaciona con un área de 0.05 en la cola superior de una distribución normal, resultando en $z_{0.05}$ = 1.645.

Se empleó la técnica del valor crítico para establecer la regla de rechazo, que dicta que la hipótesis nula (H0) debe ser rechazada cuando z > 1.645. En este caso específico, z es igual a 4.503, lo que supera el umbral crítico de 1.645. Por lo tanto, se rechaza la hipótesis nula (H0), lo que sugiere que más del 50% de las empresas de servicios en la ciudad de Pucallpa en 2024 experimentan una afectación en su eficiencia operativa debido al uso de inteligencia artificial.

4.2.4. Contraste de la Hipótesis General

Partiendo de la hipótesis general, se plantean las hipótesis científicas nula (Ho) y alterna (Ha):

Ho: El delito de fraude mediante el uso inteligencia artificial se cometió en perjuicio en no más del 50% de las empresas de servicios de la ciudad de Pucallpa, 2024.

Ha: El delito de fraude mediante el uso inteligencia artificial se cometió en perjuicio en más del 50% de las empresas de servicios de la ciudad de Pucallpa, 2024.

A partir de esto, es importante tener en cuenta la proporción p de empresas de servicios formalizadas en la ciudad de Pucallpa. Se utilizó una proporción hipotética de p_0 = 0,5, dado que superar el 50% indica que la mayoría de las empresas formalizadas han sido víctimas de un delito de fraude perpetrado mediante el uso de inteligencia artificial. Con esta proporción poblacional, se definen las hipótesis estadísticas pertinentes:

$$Ho: p \leq 0{,}50 \quad ; \quad Ha: p > 0{,}50$$

La verificación de la hipótesis se realizó mediante la prueba Z estándar para la proporción poblacional, partiendo de la premisa de que las proporciones muestrales se distribuyen normalmente. Esta premisa se justifica porque el tamaño de la muestra, n=95 (>30), es lo bastante grande para aplicar la prueba normal de una cola, empleando valores críticos y utilizando z como el estadístico de prueba.

La fase de recolección de datos consistió en aplicar un cuestionario de encuesta a un total de 95 empresas de servicios. Este proceso permitió obtener la proporción muestral relacionada con las dimensiones de las variables vinculadas tanto con la inteligencia artificial como con el delito de fraude, resultando en una proporción de $\overline{p}$ = 0.721. Esta proporción se calculó a partir de las respuestas obtenidas en la encuesta: las respuestas que recibieron los valores ordinales 4 y 5 indicaron que el delito de fraude se cometía siempre o casi siempre a través del uso de inteligencia artificial. En comparación, las respuestas asignadas al valor ordinal 3 (a veces) se interpretaron de modo que la mitad de la frecuencia en esta categoría sugería que el fraude se cometía mediante el uso de inteligencia artificial en un grado intermedio. Por otro lado, las respuestas correspondientes a nunca (1) y casi nunca (2) indicaron que el uso de inteligencia artificial no tenía una relevancia significativa en la comisión de delitos de fraude en estas empresas. Además, se analizaron las tendencias en el uso de inteligencia artificial para detectar patrones y prevenir fraudes, y se evaluó cómo estas prácticas afectaban la gestión operativa y la seguridad en las transacciones. Los detalles completos y los datos utilizados para calcular esta proporción muestral se encuentran en la tabla 49, la cual ofrece un desglose detallado de las respuestas y su interpretación en el contexto del estudio.

Tabla 12 Porcentaje de respuestas con respecto a la variable 1: Inteligencia artificial

Dimensión	Indicadores	% Respuestas obtenidas				
		Nunca	Casi nunca	A veces	Casi siempre	Siempre
Detección de patrones anómalos	Identificación de transacciones inusuales	4,2%	8,4%	27,4%	37,9%	22,1%
		5,3%	15,8%	27,4%	26,3%	25,3%
	Reconocimiento de Comportamientos Atípicos	6,3%	14,7%	31,6%	26,3%	21,1%
		3,2%	11,6%	29,5%	30,5%	25,3%
	Alertas de Fraude	4,2%	12,6%	28,4%	33,7%	21,1%
		5,3%	10,5%	31,6%	26,3%	26,3%
Seguridad den las transacciones	Autenticación robusta	2,1%	15,8%	25,3%	31,6%	25,3%
		6,3%	7,4%	18,9%	43,2%	24,2%
	Protección contra ataques	2,1%	5,3%	27,4%	37,9%	27,4%
		7,4%	8,4%	20,0%	28,4%	35,8%
	Seguridad en la comunicación	3,2%	8,4%	27,4%	30,5%	30,5%
		4,2%	9,5%	22,1%	30,5%	33,7%
Eficiencia operativa	Recursos utilizados por transacción detectada	3,2%	11,6%	27,4%	30,5%	27,4%
		4,2%	4,2%	31,6%	31,6%	28,4%
	Costo operativo	5,3%	10,5%	28,4%	28,4%	27,4%
		3,2%	7,4%	28,4%	37,9%	23,2%
	Disponibilidad del sistema	5,3%	5,3%	27,4%	36,8%	25,3%
		5,3%	10,5%	28,4%	27,4%	28,4%
Promedio		4%	10%	27%	32%	27%
Acumulado		Menor a 50			Mayor a 50	
		0,279			**0,721**	

El error estándar se calculó mediante la aplicación de la fórmula que se presenta a continuación:

$$\sigma_p = \sqrt{\frac{p_0(1 - p_0)}{n}}$$

$$\sigma_p = \sqrt{\frac{0.5\ (1-0.5)}{95}} = 0{,}0513$$

Dado que tanto np_0 $como$ $n(1 - p_0)$ exceden los umbrales de 5 y 0.05, respectivamente, se puede inferir con un nivel de confianza del 95% que la distribución de la media muestral $\overline{p}$ se aproxima bastante a una distribución normal. Basado en esta observación, el estadístico de prueba z fue calculado utilizando la siguiente fórmula:

$$z = \frac{\overline{p} - p_0}{\sigma_p}$$

$$z = \frac{0,721 - 0,5}{0,0513} = 4,308$$

Con un nivel de significancia de α=0.05, el valor crítico corresponde a un área de 0.05 en la cola superior de una distribución normal, lo que da como resultado $z_{0.05} = 1.645$.

Se utilizó el método del valor crítico para definir la regla de rechazo, que establece que la hipótesis nula (H0) debe ser desestimada cuando z supera 1.645. En este caso particular, el valor de z es 4.308, lo que excede el umbral crítico de 1.645. Como resultado, se rechaza la hipótesis nula (H0), lo que indica que más del 50% de las empresas de servicios en la ciudad de Pucallpa, en 2024, han sido afectadas por delitos de fraude relacionados con el uso de inteligencia artificial.

