UNIVERSIDAD ANDINA

NESTOR CACERES VELASQUEZ

FACULTAD DE CIENCIAS JURÍDICAS Y POLÍTICAS

ESCUELA PROFECIONAL DE: DERECHO

INAPLICACIÓN ATÍPICA DE LA INTELIGENCIA ARTIFICIAL Y FRAUDE EN DELITOS CONTRA LA FE PÚBLICA - PUNO 2023

TESIS PRESENTADA POR:

Bach: JOSÉ FERNANDO MAMANI CONDORI

PARA OPTAR EL TÍTULO PROFESIONAL DE:

ABOGADO

JULIACA – PERÚ

2025

UNIVERSIDAD ANDINA

NÉSTOR CÁCERES VELÁSQUEZ

FACULTAD DE CIENCIAS JURÍDICAS Y POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO

INAPLICACIÓN ATÍPICA DE LA INTELIGENCIA ARTIFICIAL Y FRAUDE EN DELITOS CONTRA LA FE PÚBLICA – PUNO 2023

TESIS PRESENTADA POR:

Bach. JOSE FERNANDO MAMANI CONDORI

PARA OPTAR EL TÍTULO PROFESIONAL DE:

ABOGADO

APROBADA POR EL JURADO REVISOR:

PRESIDENTE : _____
Dra. KATTY AGRIPINA PEREZ ORDOÑEZ

PRIMER MIEMBRO : _____
Dr. WALTHER MARCELINO NIETO PORTOCARRERO

SEGUNDO MIEMBRO : _____
Mgtr. JULIO CESAR CHUCUYA ZAGA

ASESOR DE TESIS : _____
Dr. JAVIER ROMULO QUISPE ZAPANA

LÍNEA DE INVESTIGACIÓN: DERECHO PÚBLICO – P05

RESOLUCIÓN N° 00205-2025-D/FCJP-UANCV

Juliaca, 26 de septiembre de 2025.

Vistos: El expediente, **2025-C-3603** presentado por el Bachiller en Derecho **Sr. JOSE FERNANDO MAMANI CONDORI,** quien solicita nominación de jurados, fecha y hora para rendir el examen de sustentación de borrador de tesis denominado: **INAPLICACIÓN ATÍPICA DE LA INTELIGENCIA ARTIFICIAL Y FRAUDE EN DELITOS CONTRA LA FE PÚBLICA - PUNO 2023**, línea de investigación: **DERECHO PÚBLICO - P05**, para optar el Título Profesional de **ABOGADO** y;

CONSIDERANDO:

Que, de conformidad al Reglamento de Grados y Títulos de la Facultad de Ciencias Jurídicas y Políticas, Escuela Profesional de Derecho, concordante con el Reglamento General de Grados y Títulos de la UANCV, es procedente acceder a la petición del interesado.

Y estando, la opinión favorable del Director de la Unidad de Investigación y el Decano de la Facultad de Ciencias Jurídicas y Políticas y las atribuciones que confiere el artículo 28ª del Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos, Resolución Nª 0294-2023-UANCV-CU-R.

RESUELVE:

Primero.- **DECLARAR APTO** el informe final de la investigación (Borrador de Tesis), por tanto debe señalarse lugar, día y hora para la sustentación del borrador de tesis, en forma presencial, presentado por el Bach. **Sr. JOSE FERNANDO MAMANI CONDORI,** para optar el Título Profesional de **ABOGADO**, el mismo que se llevará a cabo el próximo **viernes, 03 de Octubre de 2025 a las 4:30:00 PM.** lugar **FILIAL PUNO - SALON DE GRADOS JR. TACNA N° 787.**

Segundo.- **Designar** como Jurados, para la evaluación del examen de sustentación de tesis referido, Integrado por los siguientes docentes:

Presidente del jurado : **Dra. KATTY AGRIPINA PEREZ ORDOÑEZ**

Primer miembro : **Dr. WALTHER MARCELINO NIETO PORTOCARRERO**

Segundo miembro : **Mgtr. JULIO CESAR CHUCUYA ZAGA**

ASESOR:

Dr. JAVIER ROMULO QUISPE ZAPANA

Tercero.- La Comisión de Grados y Títulos de la Facultad, Secretaria Académica y Administrativa quedan encargadas del cumplimiento de la presente resolución.

Regístrese, comuníquese y archívese.

UNIVERSIDAD ANDINA "NESTOR CÁCERES VELÁSQUEZ"
Dr. JOSÉ DOMINGO CHOQUEHUANCA CALCINA
DECANO
FAC. Cs. JURÍDICAS Y POLÍTICAS

UNIVERSIDAD ANDINA NÉSTOR CÁCERES VELÁSQUEZ DECANO JULIACA

DISTRIBUCIÓN:
DECANATURA FCJP, INTERESADO.
ARCH. FTChV/ncv.

UNIVERSIDAD ANDINA "Néstor Cáceres Velásquez"
Facultad de Ciencias Jurídicas y Políticas
UNIDAD DE INVESTIGACIÓN

DERECHO

RESOLUCIÓN Nº 0354-2025-UI-FCJP-UANCV-J

Juliaca, 16 de junio de 2025

VISTOS:

El Expediente: **2025-CU-4153** de fecha **06 de junio de 2025**, presentado por el **Bach. JOSE FERNANDO MAMANI CONDORI,** quien solicita Revisión del Informe Final de la Investigación (borrador de Tesis) y el **Anexo (04 o 05) "Ficha de Opinión del Informe Final de la Investigación (borrador de Tesis)"** que fue revisada por el Comité de Investigación de la Facultad de Ciencias Jurídicas y Políticas, Escuela Profesional de Derecho.

CONSIDERANDO:

Que, las Unidades de Investigación son unidades académicas que agrupan a docentes y estudiantes de diversas disciplinas, en razón del desarrollo de investigación científica, tecnológica y humanista de acuerdo al Estatuto Universitario Modificado 2020 de nuestra primera Casa Superior de Estudios.

Que, el **Bach.** JOSE FERNANDO MAMANI CONDORI, quien solicita la revisión del Informe Final de la Investigación (borrador de Tesis) del tema titulado**: INAPLICACIÓN ATÍPICA DE LA INTELIGENCIA ARTIFICIAL Y FRAUDE EN DELITOS CONTRA LA FE PÚBLICA - PUNO 2023**, línea de investigación:. **DERECHO PÚBLICO - P05,** conducente para optar el Título profesional de **ABOGADO.**

Que, al haberse cumplido con los requisitos exigidos por el Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos plasmado en la Resolución Nº 0294-2023-UANCV-CU-R.

Que, el Comité de Investigación emitió su opinión favorable al Informe Final de la Investigación (borrador de Tesis).

Que, el Director de la Unidad de Investigación de la Facultad de Ciencias Jurídicas y Políticas, Escuela Profesional de Derecho, corroboro el asesoramiento en el Informe Final de la Investigación (borrador de Tesis) del ASESOR Dr. JAVIER ROMULO QUISPE ZAPANA,

Estando, la opinión favorable del comité de Investigación, en concordancia con el Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos Resolución Nº 0294-2023-UANCV-CU-R, de conformidad a lo que establece la Ley Universitaria Nº 30220, Ley de Creación de la UANCV Nº 23738 y Modificatoria Nº 24661 y el Estatuto de la UANCV, que confiere facultades a la unidad de Investigación de la Facultad de Ciencias Jurídicas y Políticas.

SE RESUELVE:

ARTICULO PRIMERO.- APROBAR Y AUTORIZAR EL INFORME FINAL DE LA INVESTIGACIÓN (BORRADOR DE TESIS) para la **REVISIÓN DE SIMILITUD TURNITIN**, del tema titulado: **INAPLICACIÓN ATÍPICA DE LA INTELIGENCIA ARTIFICIAL Y FRAUDE EN DELITOS CONTRA LA FE PÚBLICA - PUNO 2023**, presentado por el **Bach. JOSE FERNANDO MAMANI CONDORI**, para optar el Título Profesional de **ABOGADO**, en virtud de los considerandos expuestos.

ARTICULO SEGUNDO.- RATIFICAR, como ASESOR al **Dr. JAVIER ROMULO QUISPE ZAPANA.**

ARTICULO TERCERO.- DISPONER que la facultad, secretarias académicas y administrativas, quedan encargados del cumplimiento de la presente resolución.

Regístrese, comuníquese y archívese.

UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ" – DECANO – JULIACA

Dr. José Domingo Choquehuanca Calcina
DECANO
FAC. Cs. JURÍDICAS Y POLÍTICAS

UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ" – DIRECCIÓN – JULIACA

UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ"
M.J. LUIS CHAYNA AGUILAR
DIRECTOR (e)
UNIDAD DE INVESTIGACIÓN
FAC. Cs. JURÍDICAS Y POLÍTICAS

DISTRIBUCIÓN:
DECANATURA FCJP, INTERESADO

UNIVERSIDAD ANDINA "Néstor Cáceres Velásquez"
Facultad de Ciencias Jurídicas y Políticas
UNIDAD DE INVESTIGACIÓN

DERECHO

RESOLUCIÓN Nº 658-2024-UI-FCJP-UANCV-J

Juliaca, 17 de octubre de 2024

VISTOS:

El Expediente: **2024-CU-14835** de fecha **14 de octubre de 2024**, el cual solicita Revisión de propuesta de Investigación y el **Anexo (02 o 03) "Ficha de Opinión de la Propuesta de Investigación"** que fue revisada por el Comité de Investigación de la Facultad de Ciencias Jurídicas y Políticas, Escuela Profesional de Derecho.

CONSIDERANDO:

Que, las Unidades de Investigación son unidades académicas que agrupan a docentes y estudiantes de diversas disciplinas, en razón del desarrollo de investigación científica, tecnológica y humanista de acuerdo al Estatuto Universitario Modificado 2020 de nuestra primera Casa Superior de Estudios.

Que, el (la) **Bach.** JOSE FERNANDO MAMANI CONDORI, quien solicita la revisión y aprobación de la propuesta de Investigación de **Título: INAPLICACIÓN ATÍPICA DE LA INTELIGENCIA ARTIFICIAL Y FRAUDE EN DELITOS CONTRA LA FE PÚBLICA - PUNO 2023**, conducente para optar el Título profesional de **ABOGADO(A).**

Que, al haberse cumplido con los requisitos exigidos por el Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos plasmado en la Resolución Nº 0294-2023-UANCV-CU-R.

Que, el Comité de Investigación emitió su opinión favorable a la propuesta de investigación.

Que, el Director de la Unidad de Investigación de la Facultad de Ciencias Jurídicas y Políticas, Escuela Profesional de Derecho, corroboro la propuesta del ASESOR Dr. JAVIER ROMULO QUISPE ZAPANA, quien debe estar acreditado y facultado para orientar y ayudar al asesorado en el proceso de elaboración del trabajo de investigación (Tesis) de acuerdo a la DIRECTIVA Nº 004-2019-UANCV-VRAD-OI; y,

Estando, la opinión favorable del comité de Investigación, en concordancia con el Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos Resolución Nº 0294-2023-UANCV-CU-R, de conformidad a lo que establece la Ley Universitaria Nº 30220, Ley de Creación de la UANCV Nº 23738 y Modificatoria Nº 24661 y el Estatuto de la UANCV, que confiere facultades a la unidad de Investigación de la Facultad de Ciencias Jurídicas y Políticas.

SE RESUELVE:

ARTICULO PRIMERO.- APROBAR Y AUTORIZAR LA EJECUCIÓN DE LA PROPUESTA DE INVESTIGACIÓN, titulado: **INAPLICACIÓN ATÍPICA DE LA INTELIGENCIA ARTIFICIAL Y FRAUDE EN DELITOS CONTRA LA FE PÚBLICA - PUNO 2023,** presentado por el (la) **Bach. JOSE FERNANDO MAMANI CONDORI,** en virtud de los considerandos expuestos.

ARTICULO SEGUNDO.- RECONOCER, como ASESOR al **Dr. JAVIER ROMULO QUISPE ZAPANA.**

ARTICULO TERCERO.- DISPONER que la facultad, secretarias académicas y administrativas, quedan encargados del cumplimiento de la presente resolución.

Regístrese, comuníquese y archívese.

UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ"
DECANO
Dr. JAVIER ROMULO QUISPE ZAPANA
DECANO
FAC. Cs. JURÍDICAS Y POLÍTICAS

Dr. Fredy Chalco Vargas
DIRECTOR
UNIDAD DE INVESTIGACIÓN
FAC. CIENCIAS JURÍDICAS Y POLÍTICAS

DISTRIBUCIÓN:
DECANATURA FCJP, INTERESADO.
ARCH. FTChV/ncv.

ENAPLICACIÓN ATÍPICA DE LA INTELIGENCIA ARTIFICIAL Y FRAUDE EN DELITOS CONTRA LA FE PÚBLICA - PUNO 2023

INFORME DE ORIGINALIDAD

15%	13%	7%	10%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Universidad Andina Nestor Caceres Velasquez Trabajo del estudiante	4%
2	repositorio.uancv.edu.pe Fuente de Internet	1%
3	lpderecho.pe Fuente de Internet	1%
4	www.coursehero.com Fuente de Internet	<1%
5	apirepositorio.unu.edu.pe Fuente de Internet	<1%
6	Submitted to Corporación Universitaria Minuto de Dios, UNIMINUTO Trabajo del estudiante	<1%
7	repositorio.ucv.edu.pe Fuente de Internet	<1%
8	repositorio.unsch.edu.pe Fuente de Internet	<1%
9	cybertesis.unmsm.edu.pe Fuente de Internet	<1%
10	Submitted to Universidad Continental Trabajo del estudiante	<1%

Título de la tesis	
INAPLICACIÓN ATÍPICA DE LA INTELIGENCIA ARTIFICIAL Y FRAUDE EN DELITOS CONTRA LA FE PÚBLICA - PUNO 2023	
Datos del autor	
Nombres y apellidos	Jose Fernando Mamani Condori
Tipo de documento de identidad	DNI
Número de documento de identidad	72418433
URL de ORCID	https://orcid.org/0009-0004-6321-9031
Datos del asesor	
Nombres y apellidos	Javier Romulo Quispe Zapana
Tipo de documento de identidad	DNI
Número de documento de identidad	01324996
URL de ORCID	https://orcid.org/0000-0002-2532-8921
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Katty Agripina Perez Ordoñez
Tipo de documento	DNI
Número de documento de identidad	01225791
Miembro del jurado 1	
Nombres y apellidos	Walther Marcelino Nieto Portocarrero
Tipo de documento	DNI
Número de documento de identidad	23945399
Miembro del jurado 2	
Nombres y apellidos	Julio Cesar Chucuya Zaga
Tipo de documento	DNI
Número de documento de identidad	01328442

Datos de investigación	
Línea de investigación	Derecho Público – P05
Grupo de investigación	No aplica.
Agencia de financiamiento	Sin financiamiento.
Ubicación geográfica de la investigación	**Ubicación:** **País:** Perú **Departamento:** Puno **Provincia:** Puno **Distrito:** Puno **Coordenadas:** **Latitud:** -15.8424494 **Longitud:** -70.0475454  **URL:** https://www.google.com.pe/maps/place/Puno/@-15.8459534,-70.0577436,13z/data=
Año o rango de años en que se realizó la investigación	Octubre 2024 - Junio 2025
URL de disciplinas OCDE https://concytec-pe.github.io/Peru-CRIS/vocabularios/ocde_ford.html -Librería	**Derecho** https://purl.org/pe-repo/ocde/ford#5.05.00 **Derecho Penal** https://purl.org/pe-repo/ocde/ford#5.05.02

UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ"
UNIVERSIDAD ANDINA NÉSTOR CÁCERES VELÁSQUEZ - UNIDAD DE INVESTIGACIÓN - DIRECCIÓN - JULIACA
Mg. LUIS CHAYÑA AGUILAR
DIRECTOR (e)
UNIDAD DE INVESTIGACIÓN
FAC. CS. JURÍDICAS Y POLÍTICAS

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo JOSE FERNANDO MAMANI CONDORI, identificado con DNI Nro. 72418433 en mi condición de egresado de:

☒ **Escuela Profesional**

☐ **Programa de Segunda Especialidad,**

☐ **Programa de Maestría o Doctorado**

DERECHO,

informo que he elaborado el/la ☒ **Tesis** o ☐ **Trabajo de Investigación,** ☐ **Trabajo Académico** denominada:

INAPLICACIÓN ATÍPICA DE LA INTELIGENCIA ARTIFICIAL Y FRAUDE EN DELITOS CONTRA LA FE PÚBLICA – PUNO 2023

Asesorado por: Dr. JAVIER ROMULO QUISPE ZAPANA

Es un tema original.

Declaro que el presente trabajo de tesis es elaborado por mi persona y no existe plagio/copia de ninguna naturaleza, en especial de otro documento de investigación (tesis, revista, texto, congreso, o similar) presentado por persona natural o jurídica alguna ante instituciones académicas, profesionales, de investigación o similares, en el país o en el extranjero.

Dejo constancia que las citas de otros autores han sido debidamente identificadas en el trabajo de investigación, por lo que no asumiré como suyas las opiniones vertidas por terceros, ya sea de fuentes encontradas en medios escritos, digitales o Internet.

Asimismo, ratifico que soy plenamente consciente de todo el contenido de la tesis y asumo la responsabilidad de cualquier error u omisión en el documento, así como de las connotaciones éticas y legales involucradas.

El incumplimiento de lo declarado da lugar a responsabilidad del declarante, en consecuencia; a través del presente documento asumo frente a terceros, la Universidad Andina Néstor Cáceres Velásquez y/o la Administración Pública toda responsabilidad que pueda derivarse por el trabajo final presentado. Lo señalado incluye responsabilidad pecuniaria incluido el pago de multas u otros por los daños y perjuicios que se ocasionen.