4.3. Discusión de los resultados

Con respecto al objetivo general, el cual fue determinar de qué manera se comete el delito de fraude mediante el uso inteligencia artificial a las empresas de servicios de la ciudad de Pucallpa, 2024, para abordarlo se ejecutó una encuesta a 95 empresas de servicios formalizadas, las cuales fueron elegidas aleatoriamente, el cual arrojó como resultado que el 58,9% de encuestados indicaron a través de la inteligencia artificial se dan con mayor facilidad los casos de delito de fraude, asimismo, el 29,5% de encuestados señalan que la inteligencia artificial en los

casos de delito de fraude cumple un papel regular. Resultados similares fueron obtenidos por Rayo (2022) en su tesis titulada “Prototipo de detección de fraudes con tarjetas de crédito basado en inteligencia artificial aplicado a un banco peruano”. El objetivo de esta tesis fue apoyar al analista de fraudes a través de una plataforma web confiable, que permita detectar de manera oportuna los casos de fraudes en tiempo real, basado en inteligencia artificial. Los resultados experimentales en el conjunto de datos de pruebas indicaron que el modelo presenta una precisión del 48.10%, con un índice de falsos positivos de 4.35, concluyendo que se espera que esta precisión mejore conforme aumente el volumen transaccional y el modelo se ejecute progresivamente en base a la nueva información entrante. Otro resultado similar lo expresa Aldea (2020) en su tesis titulada “*El impacto de la inteligencia artificial en el sistema financiero*”, quien tuvo como objetivo hacer un recorrido histórico de la evolución de la inteligencia artificial, analizar el impacto que el “high frenquency tradign” y el trading algorítmico han tenido en los mercados financieros. Se examinaron artículos científicos, informes de organismos especializados, obras de expertos y artículos de periódicos para obtener una comprensión completa de la situación actual. Como conclusión se obtuvo, que el impacto de la inteligencia artificial en el ámbito de la ciberseguridad ha sido destacado. Aunque algunas empresas ya han incorporado esta tecnología en sus soluciones de ciberseguridad, su adopción no es generalizada. Entre las tecnologías más prometedoras en este campo se encuentran las redes neuronales artificiales, los agentes inteligentes, los algoritmos genéticos, los sistemas inmunes artificiales y los sistemas expertos.

En relación al primer objetivo específico, el cual fue establecer de qué manera se vienen ejecutando patrones anómalos mediante el uso de inteligencia

artificial a las empresas de servicios de la ciudad de Pucallpa, 2024, para abordarlo se ejecutó una encuesta a 95 empresas de servicios formalizadas, las cuales fueron elegidas aleatoriamente, el cual arrojó como resultado que el 58,9% de encuestados indicaron que la detección de patrones anómalos se da a través de la inteligencia artificial y se percibe como un componente esencial y significativo en los casos de delito de fraude. Por otro lado, Villegas (2021) en su tesis titulada "Modelo de machine learning en la detección de sitios web phishing", tuvo como objetivo primordial aplicar un sistema de detección de phishing, sustentada en un modelo de machine learning, para el rendimiento en la detección de sitios web falsos. Concluyendo que, se obtuvo que el rendimiento medio de los sistemas de detección de phishing es del 93.80%, representando la proporción de detecciones correctas en general. Además, se logró una precisión del 91.20% al clasificar correctamente los sitios web de phisihing y un 95.35% al clasificar adecuadamente los sitios web legítimos.

En cuanto al segundo objetivo específico, el cual fue precisar en qué forma vulneran la seguridad en las transacciones mediante el uso inteligencia artificial a las empresas de servicios de la ciudad de Pucallpa, 2024, para abordarlo se ejecutó una encuesta a 95 empresas de servicios formalizadas, las cuales fueron elegidas aleatoriamente, el cual arrojó como resultado que el 60% de encuestados indicaron que la vulneración de la seguridad en las transacciones es gracias a la inteligencia artificial y se percibe como un componente esencial y significativo en los casos de delito de fraude. Un resultado similar se presenta en la tesis de Cataño y Panduro (2023) en su tesis titulada "El delito informático y su incidencia en las operaciones financieras en los bancos de la provincia Coronel Portillo- Ucayali, 2022", cuyo objetivo general fue determinar como el delito de información incide en las

operaciones financieras en los bancos de la provincia de Coronel Portillo. Luego de analizar los resultados se obtuvo un nivel de confiabilidad del 95% con un Rho de Spearman 0.756. por lo tanto, se concluyó que existe correlación positiva fuerte entre el delito informático y las operaciones financieras.

Respecto al tercer objetivo específico, el cual fue caracterizar cómo afectan la eficiencia operativa mediante el uso inteligencia artificial a las empresas de servicios de la ciudad de Pucallpa, 2024, para abordarlo se ejecutó una encuesta a 95 empresas de servicios formalizadas, las cuales fueron elegidas aleatoriamente, el cual arrojó como resultado que el 45,3% de encuestados indicaron que la inteligencia artificial afecta a la eficiencia operativa y se percibe como un componente esencial y significativo en los casos de delito de fraude. Un resultado similar obtuvo Cataño y Panduro (2023) en su tesis titulada "*El delito informático y su incidencia en las operaciones financieras en los bancos de la provincia Coronel Portillo- Ucayali, 2022*", donde tuvo como objetivo determinar como el delito de información incide en las operaciones financieras en los bancos de la provincia de Coronel Portillo. Lo cual, luego de evaluar los resultados obtenidos se determinó un nivel de confiabilidad del 95% con un Rho de Spearman 0.756. por lo tanto, se concluyó que existe correlación positiva fuerte entre el delito informático y las operaciones financieras.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- El delito de fraude mediante el uso inteligencia artificial se cometió en perjuicio del más del 50% de las empresas de servicios de la ciudad de Pucallpa, 2024. La presente conclusión se sustenta en los resultados del cuestionario enfocada a analizar 95 empresas de servicios formalizadas de la ciudad de Pucallpa. Estos resultados revelaron una proporción muestral de $\overline{p} = 0.721$, siendo esta una cifra que representa más del 50%, indicando de este modo que el delito de fraude mediante el uso inteligencia artificial se cometió en perjuicio en la mayoría de los casos a las empresas de servicios de la ciudad de Pucallpa.
- Los patrones anómalos mediante el uso de inteligencia artificial se vienen ejecutando en más del 50% de las empresas de servicios de la ciudad de Pucallpa, 2024. Esta conclusión se basa en los hallazgos obtenidos del cuestionario enfocada a analizar 95 empresas de servicios formalizadas de la ciudad de Pucallpa. Dichos resultados evidenciaron una proporción muestral de $\overline{p} = 0.684$, lo cual equivale a más del 50%. Esto señala que, en la mayoría de los casos, los patrones anómalos mediante el uso de inteligencia artificial se vienen ejecutando a las empresas de servicios de la ciudad de Pucallpa.
- La vulneración de la seguridad en las transacciones mediante el uso inteligencia artificial se está produciendo en más del 50% de las empresas de servicios de la ciudad de Pucallpa, 2024. La conclusión se apoya en los descubrimientos derivados del cuestionario enfocada a analizar 95

empresas de servicios formalizadas de la ciudad de Pucallpa. Dichos resultados evidenciaron una proporción muestral de $\overline{p}$ = 0.749, esto significa que, en la mayoría de las situaciones, la vulneración de la seguridad en las transacciones mediante el uso inteligencia artificial se está produciendo en las empresas de servicios de la ciudad de Pucallpa.