Juliaca, 08 de enero del 2026

HUELLA

Dr. JAVIER ROMULO QUISPE ZAPANA
ASESOR DE TESIS
DNI: 01324996

JOSE FERNANDO MAMANI CONDORI
DNI: 72418433

DEDICATORIA

Dedico esta tesis, a mis padres por siempre confiar en mí, a mis abuelos que uno de ellos ya me mira desde arriba, a mi familia por siempre darme una sonrisa y ánimos, a mis maestros por el conocimiento, a mi hermano por consejos en la vida, a mi enamorada por su infinita paciencia y a mí por animarme cuando quería rendirme...

AGRADECIMIENTO

Mi sincero agradecimiento a mi familia, por su apoyo incondicional y su comprensión durante esta etapa crucial.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La presente investigación tiene como **Objetivo:** Evaluar el impacto de la inaplicación atípica de la inteligencia artificial (IA) y fraude en delito contra la fe pública - 2023, identificando las principales vulnerabilidades, las consecuencias socioeconómicas y proponiendo medidas para mitigar los riesgos. **La metodología:** La Investigación se basó en un estudio evaluativo de enfoque mixto. Se aplicó una encuesta a 40 profesionales, incluyendo abogados e ingenieros informáticos, y se realizó un análisis de documentos clave para complementar la recolección de datos**. Resultados**: Se revelaron una marcada falta de familiaridad y conocimiento sobre la IA y su uso fraudulento entre los expertos. A esto se suma una percepción crítica sobre el bajo nivel de seguridad cibernética en la región y la creencia generalizada de que las autoridades no están preparadas para enfrentar estos delitos. Además, se constató un consenso unánime sobre la desinformación de la población acerca de estos riesgos. Aunque la victimización directa reportada en la muestra fue mínima, se percibe una amenaza latente y creciente. **Conclusiones:** La "inaplicación atípica" de la IA en Puno se manifiesta como una profunda brecha de conocimiento, preparación y recursos, lo que genera una alta vulnerabilidad ante fraudes sofisticados y amenaza directamente la fe pública. Se recomienda de forma urgente implementar capacitación especializada, fortalecer el marco legal, invertir en tecnología y ejecutar campañas de concienciación ciudadana.

Palabras clave: Inteligencia artificial, fraude cibernético, confianza pública, ciberseguridad, no aplicación atípica.

ABSTRACT

This research aims to evaluate the impact of the atypical non-application of artificial intelligence (AI) on fraud against public trust in the Puno region, identifying the main vulnerabilities, the socioeconomic consequences, and proposing measures to mitigate the risks. Methodology: The research was based on a mixed-method evaluative study. A survey was administered to 40 professionals, including lawyers and computer engineers, and an analysis of key documents was conducted to complement the data collection. Results: A marked lack of familiarity and knowledge about AI and its fraudulent use was revealed among experts. This is compounded by a critical perception of the low level of cybersecurity in the region and a widespread belief that authorities are unprepared to confront these crimes. Furthermore, a unanimous consensus was found regarding the population's misinformation about these risks. Although direct victimization reported in the sample was minimal, a latent and growing threat is perceived. Conclusions: The "atypical underapplication" of AI in Puno manifests itself as a profound gap in knowledge, training, and resources, which creates a high vulnerability to malicious fraud and directly threatens public trust. It is urgently recommended to implement specialized training, strengthen the legal framework, invest in technology, and implement citizen awareness campaigns.

Keywords: Artificial intelligence, cyber fraud, public trust, cybersecurity, not an atypical application.

INTRODUCCIÓN

La presente investigación, titulada **"Inaplicación atípica de la Inteligencia Artificial y fraude en delitos contra la fe pública – Puno 2023"**, aborda un fenómeno de creciente complejidad y relevancia en el contexto de la acelerada digitalización global. Este estudio se sumerge en la particular situación de Puno, donde la sofisticación y la incidencia de los fraudes cibernéticos se ven exacerbadas por la peculiar "inaplicación atípica" de la inteligencia artificial (IA), un concepto que desglosaremos y analizaremos profundamente. Esto no es solo una cuestión tecnológica, sino una amenaza palpable para la seguridad, el bienestar ciudadano y la estabilidad socioeconómica de nuestra región.

Asimismo, al embarcarnos en esta investigación, hacemos énfasis en que la cibercriminalidad ha trascendido fronteras, transformando el panorama delictivo en un escenario complejo donde la IA se utiliza para perpetrar fraudes sofisticados a escala internacional. La velocidad con la que la IA evoluciona, supera la capacidad de las legislaciones nacionales e internacionales para adaptarse y establecer marcos regulatorios claros y efectivos. Esta brecha regulatoria expone de manera desproporcionada a países en desarrollo como Perú a mayores riesgos, dada la notoria desigualdad en la capacidad tecnológica para detectar y responder a estas amenazas. A nivel nacional, la escasez de profesionales capacitados en ciberseguridad se convierte en un cuello de botella, limitando la capacidad del país para detectar, prevenir y combatir los delitos cibernéticos que involucran IA. La falta de una coordinación efectiva entre instituciones clave (policía, fiscalía, sector privado) complejiza aún más la respuesta a incidentes. Además, la vulnerabilidad de muchos sistemas informáticos del Estado peruano facilita la comisión de fraudes y la manipulación de información.

El estudio que estamos realizando determina que, en Puno, esta situación se agrava por una marcada falta de conciencia ciudadana sobre los riesgos asociados al uso de tecnologías digitales y las ingeniosas formas en que la IA puede ser utilizada para cometer fraudes. Las limitaciones en el acceso a internet de alta velocidad y a dispositivos seguros en ciertas zonas de Puno dificultan no solo la detección sino también la denuncia de delitos cibernéticos. La dependencia de sistemas informáticos obsoletos en numerosas instituciones y empresas de la región incrementa su vulnerabilidad. Todo esto, en su conjunto, provoca un impacto negativo tangible en la economía local, afectando directamente a empresas, instituciones financieras y al patrimonio de los ciudadanos. La presente investigación busca identificar estas vulnerabilidades y sus consecuencias y proponer medidas concretas para mitigar estos riesgos en el contexto particular de Puno.

Teniendo en cuenta la siguiente composición, nuestra tesis se estructura para guiar al lector de manera lógica y coherente.

Capítulo I: Se desarrollará el contexto del problema, su planteamiento, los objetivos que nos guían, la justificación de por qué este estudio es tan necesario, las hipótesis que buscaremos contrastar y la operacionalización de nuestras variables.

Capítulo II: Marco Teórico, realiza un desarrollo exhaustivo de la literatura pertinente, sentando las bases conceptuales y teóricas que sustentan nuestra investigación, desde la evolución de la IA hasta el marco legal del cibercrimen en Perú.

Capítulo III: Se detalla el diseño, los métodos aplicados, la población y muestra, las técnicas e instrumentos de recolección de datos, y los procesos de validación y confiabilidad.

Capítulo IV: Se presenta la interpretación profunda de los hallazgos cuantitativos y cualitativos, conectándolos con nuestros objetivos y la literatura. Posteriormente, para complementar esta información, tenemos las referencias bibliográficas, en la que todas las fuentes consultadas, y los anexos, con la finalidad de, detallar información adicional relevante para el estudio.

CAPÍTULO I

ASPECTOS GENERALES

1.1 EXPOSICION DE LA SITUACIÓN

En el contexto actual, marcado por la acelerada digitalización y la proliferación de tecnologías disruptivas, la región de Puno se enfrenta a un desafío complejo: la creciente incidencia y sofisticación de los fraudes cibernéticos, exacerbados por la inaplicación atípica de la inteligencia artificial (IA). Este fenómeno representa una amenaza significativa para la seguridad y el bienestar de la población, así como para la estabilidad económica de la región.

La globalización de la cibercriminalidad ha transformado el panorama de la delincuencia, generando un escenario complejo donde la IA se utiliza para perpetrar fraudes sofisticados a escala internacional (Howard & Lipner, 2014). Esta rápida evolución de la IA supera la capacidad de las legislaciones nacionales e internacionales para adaptarse y establecer marcos regulatorios claros y efectivos (Turkle, 1997). La brecha regulatoria existente expone a los países en desarrollo, como Perú, a mayores riesgos de ser víctimas de delitos cibernéticos que utilizan IA debido a la desigualdad en la capacidad tecnológica (Levy, 1997).

El primer pilar del Derecho Público directamente afectado es la protección del bien jurídico de la fe pública. Esta no es solo la confianza en la veracidad de un documento, sino "la confianza que la sociedad, por mandato del Estado, deposita en

objetos, signos y formas que son cruciales para el tráfico jurídico y las interacciones sociales" (Salinas Siccha, 2017, p. 1120). Los fraudes tradicionales constituían ataques individualizados a este bien. En contraste, los fraudes potenciados por IA —como la generación de deepfakes para suplantar a funcionarios o la creación masiva de documentos fraudulentos algorítmicamente perfectos— constituyen un ataque sistémico y a escala. Como advierte Frank Pasquale, operamos en una "sociedad de la caja negra", donde los procesos algorítmicos opacos que gobiernan la información desafían la capacidad de supervisión y auditoría del Estado (Pasquale, 2015). La administración pública en Puno, al carecer de las herramientas técnicas y normativas para validar identidades y actos en este nuevo paradigma, ve erosionada su potestad de dar fe, lo que debilita la seguridad jurídica y la confianza en toda la estructura administrativa.

La Constitución impone al Estado un rol activo en la salvaguarda de derechos como la intimidad y la protección de datos personales (Art. 2, inc. 6, Constitución Política del Perú). No obstante, el modelo económico descrito por Shoshana Zuboff como "capitalismo de la vigilancia" se basa en la extracción masiva y sin control de datos personales, que se convierten en la materia prima para la ciberdelincuencia (Zuboff, 2019). El Estado peruano, y sus instituciones descentralizadas en Puno, fallan en su deber de protección por omisión: primero, al no regular eficazmente la recolección de datos por parte de actores privados y, segundo, al no contar con una

infraestructura de ciberseguridad robusta para proteger la información que él mismo administra. Esta doble omisión deja al ciudadano en un estado de indefensión, donde su información más sensible es monetizada y utilizada para fraudes, sin que la administración pública pueda ofrecer una tutela real y efectiva.

La falta de profesionales capacitados en ciberseguridad en Perú limita la capacidad del país para detectar, prevenir y combatir los delitos cibernéticos que involucran IA. La falta de una coordinación efectiva entre las diferentes instituciones encargadas de la seguridad cibernética (policía, fiscalía, sector privado) dificulta la respuesta a los incidentes. Muchos sistemas informáticos del Estado peruano son susceptibles a ataques cibernéticos, lo que puede facilitar la comisión de fraudes y la manipulación de información.

En Puno, la situación se agrava por la falta de conciencia ciudadana sobre los riesgos asociados al uso de tecnologías digitales y las formas en que la IA puede ser utilizada para cometer fraudes. La falta de acceso a internet de alta velocidad y dispositivos seguros en algunas zonas de Puno dificulta la detección y denuncia de delitos cibernéticos. Muchas instituciones y empresas en Puno aún dependen de sistemas informáticos obsoletos, lo que los vuelve más vulnerables a ataques cibernéticos. Los fraudes cibernéticos pueden tener un impacto negativo en la

economía local de Puno, afectando a empresas, instituciones financieras y ciudadanos.

1.2 FORMULACIÓN DEL PLANTEAMIENTO DEL PROBLEMA

1.2.1. Problema general

¿Cómo la inaplicación atípica de la inteligencia artificial (IA) en la región de Puno ha incrementado la incidencia y sofisticación de los fraudes contra la fe pública, generando un impacto negativo en la economía local y la confianza de la población?

1.2.2 Problemas específicos

- ¿Cuál es el nivel de vulnerabilidad de los sistemas informáticos gubernamentales, empresariales y personales en Puno frente a ataques cibernéticos que utilizan inteligencia artificial?
- ¿En qué medida las instituciones encargadas de la seguridad cibernética en Puno cuentan con los recursos y la capacitación necesaria para investigar y combatir los delitos cibernéticos que involucran IA?

1.3 OBJETIVOS

1.3.1 Objetivos generales

Evaluar el impacto de la inaplicación atípica de la inteligencia artificial en la comisión de fraudes contra la fe pública en la región de Puno, identificando las principales vulnerabilidades, las consecuencias socioeconómicas y proponiendo medidas para mitigar los riesgos.

1.3.2 Objetivos específicos

- Caracterizar los tipos de fraudes cibernéticos más comunes en Puno y analizar las técnicas de inteligencia artificial utilizadas por los ciberdelincuentes.
- Identificar las principales vulnerabilidades en los sistemas informáticos y las debilidades institucionales que facilitan la comisión de estos delitos en la región.
- Evaluar el impacto socioeconómico de los fraudes cibernéticos en la población de Puno, con énfasis en los sectores más vulnerables.

1.3 JUSTIFICACIÓN DEL ESTUDIO

La razón del estudio propone una solución en la necesidad de abordar un fenómeno emergente con profundas implicaciones para la sociedad. Se observa una escasez de investigaciones previas que estudien la relación específica entre la inteligencia artificial y los fraudes en contextos regionales como el de Puno. Este estudio busca llenar ese vacío, proporcionando información crucial sobre las dinámicas de la ciberdelincuencia en la era de la IA en la región. Además, la rápida evolución de la IA exige una constante actualización del conocimiento criminológico. Esta investigación permitirá comprender cómo los delincuentes utilizan la IA para cometer fraudes y cómo estas nuevas modalidades delictivas impactan en la sociedad puneña. El marco legal peruano, si bien ha avanzado, aún presenta vacíos en la regulación del uso delictivo de la IA, y este estudio aportará evidencia para su actualización y mejora, con especial atención a las necesidades de Puno.

A nivel práctico, la investigación permitirá identificar las vulnerabilidades de los sistemas informáticos (gubernamentales, empresariales y personales) y las debilidades institucionales que facilitan los fraudes con IA en Puno. Esta información será crucial para el diseño de estrategias de prevención y mitigación a nivel local. Los resultados de la investigación servirán como base para la formulación de políticas públicas más efectivas en la lucha contra los ciberdelitos en Puno. Además, el estudio contribuirá a sensibilizar a la población sobre los riesgos de los fraudes cibernéticos y la importancia de la ciberseguridad, promoviendo la adopción de medidas de protección. Finalmente, ayudará a fortalecer las capacidades de las instituciones encargadas de la seguridad cibernética en Puno (policía, fiscalía, etc.), proporcionándoles información clave para la investigación y persecución de estos delitos.

La solidez metodológica de este estudio se basa en la triangulación de enfoques: revisión bibliográfica para construir un marco teórico sólido, análisis de datos estadísticos para una visión cuantitativa del problema, estudio de casos para profundizar en la comprensión del fenómeno en la región, y análisis del marco legal vigente para identificar lagunas y necesidades de actualización.

1.4 HIPÓTESIS

1.4.1 Hipótesis general

La inaplicación atípica de la inteligencia artificial en la región de Puno ha incrementado significativamente la incidencia y sofisticación de los fraudes contra la fe pública, generando un impacto negativo en la economía local y la confianza de la población.

1.4.2. Hipótesis específicas

- Existe una correlación directa entre la vulnerabilidad de los sistemas informáticos en Puno y la frecuencia de ataques cibernéticos que utilizan inteligencia artificial.

- La falta de capacitación especializada en ciberseguridad en las instituciones encargadas de la persecución de delitos en Puno limita su capacidad para investigar y procesar eficazmente los casos de fraude cibernético.

- El bajo nivel de conciencia de la población de Puno sobre los riesgos de los fraudes cibernéticos y las medidas de seguridad informática los convierte en blancos más fáciles para los ciberdelincuentes.

1.5. VARIABLES

15.1 Variable Independiente (VI)

Nivel de preparación frente al uso delictivo de la IA

1.5.2. Variable Dependiente (VD)

Impacto de los fraudes con IA en Puno

1.5.3 Operacionalización de variables

Variables	Dimensiones	Indicadores
Variable Independiente (VI) Nivel de preparación frente al uso delictivo de la IA	Marco legal e institucional Conocimiento y conciencia ciudadana Infraestructura tecnológica	Existencia y aplicación de leyes, capacitación de las autoridades, coordinación interinstitucional. Nivel de comprensión sobre los riesgos de la IA en los fraudes, adopción de medidas de ciberseguridad. Acceso a internet seguro, uso de sistemas informáticos actualizados y protegidos.

Variable Dependiente (VD) Impacto de los fraudes con IA en Puno	Número de víctimas Pérdidas económicas Impacto en la confianza Efectos psicológicos en las víctimas	Cantidad de personas o instituciones afectadas. Monto de dinero perdido por fraudes con IA. Percepción de la seguridad en las transacciones digitales, confianza en las instituciones. Nivel de estrés, ansiedad o trauma experimentado por las víctimas.

CAPÍTULO II.

MARCO TEÓRICO

2.1 Antecedentes de la Investigación

2.1.1 A nivel internacional

Howard y Lipner (2014), en su libro "Seguridad de la información para directivos y profesionales de la informática", ofrecen una guía completa sobre cómo construir y mantener sistemas seguros. Los autores, reconocidos expertos en seguridad informática, enfatizan la importancia de integrar la seguridad en todas las fases del desarrollo de software, desde el diseño hasta el despliegue y mantenimiento. Además, proporcionan un marco para la gestión de riesgos de seguridad, que incluye la identificación de activos, la evaluación de amenazas y vulnerabilidades, y la selección de controles de seguridad apropiados. El libro ofrece consejos prácticos y ejemplos reales para ayudar a los profesionales de la seguridad a implementar medidas de seguridad efectivas.