- La eficiencia operativa es afectada mediante el uso inteligencia artificial en más del 50% de las empresas de servicios de la ciudad de Pucallpa, 2024. Esta conclusión se fundamenta en los resultados obtenidos del cuestionario enfocada a analizar 95 empresas de servicios formalizadas de la ciudad de Pucallpa. Tales resultados contaron con una proporción muestral de $\overline{p}$ = 0.731, esto indica que, en la mayoría de los casos, la eficiencia operativa es afectada mediante el uso inteligencia artificial.

5.2. Recomendaciones

- Se recomienda efectuar un estudio que profundice el análisis de cómo el delito de fraude y la inteligencia artificial afectan las empresas de servicios de la ciudad de Pucallpa, el cual implique la investigación exhaustiva de casos recientes, examinando detalladamente las tendencias delictivas y los métodos utilizados presentadas en cada empresa, dado que, de esta manera proporcionaría una comprensión más completa de cómo el fraude y la inteligencia artificial impactan específicamente a las empresas de servicios en Pucallpa y podría ofrecer recomendaciones prácticas para mejorar la prevención y detección de estas actividades ilícitas.
- Se recomienda desarrollar una investigación que se base en el análisis comparativo de casos previos que permita identificar patrones anómalos mediante el uso de inteligencia artificial en las empresas de servicios de la

ciudad de Pucallpa. Además, que incluya la exploración de cómo se pueden mejorar los sistemas de detección y prevención del fraude mediante la implementación de algoritmos avanzados de inteligencia artificial para garantizar que se cumplan los estándares de seguridad y protección de datos.

- Se recomienda plantear un estudio detallado que se centre en analizar cómo examinar la vulneración de la seguridad en las transacciones mediante el uso inteligencia artificial afectan las empresas de servicios de la ciudad de Pucallpa y cómo se pueden optimizar las medidas de protección existentes para garantizar que se pueda reducir al mínimo cualquier riesgo potencial en cada empresa, para que de este modo se pueda obtener un panorama claro de la importancia de la seguridad en las transacciones para las empresas en Pucallpa.
- Se recomienda ejecutar un estudio que se enfoque en examinar la eficiencia operativa afectada mediante el uso inteligencia artificial, de manera que se puedan identificar las mejoras potenciales en los procesos y la optimización de recursos, que ponen en riesgo la eficiencia y competitividad de la empresa, y cómo esto viene afectando el desempeño general de la empresa.

REFERENCIAS BIBLIOGRÁFICAS

Alcalá, C., Ochoa, M. (2022).Trastorno del espectro autista (TEA). *Rev. Fac. Med., 65(1)*, 7-20. https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0026-17422022000100007

Alcayaga, B., Dalmazzo, E., y Garrido, D. (2024). Integración de la inteligencia artificial en la administración fiscal: un análisis comparativo y multidimensional. *Revista de investigación aplicada en ciencias empresariales, 12* (1). https://iace.uv.cl/index.php/IACE/article/view/4115

Aldea, C. (2020). *El impacto de la inteligencia artificial en el sistema financiero*. [Tesis de pregrado, Universidad Pontifica Comillas] https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/37543/TFG-%20Aldea%20Torres%2C%20Carlos.pdf?sequence=1

Almonacid, J., Coronel, Y. (2020). Aplicabilidad de la inteligencia artificial y la tecnología blockchain en el derecho contractual privado. *Revista de Derecho Privado*, (38), 119-142. http://www.scielo.org.co/scielo.php?pid=S0123-43662020000100119&script=sci_arttext

Alzate, P., y Giraldo, D. (2023). Tendencias de investigación del blockchain en la cadena de suministro, transparencia, trazabilidad y seguridad. Revista Universidad y empresa, 25(44), 1-29. http://www.scielo.org.co/scielo.php?pid=S0124-46392023000100011&script=sci_arttext

Barrera, J. (2020). Control interno, su vínculo con la eficiencia operativa y la rentabilidad. *Vinculatégica EFAN,* 6(1), 734-741. https://vinculategica.uanl.mx/index.php/v/article/view/626

Berrones-Sanz, L. D. (2021). Costos operativos en el transporte de mercancía por carretera: El caso de los sistemas de construcción ligera en México. *Dirección y Organización*, (73), 5-17. https://revistadyo.es/DyO/index.php/dyo/article/view/589

Boden, M. A. (2017). Inteligencia artificial. *Turner*. https://books.google.es/books?hl=es&lr=&id=LCnYDwAAQBAJ&oi=fnd&pg=PT3&dq=INTELIGENCIA+ARTIFICIAL+&ots=dsQmvUdHlc&sig=VTikenkN1b78WfMOnUJ72GXATfc

Cajigas, L. y Pérez, G. (2023). *La incidencia de las nuevas tecnologías en el delito de fraude informático y su aplicación en la ley N° 30096 en el Perú.* [Tesis de pregrado, Universidad Andina del Cusco] https://repositorio.uandina.edu.pe/handle/20.500.12557/5739

Cando, M. y Medina, P. (2021). Prevención en ciberseguridad: enfocada a los procesos de infraestructura tecnológica. 3C TIC. *Cuadernos de desarrollo aplicados a las TIC, 10(1),* 17-41. https://dialnet.unirioja.es/descarga/articulo/7888164.pdf

Castellano, P. (2021). Inteligencia artificial y Administración de Justicia: ¿ Quo vadis, justitia?. *IDP. Revista de Internet, Derecho y Política*, (33). https://doi.org/10.7238/idp.v0i33.373817

Castro, J., Gómez, L. y Camargo, E. (2023). La investigación aplicada y el desarrollo experimental en el fortalecimiento de las competencias de la sociedad del siglo XXI. *Tecnura, 27(75),* 140-174. https://dialnet.unirioja.es/descarga/articulo/8728928.pdf

Cataño, T., y Panduro, L. (2023). *El delito informático y su incidencia en las operaciones financieras en los bancos de la provincia Coronel Portillo-*

Ucayali, 2022. [Tesis de pregrado, Universidad Nacional de Ucayali] http://repositorio.unu.edu.pe/handle/UNU/6320