Sherry Turkle (1997), en su obra "La vida en la pantalla", analiza cómo la tecnología, especialmente las computadoras e internet, está transformando la vida social, la identidad y las relaciones humanas. La autora explora las implicaciones psicológicas y sociales de la interacción con la tecnología, argumentando que la vida en línea puede afectar la forma en que nos relacionamos con nosotros mismos y con los demás.

Pierre Levy (1997), en su libro "¿Qué es la virtualidad?", explora el concepto de virtualidad y su impacto en la cultura, la sociedad y el conocimiento. El autor define la virtualidad como "lo que existe en potencia, lo que tiende a actualizarse", y analiza cómo la

tecnología está creando nuevos espacios de interacción y comunicación, como el ciberespacio.

Nick Bostrom (2014), en su libro "Superinteligencia: Caminos, peligros, estrategias", advierte sobre los riesgos existenciales que plantea la inteligencia artificial. El autor argumenta que, si la IA supera la inteligencia humana, podría representar una amenaza para la humanidad, y propone estrategias para controlar su desarrollo y evitar posibles consecuencias negativas.

Luciano Floridi (2014), en su libro "La cuarta revolución: hacia una filosofía de la información", propone una nueva filosofía para la era digital. El autor argumenta que la información es un elemento fundamental de la realidad, y que la tecnología está transformando la forma en que interactuamos con el mundo. Floridi explora las implicaciones éticas y sociales de la tecnología, y propone un marco para comprender la información y su papel en la sociedad.

Edwin H. Sutherland (1992), en su obra "Criminología", sentó las bases del estudio de la delincuencia de cuello blanco, es decir, los delitos cometidos por personas de alto estatus social en el curso de sus ocupaciones. Sutherland desafió la idea de que la delincuencia estaba asociada exclusivamente a la pobreza y la marginalidad, y demostró que las personas de clase alta también cometían delitos, aunque de una forma diferente.

Howard S. Becker (1988), en su libro "Outsiders: Estudios de sociología de la desviación", analizó la desviación social desde una perspectiva interaccionista. Becker argumentó que la desviación no es una cualidad inherente a un acto, sino una consecuencia de la aplicación de normas y sanciones por parte de otros. El autor estudió cómo los grupos

sociales crean y aplican las normas, y cómo las personas etiquetadas como "desviadas" son afectadas por esta etiqueta.

2.1.2 A nivel nacional

A nivel nacional, la preocupación por la IA en el ámbito penal es evidente. La Ley N.° 32314 (2025) en Perú incorpora por primera vez sanciones específicas para delitos cometidos mediante IA, incluyendo deepfakes y estafas, reflejando la necesidad de adaptar el marco legal a las nuevas realidades tecnológicas (EGEPUD, 2025). Esta legislación busca abordar el uso no consentido o fraudulento de la voz, imagen, audio o movimiento corporal de terceros con IA para fines ilícitos, impactando directamente en la afectación de la confianza en documentos, identidades y representaciones de la realidad que constituyen la fe pública.

A nivel de ciberseguridad, las propuestas de Rodríguez y Cruzado (2020) sobre la implementación de la norma ISO 27001 en empresas peruanas, y el análisis de León, Tesillo, Escobar y Godoy (2022) sobre los avances generales en ciberseguridad en el Perú en el marco de la transformación digital, evidencian un esfuerzo por fortalecer las defensas de la información en el país. Asimismo, Chavarría y Rubio (2021) han propuesto arquitecturas de seguridad de la información específicamente diseñadas para la protección de activos digitales en PYMES peruanas, reconociendo la vulnerabilidad de este sector a nivel nacional. Estos trabajos subrayan la importancia de adaptar constantemente las estrategias de defensa para proteger la información en un entorno cada vez más digitalizado y con amenazas emergentes.

La Ley N.° 32314 (2025) en Perú, por ejemplo, incorpora por primera vez sanciones específicas para delitos cometidos mediante IA, incluyendo la generación de deepfakes y estafas (EGEPUD, 2025). Esta legislación es una respuesta directa a la necesidad de

abordar el uso no consentido o fraudulento de la voz, imagen, audio o movimiento corporal de terceros con IA para fines ilícitos. La existencia de esta ley demuestra la conciencia nacional sobre el potencial de la IA para afectar la confianza en documentos, identidades y representaciones de la realidad, elementos que constituyen la fe pública. Reportes de la prensa nacional también alertan sobre el incremento de estafas con deepfakes en el país (El Peruano, 2024; Infobae, 2025), lo que valida la relevancia de la IA como un vector de fraude en el contexto peruano.

Un aspecto relevante a nivel nacional, aunque no directamente sobre la IA en fraudes, es el estudio de Anaya, Montalvo, Calderón y Arispe (2021). Si bien su foco está en las brechas digitales en escuelas rurales peruanas, sus hallazgos indirectamente evidencian disparidades significativas en el acceso y manejo de tecnología en el ámbito educativo, un indicador del nivel de digitalización general en ciertas zonas del país. El CEPLAN (2025) también ha documentado el incremento del ciberdelito a nivel nacional, señalando una tendencia al alza en la sofisticación de las amenazas cibernéticas en el Perú.

En el ámbito del derecho penal y la tecnología, la obra de **Villavicencio Terreros (2018)** sobre el principio de lesividad en los delitos informáticos ofrece una base para comprender cómo el ordenamiento jurídico peruano aborda la afectación a bienes jurídicos protegidos en el entorno digital, lo cual es fundamental para analizar los fraudes contra la fe pública mediantey no menciona la IA. De igual forma, **Salinas Siccha (2017)**, en su tratado sobre el derecho penal peruano, discute la tipificación de los delitos contra la fe pública desde una perspectiva tradicional, lo que puede servir para contrastar la "inaplicación atípica" de la IA en estos ilícitos.

2.1.2 A nivel local

Al enfocar el análisis en la región de Puno, la dinámica observada en los delitos contra la fe pública ha estado tradicionalmente vinculada a modalidades más convencionales. Intervenciones policiales y reportes fiscales en Puno señalan casos de falsificación de documentos, sellos y falsedad ideológica (Ministerio Público Fiscalía de la Nación, 2024; Gob.pe, 2020). Un estudio relevante sobre el incremento de delitos informáticos en la ciudad de Puno en 2023 indicó que el fraude informático es el principal delito contra el patrimonio, con modalidades como el phishing y la clonación de tarjetas (Redalyc, 2024). Es crucial observar que este análisis, aunque exhaustivo, no detalla explícitamente la aplicación de Inteligencia Artificial avanzada en la comisión de dichos delitos contra la fe pública en la región. Esta ausencia de mención directa podría ser un indicativo clave de la "inaplicación atípica" que es objeto de la presente investigación.

La brecha digital y el nivel de adopción tecnológica en la región de Puno son factores determinantes que podrían influir en esta "inaplicación atípica". La investigación de Hurtado (2022) sobre el impacto de la pandemia y la educación virtual en Puno refuerza la idea de desafíos significativos en competencias digitales y acceso a infraestructura tecnológica. Estos desafíos pueden limitar la capacidad de los potenciales ciberdelincuentes locales para implementar fraudes con IA sofisticada, así como la capacidad de las autoridades e instituciones para detectarlos, investigarlos y rastrear su origen. De forma complementaria, Condori y Mamani (2021) han estudiado la percepción del uso de las tecnologías de información y comunicación en el sector público de Puno, revelando limitaciones en la infraestructura y capacitación, lo que podría explicar una menor sofisticación en los delitos informáticos detectados localmente.

La escasez de reportes o sentencias judiciales que detallen explícitamente el uso de

IA en fraudes contra la fe pública en Puno hasta la fecha de 2024, a pesar del aumento general de delitos informáticos (Redalyc, 2024), sugiere que la IA, si bien es una amenaza latente y creciente a nivel nacional, aún no es un elemento central o reconocido de manera significativa en la comisión de estos delitos específicos en la región. Es plausible que, debido a las condiciones locales, métodos de fraude tradicionales o menos complejos sigan siendo efectivos debido a la falta de concienciación, infraestructura robusta o capacitación especializada en ciberseguridad por parte de las víctimas o de los organismos de control. Esta situación, al ser "atípica" en un mundo digitalmente avanzado, justifica la relevancia de investigar las causas y consecuencias de esta particular "inaplicación" en Puno.

2.2 Propuesta de la IA y evolución

La Inteligencia Artificial (IA) se define primariamente como la ciencia y la ingeniería dedicada a la creación de máquinas o programas de computadora que poseen la capacidad de razonar, aprender y actuar de manera que, si fueran realizados por humanos, requerirían inteligencia. Esta conceptualización inicial, que se remonta al trabajo de John McCarthy (2007), uno de los fundadores del campo, enfatiza la IA como una disciplina de la informática enfocada en replicar procesos cognitivos. En términos más prácticos y funcionales, la IA es la habilidad de un sistema para interpretar datos externos, aprender de dichos datos y utilizar ese conocimiento para lograr objetivos y tareas específicas a través de la adaptación flexible.

El enfoque moderno predominante, popularizado por Russell y Norvig (2020) en su obra fundamental *Inteligencia Artificial: Un Enfoque Moderno*, tiende a definir la IA como el estudio de los agentes racionales. Un agente racional es

un sistema que actúa para lograr el mejor resultado esperado o, si hay incertidumbre, el mejor resultado promedio esperado. Esta perspectiva es la más utilizada en la ingeniería de IA contemporánea, ya que se centra en construir sistemas que "actúen racionalmente" para maximizar el rendimiento. Por ejemplo, los sistemas actuales de IA Débil (o estrecha), como los asistentes virtuales o los motores de recomendación, están diseñados para ejecutar una tarea específica de la manera más racional y eficiente posible.

Además de los enfoques técnicos y racionales, existe una definición más orientada al comportamiento que se enfoca en si la máquina puede imitar el pensamiento o el comportamiento humano. Esto se relaciona con la famosa prueba propuesta por Alan Turing (1950, como se citó en Russell & Norvig, 2020). Desde esta óptica, la IA busca crear sistemas que, al interactuar, sean indistinguibles de una persona, como bien lo resumió Marvin Minsky (1968, como se citó en López de Mántaras & Brunet, 2023): "La IA es la ciencia de hacer que las máquinas hagan cosas que requerirían inteligencia si fueran hechas por humanos".

IA o inteligencia artificial, fue presentada como la capacidad en las máquinas de “emular la inteligencia humana” y ser capaz de procesar grandes cantidades de datos, así como la realización de tareas que de todas formas requieren intervención humana como el aprendizaje o la toma de decisiones (Turkle, 1997).

La inteligencia artificial en ciberseguridad ha abierto la posibilidad de que los agentes de ciberseguridad puedan detectar y prevenir ataques cibernéticos,

pero también ha permitido a los criminales utilizar estas tecnologías para cometer fraudes a gran escala como en (Bostrom, 2014)

El crecimiento de la inteligencia artificial ha generado perjuicios y oportunidades por partes iguales. Si bien sus aplicaciones en seguridad cibernética pueden mejorar la protección de su plataforma de datos, la criminalidad utilizando IA ha originado fraudes más sofisticados que son difíciles de descubrir para instituciones de protección digital (Floridi, 2014). El uso no autorizado de IA, representa, un riesgo para la privacidad y la estabilidad económica de las regiones vulnerables, como es el caso de Puno.

Ciberseguridad significa un conjunto de herramientas y enfoques para la protección de los sistemas informáticos y los datos contra el acceso no autorizado - ataques hostiles, daños. Howard y Lipner (2014) sostienen que los avances tecnológicos, especialmente en IA, han aumentado drásticamente las ciberestafas en la era contemporánea. La Inteligencia Artificial permite a los hackers realizar lo que ellos llaman «algoritmos inteligentes» que les permitirán eludir las medidas de seguridad tradicionales y cometer fraudes sin la participación humana indirecta en todo el proceso, tal como lo describe Turkle (1997).

El fraude cibernético se define como el acto ilegal o conducta engañosa que se lleva a cabo a través de medios tecnológicos, como sistemas informáticos, redes e Internet, con el objetivo de obtener un beneficio económico ilícito a expensas de una víctima (Mayer & Oliver, 2020). Esencialmente, constituye la

manifestación digital de los delitos de estafa y engaño, aprovechando las vulnerabilidades de la infraestructura tecnológica y la confianza del usuario (Salgado, 2009). La característica distintiva de este tipo de fraude es que el proceso delictivo, desde la manipulación hasta la consumación del perjuicio patrimonial, tiene lugar dentro del entorno informático.

La delimitación conceptual del fraude cibernético se centra en las acciones que implican una manipulación de datos o una alteración del funcionamiento de un sistema para causar un menoscabo económico (Velásquez, 2024). Esta manipulación puede ser directa (por ejemplo, alterando registros bancarios) o, más comúnmente, indirecta, mediante la suplantación de identidad (*phishing*) o la ingeniería social, donde el perpetrador engaña a la víctima para que esta misma entregue sus datos o realice una transferencia de fondos. Según Mayer y Oliver (2020), el foco está en la disposición patrimonial que se consigue debido al error provocado por el engaño digital.

En Puno, como la infraestructura tecnológica tiene un puntaje avanzado y el nivel de conocimiento son muy bajos entre las organizaciones tanto públicas como privadas de la ciudad. Además, tienen poca capacidad de respuesta ante este tipo de delitos debido a que las instituciones peruanas carecen de competencias en ciberseguridad (Levy, 1997).

2.2.1. Marco Legal y Regulación del Cibercrimen en Perú

La regulación del cibercrimen en el Perú es insuficiente a nivel nacional ya que no hace frente a los nuevos riesgos que ha traído consigo la inteligencia artificial que se ha introducido. En la actualidad, la Ley de Delitos Informáticos, también conocida como Ley Nº 30096, es la encargada de regular delitos como el acceso no autorizado, el acceso indebido a sistemas informáticos, o las alteraciones que se hayan realizado a los datos. Sin embargo, esta ley no contempla específicamente los delitos que se cometen con ayuda de inteligencia artificial, por lo que existe un vacío legal.

El Texto Completo del Código Penal Peruano, enuncia en el artículo 196 en los delitos contra la administración de justicia crea consecuencias para quien cometa los fraudes con escarmiento; sin embargo, no incluye la tecnología sofisticada ni la Inteligencia Artificial:

Artículo 196. Fraude

"El que, con ánimo de lucro, engañare a otro, obteniendo para sí o para otro un beneficio económico ilícito, incurrirá en pena privativa de libertad no menor de dos ni mayor de seis años."

(Código Penal Peruano, 1991)

A pesar de su utilidad en casos de fraude tradicional, el artículo carece de especificidad en cuanto a los fraudes cibernéticos y el uso de IA, lo que impide una regulación efectiva de estos delitos en el contexto digital actual.

2.2.2. Consecuencias financieras y sociales del fraude cibernético en Puno

Los fraudes cibernéticos no sólo pueden afectar a la seguridad de la información personal, sino que también tienen repercusiones a nivel socioeconómico y repercuten en otros ámbitos. Sutherland (1992) ha sugerido que los fraudes cibernéticos son un tipo de corrupción de cuello blanco. Esto se debe al hecho de que los delincuentes, muchos de los cuales tienen un alto grado de conocimientos tecnológicos, aprovechan su capacidad para investigar agujeros en el sistema de manera que no puedan ser detectados rápidamente al instante.

Las pequeñas empresas y los habitantes de Puno que no pueden gastar dinero en inversiones beneficiosas en seguridad han sido víctimas de estafas cibernéticas, que normalmente han causado trastornos. Debido a esta deficiencia, se han producido pérdidas económicas sustanciales, y la fe de la gente en los sistemas digitales se ha erosionado por completo. Según Floridi (2014), la falta de seguridad en el software digital se corresponde con una reducción de la conexión económica, lo que a su vez dificulta el crecimiento de la comunidad local.

2.2.3. Discordancias en la Normativa y Sugerencias para la Reforma del Derecho Institucional

El Estado peruano se encuentra actualmente en una condición de significativa pre-cautela respecto a la adecuada conducción de la inteligencia artificial en el contexto del uso de la tecnología en el campo de la

ciberdelincuencia. Como resultado de ello, la inteligencia artificial es «más fastidiosamente acrecentadora que cualquier otro recurso humano», como lo afirma Bostrom. Uno de los retos más importantes es la incapacidad de la regulación para seguir el ritmo de la progresión de A con motor de IA. Floridi sugiere que «las leyes deben ser modernas y, por tanto, sencillas», y que estas leyes deben modificarse para incorporar medidas que tengan en cuenta el uso de la inteligencia artificial en la ciberdelincuencia.

Además, debería reforzarse la colaboración internacional en la lucha contra la ciberdelincuencia facilitada por la inteligencia artificial. El Convenio de Budapest sobre la Ciberdelincuencia, al que Perú se ha adherido, estipula que la colaboración en la persecución de la ciberdelincuencia está prohibida; sin embargo, la ejecución de este convenio está supeditada a una nación que haya promulgado leyes sólidas y recientes (Howard & Lipner, 2014).

2.2.4. Ley N° 30096: Ley de Delitos Informáticos

La Ley N° 30096, Ley de Delitos Informáticos, promulgada en 2013, es la principal legislación en Perú que aborda los delitos informáticos. Esta ley busca establecer medidas para la protección de los sistemas informáticos, la información y los datos personales. Dentro de sus disposiciones, la ley penaliza el acceso no autorizado a sistemas informáticos, la alteración de datos, la interceptación de comunicaciones electrónicas y el uso indebido de información almacenada electrónicamente. Aunque esta ley cubre una amplia gama de delitos cibernéticos, no aborda de manera específica el **uso de inteligencia artificial (IA)** para cometer fraudes. Los ciberdelincuentes que emplean IA para llevar a cabo ataques automatizados o diseñar algoritmos que eluden la detección no están suficientemente contemplados en la ley, lo que

constituye un vacío significativo. **L**os artículos del Código Penal Peruano tipifican delitos como el fraude, la falsificación de documentos y la estafa (artículos 196, 425 y 426), que, en teoría, podrían ser relevantes en situaciones de ciberfraude. Sin embargo, los artículos mencionados no abordan explícitamente el uso de tecnologías sofisticadas, como la inteligencia artificial, en la comisión de estos delitos.