Cerna, J. J. V., Quincho, L. M. S., & de los Santos, A. C. M. (2023). La vulnerabilidad de las tecnologías biométricas en la autenticación. *INGENIERÍA INVESTIGA*, 5. https://revistas.upt.edu.pe/ojs/index.php/ingenieria/article/view/866

Chamorro, A., Pupiales, S. y Hidalgo, J. (2022). Equipo de respuesta ante incidentes informáticos para la seguridad de la información (CSIRT-UPEC). *Sathiri, (18)1,* 220-229. https://revistasdigitales.upec.edu.ec/index.php/sathiri/article/view/1200/3522

Chávez, M., Jiménez, J., & Pushug, M. (2020). Análisis de confiabilidad, mantenibilidad y disponibilidad (CMD) del sistema de reinyección de agua de formación. *Revista Arbitrada Interdisciplinaria Koinonía, 5*(9), 249-267. https://dialnet.unirioja.es/servlet/articulo?codigo=7437976

Chuco, E. (2023). *Análisis del delito de fraude informático y hurto como delito previo, Cercado de Lima- 2020.* [Tesis de pregrado, Universidad Cesar Vallejo] https://repositorio.ucv.edu.pe/handle/20.500.12692/125058

Corti, H. (2016). Normas y aparatos conceptuales: dos aspectos del derecho. ISONOMÍA, (45), 141-188. https://www.scielo.org.mx/pdf/is/n45/1405-0218-is-45-00141.pdf

De la Torre, M. (2018). Gestión del riesgo organizacional de fraude y el rol de Auditoría Interna. *Contabilidad y Negocios (13) 25,* 57-69. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3237883

De Vito. E. (2023) Inteligencia artificial y chatGPT. ¿Usted leería a un autor artificial?. *Medicina, 83(2),* 329-336. http://www.scielo.org.ar/scielo.php?pid=S0025-76802023000400329&script=sci_arttext

Diaz, S., Angulo, J., Barboza, M. (2018). Análisis del delito de fraude electrónico: modalidad tarjeta de crédito. https://repository.ucc.edu.co/bitstreams/779709a1-437b-45f6-9396cf2a9838ace9/download

Estrada, A. y Alfaro, K. (2015). El método de casos como alternativa pedagógica para la enseñanza de la bibliotecología y las ciencias de la información. *Investigación bibliotecológica, 29(65),* 195-212. https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187358X2015000100009

Feria, H., Matilla, M. y Mantecón, S. (2020). La entrevista y la encuesta: ¿Métodos o técnicas de indagación empírica?. *Didáctica y Educación*, *11(3),* 62-79. https://revistas.ult.edu.cu/index.php/didascalia/article/view/992

Fundora, Y., & García, Y. (2021). La divulgación científica: una herramienta eficaz en centros de investigación. Bibliotecas. Anales de investigación, 7, 105-108. http://revistas.bnjm.cu/index.php/BAI/article/view/315

Galarza, C. (2021). Diseños de investigación experimental. *CienciAmérica: Revista de divulgación científica de la Universidad Tecnológica Indoamericana*, *10(1),* 1-7. https://dialnet.unirioja.es/servlet/articulo?codigo=7890336

García, Y., Juca, F., Torres, V. (2023). Automatización de procesos contables mediante Inteligencia Artificial: Oportunidades y desafíos para pequeños empresarios ecuatorianos. *Revista Transdiciplinaria de Estudios Sociales y*

Tecnológicos, *3*(3), 68-74. https://revista.excedinter.com/index.php/rtest/article/view/93

González, V., Sosa, K. (2020). Lista de cotejo. *Evaluación del y para el aprendizaje: instrumentos y estrategias*, *18*(3), 89-107. https://cuaieed.unam.mx/publicaciones/libro-evaluacion/pdf/Capitulo-14-LISTA-DE-COTEJO.pdf

Gutiérrez, H., Chamizo, J., & Puentes, J. (2022). Cumplimiento normativo sobre información sostenible de las empresas españolas y sus efectos en los avances de la Agenda 2030. *CIRIEC-España, revista de economía pública, social y cooperativa*, (105). https://ciriec-revistaeconomia.es/wp-content/uploads/CIRIEC_105_11_Gutierrez_et_al-1.pdf

Höhl, J. (2020). Pueblos indígenas, recursos y gobernanza. Un análisis de la consulta indígena como parte de la Evaluación de Impacto Ambiental del proyecto hidroeléctrico Añihuerraqui, Región de la Araucanía, Chile. *Investigaciones Geográficas,* (59), 28-40. https://acortar.link/lqp51I

Imbaquingo, D., Díaz, J., Saltos, T., Arciniega, S., De La Torre, J., & Jesús, J. (2020). Análisis de las principales dificultades en la auditoría informática: una revisión sistemática de literatura. *Revista Ibérica de Sistemas e Tecnologias de Informação,* *32*, 427-440. https://www.proquest.com/openview/8d965b8c754de2de0771f5153b163d33/1?pq-origsite=gscholar&cbl=1006393

León, C. (2019). Atacando el fraude con “más inteligencia”. *Revista Fasecolda*, (174), 18-21. https://revista.fasecolda.com/index.php/revfasecolda/article/view/531

Lobo, M., Gil, S., y Aguirre, A. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: Estudio comparativo: *Revista de ciencias sociales,* *29*(2), 356-372. https://dialnet.unirioja.es/servlet/articulo?codigo=8920556

López, A., Ramos, G. (2021). Acerca de los métodos teóricos y empíricos de investigación: significación para la investigación educativa. *Revista Conrado, 17(S3),* 22-31. https://conrado.ucf.edu.cu/index.php/conrado/article/download/2133/2079/

López, M. (2019). Las narrativas de la inteligencia artificial. Revista de bioética y derecho, (46), 5-28. https://scielo.isciii.es/scielo.php?pid=S1886-58872019000200002&script=sci_arttext

Mayer, L., & Oliver, G. (2020). El delito de fraude informático: Concepto y delimitación. *Revista chilena de derecho y tecnología,* *9*(1), 151-184.https://www.scielo.cl/scielo.php?pid=S0719-25842020000100151&script=sci_arttext

Mayer, L., Oliver, G. (2020). El delito de fraude informático: Concepto y delimitación. *Revista chilena de derecho y tecnología*, *9*(1), 151-184. https://www.scielo.cl/scielo.php?pid=S071925842020000100151&script=sci_arttext

Mojica, K. (2021). Inteligencia artificial para detectar corrupción en la administración pública municipal de Colombia. https://repositorio.uniandes.edu.co/entities/publication/413d53cd-aabe-478f-bec0-dd322cf7b739

Morán, A. (2021). Responsabilidad penal de la Inteligencia Artificial (IA).¿ La próxima frontera?. *Revista IUS*, 15(48), 289-323.

https://www.scielo.org.mx/scielo.php?pid=S187021472021000200289&script=sci_arttext

Moreno, J., Campos, J., Medina, Y., & Poloche, D. (2023). La inteligencia artificial como herramienta para la detección del fraude fiscal: Caso Colombia. *Revista Económica*, 11(2), 25-35. https://revistas.unl.edu.ec/index.php/economica/article/view/1677

Moreno, J., Campos, J., Medina, Y., Poloche, D. (2023). La inteligencia artificial como herramienta para la detección del fraude fiscal: Caso Colombia. *Revista Económica, 11*(2), 25-35. https://doi.org/10.54753/rve.v11i2.1677

Moreno, J., Campos, J., Medina, Y., Poloche, D. (2023). La inteligencia artificial como herramienta para la detección del fraude fiscal: Caso Colombia. *Revista Económica*, 11(2), 25-35. https://revistas.unl.edu.ec/index.php/economica/article/view/1677

Pacheco, D. (2022). Seguridad en redes de comunicaciones: Perspectivas y desafíos. Ingeniare. *Revista chilena de ingeniería, 30(2),* 215-217. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S071833052022000200215

Pardo, A. (2018). *Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, distrital judicial de Lima, 2018*. [Tesis de posgrado, Universidad Cesar Vallejo] https://repositorio.ucv.edu.pe/handle/20.500.12692/20372

Pavón, D., Villa, L., Rueda, M. y Xavier, E. (2019). Control interno de inventario como recurso competitivo en una PyME de Guayaquil. *Revista Venezolana de Gerencia, 24(87),* 860-873. https://www.redalyc.org/journal/290/29060499014/html/

Ramos, C. (2020). Los alcances de una investigación. *CienciAmérica, 9(3*). https://dialnet.unirioja.es/descarga/articulo/7746475.pdf

Rayo, C. (2020). *Prototipo de detección de fraudes con tarjetas de crédito basado en la inteligencia artificial aplicado a un banco peruano*. [Tesis de pregrado, Universidad De Lima] https://repositorio.ulima.edu.pe/handle/20.500.12724/15294

Robles, B. (2019). Población y muestra. *Pueblo continente, 30(1),* 245-247. http://doi.org/10.22497/PuebloCont.301.30121

Rouhiainen, L. (2018). Inteligencia artificia. *Madrid: Alienta Editorial*, 20-21. https://planetadelibrosec0.cdnstatics.com/libros_contenido_extra/40/39308_Inteligencia_artificial.pdf

Ruiz, V., & Masera, O. (2021). Energías renovables en el sector residencial rural en México: estado del arte y oportunidades de colaboración interinstitucional. *RINDERESU,* *5*(1).http://rinderesu.com/index.php/rinderesu/article/view/68/72

Sullca, E. (2023). Técnicas de inteligencia artificial para la detección de deepfakes y su impacto en la veracidad de los contenidos en línea. *International Journal of Systems Engineering*, *4*(2), 06-09. http://systemjournal.org/index.php/ijse/article/view/39

Sureda, J., Cerdá, A., Calvo, A., & Forgas, R. (2020). Las conductas fraudulentas del alumnado universitario español en las evaluaciones: valoración de su gravedad y propuestas de sanciones a partir de un panel de expertos. Revista de Investigación Educativa, 38(1), 201-219. https://revistas.um.es/rie/article/view/358781

Tejero, H. (2023). ¿Qué es la autenticación robusta y por qué dependen de ella los dispositivos conectados a la red? *Revista española electrónica*, (828), 58-59. https://dialnet.unirioja.es/servlet/articulo?codigo=9170784

Villegas, J. (2021). *Modelo de machine learning en la detección de sitios web phising*. [Tesis de posgrado, Universidad de Señor Sipán] https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/8897/Villegas%20Cubas%2C%20Juan%20El%C3%ADas.pdf?sequence=1&isAllowed=y

ANEXOS

Anexo 1: Operacionalización de las Variables

EL DELITO DE FRAUDE MEDIANTE EL USO DE LA INTELIGENCIA ARTIFICIAL A LAS EMPRESAS DE SERVICIOS DE LA CIUDAD DE PUCALLPA, 2024.					
VARIABLES	**DEFINICIÓN CONCEPTUAL**	**DEFINCIÓN OPERACIONAL**	**DIMENSIONES**	**INDICADORES**	**ESCALA DE MEDICIÓN**
Inteligencia artificial	"La inteligencia artificial se refiere a la capacidad de las máquinas para realizar tareas que normalmente requieren inteligencia humana, estas tareas incluyen el aprendizaje, el razonamiento, la percepción visual, el reconocimiento del lenguaje natural, la toma de decisiones y la resolución de problemas". (Rouhiainen, 2018)	"La inteligencia artificial es un campo de la informática que busca desarrollar sistemas capaces de emular y ejecutar funciones cognitivas humanas de manera autónoma, esta disciplina se apoya en un conjunto diverso de técnicas, algoritmos y modelos computacionales con el objetivo de capacitar a las máquinas para realizar tareas que van más allá de las capacidades tradicionales de la programación convencional". (López, 2019)	**Detección de patrones anómalos**	Identificación de transacciones inusuales	Ordinal
				Reconocimiento de Comportamientos Atípicos	
				Alertas de Fraude	
			Seguridad en las Transacciones	Autenticación Robusta	
				Protección contra Ataques	
				Seguridad en la Comunicación	
			Eficiencia operativa	Recursos utilizados por transacción detectada	
				Costo operativo	
				Disponibilidad del sistema	
Delito de fraude	"El delito de fraude se refiere a cualquier acción o conducta engañosa, astuta o fraudulenta realizada con la intención de obtener beneficios económicos o financieros de manera ilícita o injusta. Esta conducta implica el uso de engaños, mentiras, falsificaciones u otros medios deshonestos para inducir a otra persona o entidad a actuar de una manera que resulte en pérdida económica para ellos o en beneficio injusto para el perpetrador del fraude". (Lobo, Gil y Aguirre, 2023)	"El delito de fraude se refiere al uso indebido de cualquier medio, sea un sistema informático, redes o dispositivos electrónicos para realizar actividades fraudulentas, esto puede incluir el acceso no autorizado a información confidencial, la manipulación de datos, el robo de identidad en línea y la distribución de software malicioso" (Moreno, et. al, 2023).	**Cumplimiento normativo**	Transacciones que cumplen con la normativa	Ordinal
				Actualización normativa	
				Auditorías exitosas	
			Gravedad del fraude	Monto promedio de fraude	
				Casos de fraude	
				Impacto en las partes afectadas	
			Eficiencia en la Investigación y Respuesta	Respuesta a incidentes	
				Resolución de casos	
				Colaboración interinstitucional	