Por ejemplo, el Artículo 196 establece que:

"El que, con ánimo de lucro, engañare a otro, obteniendo para sí o para otro un beneficio económico ilícito, incurrirá en pena privativa de libertad no menor de dos ni mayor de seis años."

Si bien no se aborda específicamente, este artículo aborda el fraude convencional; no se contempla el fraude cometido mediante tecnología avanzada, como el que utiliza inteligencia artificial para manipular datos o llevar a cabo el robo de identidad digital. Dado que el ciberfraude puede incluir ataques automatizados a gran escala, este artículo no aborda las complejidades de los fraudes que utilizan inteligencia artificial, lo que pone de manifiesto un vacío legal.

2.2.5. Ley N° 29733: Ley de Protección de Datos Personales

Mediante la implementación de la Ley N.° 29733, también conocida como Ley de Protección de Datos Personales, promulgada en 2011, se regula el tratamiento de datos personales en el Perú, preservando así la privacidad y seguridad de la información personal de los ciudadanos. Además de definir los derechos de las

personas que son objeto de datos, esta legislación exige a las instituciones públicas y privadas implementar medidas de seguridad para proteger los datos personales.

Principales disposiciones de la Ley N° 29733:

Artículo 5: Reconoce el derecho de los ciudadanos a la protección de sus datos personales y establece las obligaciones de los responsables del tratamiento de dichos datos.

Artículo 8: Regula el consentimiento para el tratamiento de datos personales, incluyendo la recolección, almacenamiento y transmisión de los mismos.

Si bien la Ley N.° 29733 representa un avance considerable en materia de protección de datos, no aborda explícitamente el uso de inteligencia artificial para procesar o alterar estos datos de forma perjudicial. En el contexto del ciberfraude, los ciberdelincuentes podrían utilizar inteligencia artificial para evaluar grandes volúmenes de datos personales y modificarlos con el fin de obtener beneficios ilícitos. Debido a que la ley no tiene pautas claras para el uso de inteligencia artificial de esta manera, las personas tienen más probabilidades de ser vulnerables a ataques informáticos que ponen en riesgo su privacidad.

La Secretaría de Gobierno y Transformación Digital (SGTD)

Esta Secretaría pertenece a la Presidencia del Consejo de Ministros (PCM) y es el órgano rector del Sistema Nacional de Transformación Digital.

Su rol principal en la regulación de la IA se establece en la Ley N° 31814, Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país, y su posterior Reglamento (aprobado mediante Decreto Supremo N.° 115-2025-PCM).

Funciones Clave de la SGTD en materia de IA

Autoridad Técnica Normativa: La SGTD tiene la función de establecer los lineamientos, estándares y mecanismos para el uso seguro, responsable y ético de la IA en el país.

Gobernanza: Es la responsable de la gobernanza de la IA, lo que incluye la coordinación de acciones con ministerios, entes reguladores, la academia y el sector privado.

Estrategia Nacional: Está a cargo de la elaboración de la Estrategia Nacional de Inteligencia Artificial (ENIA) y la promoción de la innovación y la investigación.

Clasificación de Riesgos: El Reglamento de la Ley 31814 establece una clasificación de riesgos (Alto, Limitado y Aceptable) para los sistemas basados en IA. La SGTD supervisa el cumplimiento de las obligaciones relacionadas con estos

niveles de riesgo.

Ley N° 31814: Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país. Promulgación: Julio de 2023. Reglamento: Aprobado mediante el Decreto Supremo N.° 115-2025-PCM.

A continuación, se resumen los aspectos clave de esta legislación:

1. Entidad Rectora

La autoridad técnica normativa y el ente encargado de la gobernanza de la IA en Perú es la Secretaría de Gobierno y Transformación Digital (SGTD), que forma parte de la Presidencia del Consejo de Ministros (PCM).

2. Enfoque Regulatorio: Basado en Riesgos

La ley y su reglamento establecen una clasificación de los sistemas de IA basada en el riesgo que su uso pueda generar para los derechos fundamentales y la seguridad ciudadana:

Clasificación de Riesgo,Descripción,Implicaciones

Uso Prohibido,"Sistemas que manipulen de forma engañosa o que exploten vulnerabilidades de personas para influir en sus decisiones, o aquellos que realicen vigilancia masiva sin sustento legal.","Uso ilegal, sujeto a sanciones."

Riesgo Limitado/Alto,"Sistemas utilizados en ámbitos sensibles como salud, educación, empleo, justicia o programas sociales.",Requieren una evaluación de impacto obligatoria para garantizar la transparencia y la no discriminación.

Riesgo Aceptable,Todos los usos de IA no comprendidos en las categorías

anteriores (riesgo mínimo o nulo).,Deben cumplir con los principios éticos y las buenas prácticas establecidas en el reglamento.

3. Principios Fundamentales

La Ley N° 31814 promueve el desarrollo y uso de la IA bajo los siguientes principios éticos:

Estándares de Seguridad: Se promueve un enfoque de seguridad basado en el riesgo del sistema de IA.

Desarrollo Ético y Responsable: Se busca identificar claramente el marco de responsabilidades y las medidas para un uso ético.

Transparencia y Explicabilidad: Los sistemas de IA deben ser diseñados para que sus decisiones y procesos puedan ser comprendidos (explicados) por los usuarios.

Privacidad de la IA: La tecnología no debe transgredir la privacidad y debe cumplir con la normativa de protección de datos personales.

4. Promoción de la Innovación

La ley también tiene un fuerte componente de fomento, al establecer mecanismos como:

Estrategia Nacional de IA (ENIA): Desarrollo de una estrategia para impulsar la investigación y la adopción de la IA en el país.

Sandboxes Regulatorios: Creación de entornos de prueba controlados que permiten a las empresas probar nuevas aplicaciones de IA sin un marco regulatorio estricto inicial, siempre y cuando se mitiguen los riesgos.

Fomento a Mipymes y Emprendimientos: Apoyo a las pequeñas empresas para la adopción y el desarrollo de soluciones de IA.

2.3. MARCO CONCEPTUAL

Inteligencia Artificial (IA): En pocas palabras, la inteligencia artificial (IA) se refiere al campo de la informática que se centra en el desarrollo de sistemas que funcionan de forma similar a los sistemas humanos para llevar a cabo actividades que requieren inteligencia. El aprendizaje, el razonamiento, la resolución de problemas, la identificación de patrones, la percepción y la toma de decisiones son las cinco habilidades que se incluyen en esta categoría (Turing 1997). La inteligencia artificial permite a los ordenadores imitar los procesos cognitivos humanos empleando complejos algoritmos y estructuras de datos. Esto hace posible que las personas conecten con la tecnología de una forma que les resulta más natural.

Inteligencia artificial impacto en la ciberseguridad y el fraude cibernético: En el campo de la ciberseguridad, la Inteligencia Artificial ha revolucionado cómo se asegura la defensa computadora. Por un lado, la IA puede hacerle seguimiento al dar algo de ayuda a la contra del ataque de ciberseguridad al detectar patrones inusuales de actividad, y también hacernos probable suponer análisis de amenazas cibernéticas. Por ejemplo, los sistemas de IA podrían detectar una tarea de phishing antes de marcar daño antes de que establecerán las interacciones digitales anormalidades a través de anomalías (Floridi, 2014).

Desafíos y retos éticos de la inteligencia artificial: Los desafíos éticos que se presentan en la aplicación de IA en cárcel cibernética son los siguientes. El primer problema es el sesgo algorítmico, ya que los sistemas de IA, si no son ideados correctamente, pueden aprender de datos defectuosos y, con el tiempo, perpetuar el sesgo o intensificarlo. De hecho, si un sistema de IA ha sido entrenado sobre datos desigualitarios, por ejemplo, de discriminación racial o de género, los algoritmos

actuarán de hecho sobre la base de esos sesgos hombre por medio; un ejemplo de esto es el sistema de contratación o el sistema de crédito.

Ciberseguridad: La ciberseguridad es el entramado de práctica, proceso y tecnología que se implementa para mantener segura su comuna mediante el diseño y establecimiento para la protección contra accesos no autorizados, daños o ataques de terceros desautorizados. Con el envejecimiento de un mundo cada vez más digitalizado, la ciberseguridad ha pasado a ser una preeminencia global debido a que la adicción a las tecnologías de la información hace que su vulnerabilidad aumente a fuego las anteriormente mencionadas acciones (Turkle 1997).