Anexo 2: Matriz de Consistencia

EL DELITO DE FRAUDE MEDIANTE EL USO DE LA INTELIGENCIA ARTIFICIAL A LAS EMPRESAS DE SERVICIOS DE LA CIUDAD DE PUCALLPA, 2024.				
PROBLEMA GENERAL	**OBJETIVO GENERAL**	**HIPÓTESIS GENERAL**	**VARIABLE 1**	**METODOLOGÍA**
¿De qué manera se comete el delito de fraude mediante el uso inteligencia artificial a las empresas de servicios de la ciudad de Pucallpa, 2024?	Determinar de qué manera se comete el delito de fraude mediante el uso inteligencia artificial a las empresas de servicios de la ciudad de Pucallpa, 2024.	El delito de fraude mediante el uso inteligencia artificial se cometió en perjuicio en más del 50% de las empresas de servicios de la ciudad de Pucallpa, 2024	INTELIGENCIA ARTIFICIAL	TIPO DE INVESTIGACIÓN Aplicado (Castro, 2023, p.148)
				NIVEL DE INVESTIGACIÓN Descriptivo (Ramos, 2020, p.24)
PROBLEMA ESPECÍFICO 1	**OBJETIVO ESPECÍFICO 1**	**HIPÓTESIS ESPECÍFICA 1**		MÉTODO DE INVESTIGACIÓN Hipotético deductivo (López y Ramos, 2021, p.27)
¿De qué manera se vienen ejecutando patrones anómalos mediante el uso de inteligencia artificial a las empresas de servicios de la ciudad de Pucallpa, 2024?	Establecer de qué manera se vienen ejecutando patrones anómalos mediante el uso de inteligencia artificial a las empresas de servicios de la ciudad de Pucallpa, 2024.	Los patrones anómalos mediante el uso de inteligencia artificial se vienen ejecutando en más del 50% de las empresas de servicios de la ciudad de Pucallpa, 2024.		DISEÑO DE LA INVESTIGACIÓN No Experimental transversal (Galarza, 2021, p.150)
PROBLEMA ESPECÍFICO 2	**OBJETIVO ESPECÍFICO 2**	**HIPÓTESIS ESPECÍFICA 2**	**VARIABLE 2**	
¿De qué forma vulneran la seguridad en las transacciones mediante el uso inteligencia artificial a las empresas de servicios de la ciudad de Pucallpa, 2024?	Precisar en qué forma vulneran la seguridad en las transacciones mediante el uso inteligencia artificial a las empresas de servicios de la ciudad de Pucallpa, 2024.	La vulneración de la seguridad en las transacciones mediante el uso inteligencia artificial se está produciendo en más del 50% de las empresas de servicios de la ciudad de Pucallpa, 2024.	DELITO DE FRAUDE	POBLACIÓN: La población de interés para la investigación está compuesta por 125 empresas de servicios, formalizadas de la ciudad de Pucallpa. (N=125). MUESTRA: Se realizó un muestreo aleatorio simple, por lo cual la muestra está conformada por 95 empresas de servicios formalizadas (n=95)
PROBLEMA ESPECÍFICO 3	**OBJETIVO ESPECÍFICO 3**	**HIPÓTESIS ESPECÍFICA 3**		
¿Cómo afectan la eficiencia operativa mediante el uso inteligencia artificial dentro de las empresas de servicios de la ciudad de Pucallpa, 2024?	Caracterizar cómo afectan la eficiencia operativa mediante el uso inteligencia artificial a las empresas de servicios de la ciudad de Pucallpa, 2024.	La eficiencia operativa es afectada mediante el uso inteligencia artificial en más del 50% de las empresas de servicios de la ciudad de Pucallpa, 2024.		TÉCNICA: Encuesta INSTRUMENTO: Cuestionario

Anexo 3: Instrumento de recolección de datos

EL DELITO DE FRAUDE MEDIANTE EL USO DE LA INTELIGENCIA ARTIFICIAL A LAS EMPRESAS DE SERVICIOS DE LA CIUDAD DE PUCALLPA, 2024

CUESTIONARIO DE LA VARIABLE INTELIGENCIA ARTIFICIAL

Objetivo: Determinar de qué manera se comete el delito de fraude mediante el uso inteligencia artificial a las empresas de servicios de la ciudad de Pucallpa, 2024.

Instrucciones: En las siguientes preguntas, sírvase responder marcando, con un aspa, un numeral entre el 1 y el 5, siendo equivalente a:

1	2	3	4	5
Nunca	Casi nunca	A veces	Casi siempre	Siempre

Dimensión 1.1: Detección de patrones anómalos

N°	Ítems	Valoración				
		1	2	3	4	5
1	¿Realizan revisiones periódicas de las transacciones en busca de patrones anómalos?					
2	¿La detección de transacciones inusuales es parte de un sistema de cumplimiento normativo?					

3	¿El reconocimiento de comportamientos atípicos se basa en modelos estadísticos?					
4	¿El reconocimiento de comportamientos atípicos es parte de un sistema de gestión de riesgos?					
5	¿La detección de patrones anómalos incluye la identificación de actividades fraudulentas?					
6	¿Las alertas de fraude están integradas con sistemas de gestión de riesgos?					

Dimensión 1.2: Seguridad en las transacciones

N°	Ítems	Valoración				
		1	2	3	4	5
7	¿La autenticación robusta utiliza múltiples factores para verificar la identidad?					
8	¿La autenticación robusta ayuda a prevenir el acceso no autorizado a cuentas?					
9	¿Dentro de su empresa se han implementado medidas para prevenir ataques de phishing o suplantación de identidad?					
10	¿Se monitorean activamente las transacciones en busca de posibles intentos de intrusión o ataques cibernéticos?					
11	¿Las comunicaciones entre los sistemas involucrados en las transacciones de su empresa están encriptadas?					
12	¿La empresa utiliza redes privadas virtuales (VPN) para garantizar la seguridad de las comunicaciones?					

Dimensión 1.3: Eficiencia operativa

N°	Ítems	Valoración				
		1	2	3	4	5
13	¿Se emplean todos los recursos de la empresa por transacción detectada para mantener una eficiencia operativa en la empresa?					
14	¿La empresa al emplear todos sus recursos por transacción detectada ha aumentado sus utilidades?					
15	¿El costo operativo que abarca de la implementación de la inteligencia artificial ha aumentado la eficiencia operativa en la empresa?					
16	¿El costo operativo de la inteligencia artificial en la empresa justifica los beneficios que aporta para las utilidades de la entidad?					
17	¿La disponibilidad del sistema de inteligencia artificial permite una eficiencia operativa durante todo el día?					
18	¿La eficiencia de la empresa ha mejorado desde la implementación de la inteligencia artificial?					

EL DELITO DE FRAUDE MEDIANTE EL USO DE LA INTELIGENCIA ARTIFICIAL A LAS EMPRESAS DE SERVICIOS DE LA CIUDAD DE PUCALLPA, 2024

CUESTIONARIO DE LA VARIABLE DELITO DE FRAUDE

Objetivo: Determinar de qué manera se comete el delito de fraude mediante el uso inteligencia artificial a las empresas de servicios de la ciudad de Pucallpa, 2024.

Instrucciones: En las siguientes preguntas, sírvase responder marcando, con un aspa, un numeral entre el 1 y el 5, siendo equivalente a:

1	2	3	4	5
Nunca	Casi nunca	A veces	Casi siempre	Siempre

Dimensión 2.1: Cumplimiento normativo

N°	Ítems	Valoración				
		1	2	3	4	5
19	¿Las transacciones realizadas en la empresa cumplen con la normativa?					
20	¿Se emplean sistemas de monitoreo automatizado para detectar actividades sospechosas en las transacciones y cumplir con los requisitos normativos?					

21	¿En la empresa se realizan actualizaciones de la normativa para evitar fraudes en las transacciones?					
22	¿La actualización de la normativa permite estar al día de conocimientos nuevos y así evitar fraudes modernos al realizar transacciones por la empresa?					
23	¿Las auditorias empleadas en la empresa ayudan a su desarrollo eficiente evitando fraudes en ella?					
24	¿Las transacciones cumplen con los estándares regulatorios propuestos por las auditorias?					

Dimensión 2.2: Gravedad del fraude

N°	Ítems	Valoración				
		1	2	3	4	5
25	¿Su empresa se establece un monto promedio de fraude?					
26	¿Utiliza algún sistema para evaluar la gravedad del fraude respecto a sus utilidades totales?					
27	¿Dentro de su empresa se han dado pocos casos de fraude?					
28	¿Se monitorean activamente los casos de fraude que se han dado en su empresa para evitar que este se realice de nuevo?					
29	¿El impacto a las partes afectadas está en el rango mínimo?					

30	¿El impacto en las partes afectadas ha sido calificado en una escala de gravedad para poder recuperarse más eficientemente?					

Dimensión 2.3: Eficiencia en la investigación y respuesta

N°	Ítems	Valoración				
		1	2	3	4	5
31	¿Se ha respondido a todos los incidentes de fraude registrados?					
32	¿El tiempo promedio de respuesta a incidentes de fraude ha disminuido generando eficiencia en la investigación y respuesta del caso?					
33	¿Se han resuelto los casos de fraude se han resuelto satisfactoriamente?					
34	¿Los casos resueltos de fraude permiten tener un historial exitoso para evitar próximos casos de fraude en la empresa?					
35	¿Se ha colaborado con otras instituciones para investigar casos de fraude ocurridos?					
36	¿Se han establecido protocolos de colaboración interinstitucional para mejorar la eficiencia en la investigación y respuesta al fraude?					

Anexo 4: Validación del instrumento de recolección de datos

UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

FICHA DE VALIDACIÓN DEL CUESTIONARIO MEDIANTE EL JUICIO DE EXPERTOS

I. DATOS PERSONALES:

1.1. APELLIDOS Y NOMBRES DEL INFORMANTE: ASTOHUAMAN HUARANGA, ALEX DAVIS

1.2. GRADO ACADÉMICO / PROFESIÓN: DOCTOR EN ADMINISTRACIÓN / ABOGADO

1.3. INSTITUCIÓN DONDE LABORA: UNIVERSIDAD NACIONAL INTERCULTURAL DE LA AMAZONÍA

1.4. TÍTULO DE LA INVESTIGACIÓN: EL DELITO DE FRAUDE MEDIANTE EL USO DE LA INTELIGENCIA ARTIFICIAL A LAS EMPRESAS DE SERVICIOS DE LA CIUDAD DE PUCALLPA, 2024.

1.5. NOMBRE DEL INSTRUMENTO: CUESTIONARIO

II. ASPECTOS A EVALUAR: (CALIFICACIÓN CUANTITATIVA)

VARIABLE 1: INTELIGENCIA ARTIFICIAL

INDICADORES DEL INSTRUMENTO DE EVALUACIÓN	CRITERIOS CUALITATIVOS CUANTITATIVOS	Deficiente (01-09)	Regular (10-13)	Bueno (14-16)	Muy bueno (17-18)	Excelente (19-20)
01 CLARIDAD	Está formulado con lenguaje apropiado					19
02. OBJETIVIDAD	Está expresado con conductas observables					20
03. ACTUALIDAD	Adecuado al avance de la ciencia y calidad				18	
04. ORGANIZACIÓN	Existe una organización lógica del instrumento				18	
05. SUFICIENCIA	Valora los aspectos en cantidad y calidad				18	
06. INTENCIONALIDAD	Adecuado para cumplir con los objetivos					19
07. CONSISTENCIA	Basado en el aspecto teórico científico del tema de estudios					20
08. COHERENCIA	Entre las hipótesis, dimensiones e indicadores				18	
09. METODOLOGÍA	Las estrategias responden al propósito del estudio					19
10. OPORTUNIDAD	Genera nuevas pautas para la investigación y construcción de teorías					19
	Sub Total				72	116
	TOTAL					19

VARIABLE 2: DELITO DE FRAUDE

INDICADORES DEL INSTRUMENTO DE EVALUACIÓN	CRITERIOS CUALITATIVOS CUANTITATIVOS	Deficiente (01-09)	Regular (10-13)	Bueno (14-16)	Muy bueno (17-18)	Excelente (19-20)
01 CLARIDAD	Está formulado con lenguaje apropiado				18	
02. OBJETIVIDAD	Está expresado con conductas observables				18	
03. ACTUALIDAD	Adecuado al avance de la ciencia y calidad					20
04. ORGANIZACIÓN	Existe una organización lógica del instrumento					20
05. SUFICIENCIA	Valora los aspectos en cantidad y calidad				18	
06. INTENCIONALIDAD	Adecuado para cumplir con los objetivos				18	
07. CONSISTENCIA	Basado en el aspecto teórico científico del tema de estudios					19
08. COHERENCIA	Entre las hipótesis, dimensiones e indicadores					19
09. METODOLOGÍA	Las estrategias responden al propósito del estudio					19
10. OPORTUNIDAD	Genera nuevas pautas para la investigación y construcción de teorías					19
	Sub Total				72	116
	TOTAL					19

Leyenda: 01-13 Improcedente ; 14-16 Aceptable con recomendación ; 17-20 Aceptable

Lugar y Fecha: Pucallpa - 13-07-2024

Firma del experto: .....

DNI: 44854139

UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

FICHA DE VALIDACIÓN DEL CUESTIONARIO MEDIANTE EL JUICIO DE EXPERTOS

I. DATOS PERSONALES:

1.1. APELLIDOS Y NOMBRES DEL INFORMANTE: **NAVARRO JANAMPA, FÉLIX**

1.2. GRADO ACADÉMICO: **DOCTOR EN ADMINISTRACIÓN**

1.3. INSTITUCIÓN DONDE LABORA: **UNIVERSIDAD NACIONAL DE UCAYALI**

1.4. TÍTULO DE LA INVESTIGACIÓN: **EL DELITO DE FRAUDE MEDIANTE EL USO DE LA INTELIGENCIA ARTIFICIAL A LAS EMPRESAS DE SERVICIOS DE LA CIUDAD DE PUCALLPA, 2024.**

1.5. NOMBRE DEL INSTRUMENTO: **CUESTIONARIO**

II. ASPECTOS A EVALUAR: (CALIFICACIÓN CUANTITATIVA)

VARIABLE 1: INTELIGENCIA ARTIFICIAL

INDICADORES DEL INSTRUMENTO DE EVALUACIÓN	CRITERIOS CUALITATIVOS CUANTITATIVOS	Deficiente (01-09)	Regular (10-13)	Bueno (14-16)	Muy bueno (17-18)	Excelente (19-20)
01 CLARIDAD	Está formulado con lenguaje apropiado					19
02. OBJETIVIDAD	Está expresado con conductas observables					20
03. ACTUALIDAD	Adecuado al avance de la ciencia y calidad				18	
04. ORGANIZACIÓN	Existe una organización lógica del instrumento					19
05. SUFICIENCIA	Valora los aspectos en cantidad y calidad				18	
06. INTENCIONALIDAD	Adecuado para cumplir con los objetivos				18	
07. CONSISTENCIA	Basado en el aspecto teórico científico del tema de estudios					19
08. COHERENCIA	Entre las hipótesis, dimensiones e indicadores					20
09. METODOLOGÍA	Las estrategias responden al propósito del estudio				18	
10. OPORTUNIDAD	Genera nuevas pautas para la investigación y construcción de teorías					19
	Sub Total				72	116
	TOTAL					19

VARIABLE 2: DELITO DE FRAUDE

INDICADORES DEL INSTRUMENTO DE EVALUACIÓN	CRITERIOS CUALITATIVOS CUANTITATIVOS	Deficiente (01-09)	Regular (10-13)	Bueno (14-16)	Muy bueno (17-18)	Excelente (19-20)
01 CLARIDAD	Está formulado con lenguaje apropiado				18	
02. OBJETIVIDAD	Está expresado con conductas observables				18	
03. ACTUALIDAD	Adecuado al avance de la ciencia y calidad					20
04. ORGANIZACIÓN	Existe una organización lógica del instrumento					20
05. SUFICIENCIA	Valora los aspectos en cantidad y calidad				18	
06. INTENCIONALIDAD	Adecuado para cumplir con los objetivos				18	
07. CONSISTENCIA	Basado en el aspecto teórico científico del tema de estudios					19
08. COHERENCIA	Entre las hipótesis, dimensiones e indicadores					19
09. METODOLOGÍA	Las estrategias responden al propósito del estudio					19
10. OPORTUNIDAD	Genera nuevas pautas para la investigación y construcción de teorías					19
	Sub Total				72	116
	TOTAL					19

Leyenda: 01-13 Improcedente ; 14-16 Aceptable con recomendación ; 17-20 Aceptable

Lugar y Fecha: Pucallpa, 12/07/2024

Firma del experto: .....

DNI: 00109352

UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

FICHA DE VALIDACIÓN DEL CUESTIONARIO MEDIANTE EL JUICIO DE EXPERTOS

I. DATOS PERSONALES:

1.1. APELLIDOS Y NOMBRES DEL INFORMANTE: **CAMPOS BARRETO, ANIBAL**

1.2. GRADO ACADÉMICO / PROFESIÓN: **DOCTOR EN ADMINISTRACIÓN / ABOGADO**

1.3. INSTITUCIÓN DONDE LABORA: **UNIVERSIDAD NACIONAL DE UCAYALI**

1.4. TÍTULO DE LA INVESTIGACIÓN: **EL DELITO DE FRAUDE MEDIANTE EL USO DE LA INTELIGENCIA ARTIFICIAL A LAS EMPRESAS DE SERVICIOS DE LA CIUDAD DE PUCALLPA, 2024.**

1.5. NOMBRE DEL INSTRUMENTO: **CUESTIONARIO**

II. ASPECTOS A EVALUAR: (CALIFICACIÓN CUANTITATIVA)

VARIABLE 1: INTELIGENCIA ARTIFICIAL

INDICADORES DEL INSTRUMENTO DE EVALUACIÓN	CRITERIOS CUALITATIVOS CUANTITATIVOS	Deficiente (01-09)	Regular (10-13)	Bueno (14-16)	Muy bueno (17-18)	Excelente (19-20)
01 CLARIDAD	Está formulado con lenguaje apropiado				18	
02. OBJETIVIDAD	Está expresado con conductas observables				17	
03. ACTUALIDAD	Adecuado al avance de la ciencia y calidad					20
04. ORGANIZACIÓN	Existe una organización lógica del instrumento					19
05. SUFICIENCIA	Valora los aspectos en cantidad y calidad				18	
06. INTENCIONALIDAD	Adecuado para cumplir con los objetivos					19
07. CONSISTENCIA	Basado en el aspecto teórico científico del tema de estudios				18	
08. COHERENCIA	Entre las hipótesis, dimensiones e indicadores				18	
09. METODOLOGÍA	Las estrategias responden al propósito del estudio					19
10. OPORTUNIDAD	Genera nuevas pautas para la investigación y construcción de teorías				18	
	Sub Total				107	77
	TOTAL					18

VARIABLE 2: DELITO DE FRAUDE

INDICADORES DEL INSTRUMENTO DE EVALUACIÓN	CRITERIOS CUALITATIVOS CUANTITATIVOS	Deficiente (01-09)	Regular (10-13)	Bueno (14-16)	Muy bueno (17-18)	Excelente (19-20)
01 CLARIDAD	Está formulado con lenguaje apropiado					19
02. OBJETIVIDAD	Está expresado con conductas observables					19
03. ACTUALIDAD	Adecuado al avance de la ciencia y calidad					20
04. ORGANIZACIÓN	Existe una organización lógica del instrumento					19
05. SUFICIENCIA	Valora los aspectos en cantidad y calidad				18	
06. INTENCIONALIDAD	Adecuado para cumplir con los objetivos				18	
07. CONSISTENCIA	Basado en el aspecto teórico científico del tema de estudios				18	
08. COHERENCIA	Entre las hipótesis, dimensiones e indicadores					19
09. METODOLOGÍA	Las estrategias responden al propósito del estudio				18	
10. OPORTUNIDAD	Genera nuevas pautas para la investigación y construcción de teorías					20
	Sub Total				72	116
	TOTAL					19

Leyenda: 01-13 Improcedente ; 14-16 Aceptable con recomendación ; 17-20 Aceptable

Lugar y Fecha: Pucallpa - 12-07-2024

Firma del experto: .....

DNI: 22508611