Marco Legal en Perú y Vacíos Regulatorios: El marco legal de Perú en cuanto a delitos informáticos ha avanzado en los últimos años, pero sigue enfrentando una serie de desafíos relacionados con la tecnología emergente, como la inteligencia artificial (IA). El uso de la IA en fraudes cibernéticos ha superado las capacidades de las leyes existentes, lo que ha generado vacíos regulatorios importantes. A continuación, se abordan las principales normativas peruanas relacionadas con los delitos informáticos y los fraudes cibernéticos, así como los vacíos regulatorios y las áreas que requieren reformas.

CAPÍTULO III

PROCEDIMIENTO METODOLÓGICO DE LA INVESTIGACIÓN

3.1. DISEÑO DE LA INVESTIGACIÓN

Nuestro estudio sobre la particular situación de la inaplicación de la inteligencia artificial (IA) en los fraudes contra la fe pública en Puno se apoya en un **diseño evaluativo**. La idea es sencilla: queremos formarnos un juicio de valor sobre cómo están las cosas actualmente, contrastándolo con un escenario ideal donde Puno cuente con las herramientas adecuadas para enfrentar el uso delictivo de la IA. Esto nos lleva a evaluar si las medidas existentes —o la falta de ellas— son efectivas para prevenir y combatir estos fraudes, considerando el marco legal vigente, la capacitación del personal, la conciencia ciudadana sobre los riesgos y la infraestructura tecnológica disponible.

Representación del diseño:

M ---------- O

Donde:

(M) es la muestra de trabajo: Abogados e ingenieros informáticos de Puno (y posiblemente de otros países) que brindarán información sobre la situación actual.

(O) El conjunto de datos seleccionados: Información sobre la incidencia de fraudes con IA, la vulnerabilidad de los sistemas, el nivel de capacitación en ciberseguridad, la conciencia ciudadana sobre los riesgos de la IA, et

3.2. MÉTODO DE INVESTIGACIÓN

Nuestra investigación tiene una doble cara: es **exploratoria**, porque buscamos entender a fondo los distintos factores que hacen a nuestra región vulnerable a los fraudes con IA; y es **descriptiva**, ya que nos enfocaremos en pintar un cuadro claro de la situación actual sin alterar ninguna variable (Hernández Sampieri et al., 2014).

Para lograr una comprensión profunda del problema, vamos a combinar dos caminos: el **método inductivo** y el **deductivo**. Con el enfoque inductivo, partiremos de la información específica que recolectemos (como entrevistas, encuestas y datos de casos de fraude y registros policiales) para identificar patrones y tendencias, y así llegar a conclusiones generales sobre cómo la inaplicación de la IA se relaciona con la ocurrencia de fraudes (Defensoría del Pueblo, 2023). Por otro lado, el método deductivo nos permitirá partir de una hipótesis: que la inaplicación de la IA aumenta la vulnerabilidad a los fraudes. Buscaremos comprobar esta idea analizando la legislación, el nivel de preparación de las autoridades, la inversión en ciberseguridad y la conciencia pública (Martínez & Rodríguez, 2022). Esta combinación nos dará una visión más completa y robusta del problema, ayudándonos a generar conocimiento y proponer soluciones prácticas para Puno.

3.3 POBLACIÓN Y MUESTRA

3.3.1 Población

La población de interés para este estudio está conformada por profesionales con experticia en el ámbito legal y tecnológico en la región de Puno, cuyas

perspectivas son cruciales para el análisis de la Inteligencia Artificial en los fraudes contra la fe pública. Se consideraron dos grupos principales: abogados y ingenieros informáticos. Los ingenieros informáticos incluían a profesionales y practicantes que se desempeñan en distintos trabajos dentro de instituciones como el Ministerio Público, la Policía Nacional del Perú y el Poder Judicial en la región. Para obtener una comprensión representativa de este fenómeno, se contó con la participación de 40 profesionales de esta población para la recolección de datos, quienes fueron seleccionados para conformar la muestra del estudio.

3.3.2. Muestra

Para el presente examen, se optó por una prueba deliberada o intencional, en la que el investigador escogió directamente el número pertinente de encuestados. En este caso, la muestra estuvo conformada por 40 personas, seleccionadas según el motivo del examen y su pertinencia para el estudio. Este grupo se basó en residentes de Puno que son ingenieros informáticos o abogados, dada su relevancia directa con el tema de la inaplicación atípica de la Inteligencia Artificial en los fraudes contra la fe pública. La selección se realizó considerando su conocimiento y experiencia en los ámbitos del derecho y la tecnología.

3.4. TÉCNICAS FUENTES E INSTRUMENTOS DE INVESTIGACIÓN

3.4.1. TECNICAS

Para la presente investigación, los procedimientos de análisis se centraron en la extracción de características y peculiaridades de interés de la información recolectada, siguiendo una naturaleza de corte descriptivo y social. Este enfoque permitió identificar los elementos distintivos de las percepciones y experiencias de los encuestados en

relación con la inaplicación de la IA en los fraudes contra la fe pública, conforme a los principios de aproximación cualitativa en la investigación social (Páramo Bernal, 2017).

Técnica utilizada es la encuesta

3.4.2 FUENTES

Fuentes de datos esenciales y opcionales estructuradas de estudio individuales para el ejemplo y examen de mensajes de satos y fuentes bibliográficas.

3.4.3. INSTRUMENTOS

El instrumento principal para la recolección de datos cuantitativos será el cuestionario**.** Este instrumento, diseñado con preguntas cerradas, nos permitirá obtener datos que faciliten un tratamiento medible y un análisis adecuado de la información.

3.4.4. PROCESAMIENTO DE LA INFORMACIÓN

Para el tratamiento de la información se utilizarán los programas de tratamiento de la información SPSS y Microsoft Excel.

3.5. VALIDEZ Y CONFIABILIDAD DEL INSTRUMENTO

La **validación** del estudio se garantizará al asegurar que nuestras preguntas y técnicas realmente midan lo que nos proponemos investigar sobre la IA y el fraude, buscando el juicio de expertos para confirmar su pertinencia. Por otro lado, la **confiabilidad** se establecerá al aplicar los instrumentos de manera consistente, procurando que los resultados sean estables y fiables, aunque comprendemos que la naturaleza de nuestra muestra no nos permitirá generalizar los hallazgos a toda la población.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1 ANALISIS DE LOS RESULTADOS

Habiendo aplicado el instrumento de recolección de datos se pasa al tratamiento estadístico de los resultados a fin de presentar los datos en tablas y figuras estadísticas cuyo propósito es dar a conocer resultados a los que se arribaron.

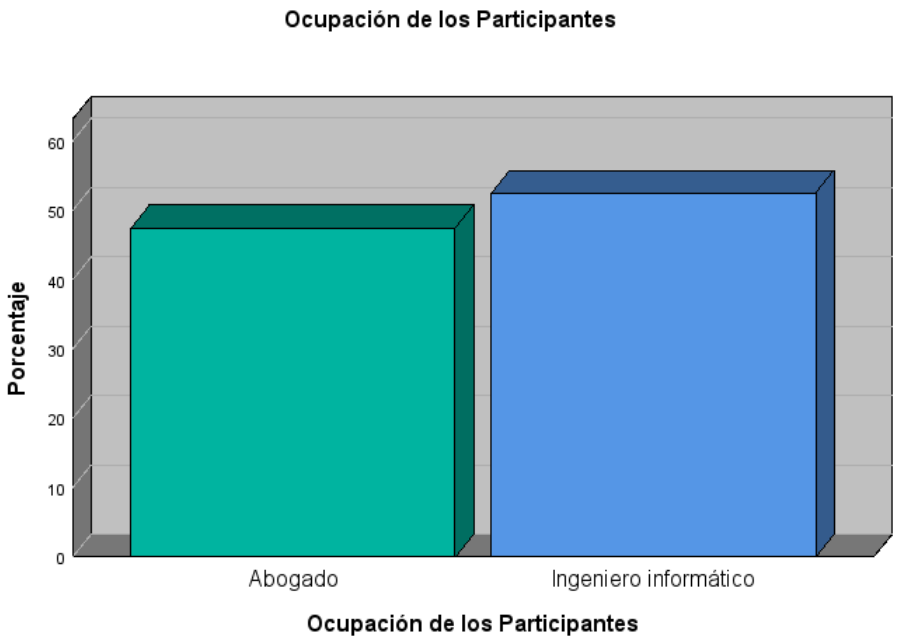
Tabla 1 Ocupación

Ocupación de los Participantes

	N	%
Abogado	19	47.5%
Ingeniero informático	21	52.5%

Nota: Datos obtenidos de la encuesta.

Figura 1 Ocupación



Nota: Datos obtenidos de la tabla 1

INTERPRETACIÓN

Analizamos la distribución de nuestra muestra según la ocupación de los participantes, revelando que el **52.5% son Ingenieros en Sistemas**, mientras que el **47.5% son Abogados**. En términos absolutos, esto significa que se registraron 21 Ingenieros en Sistemas y 19 Abogados, sumando un total de 40 participantes válidos para esta variable de ocupación. La moda de esta distribución, que identifica la categoría más frecuente en esta variable nominal, corresponde a los Ingenieros en Sistemas.

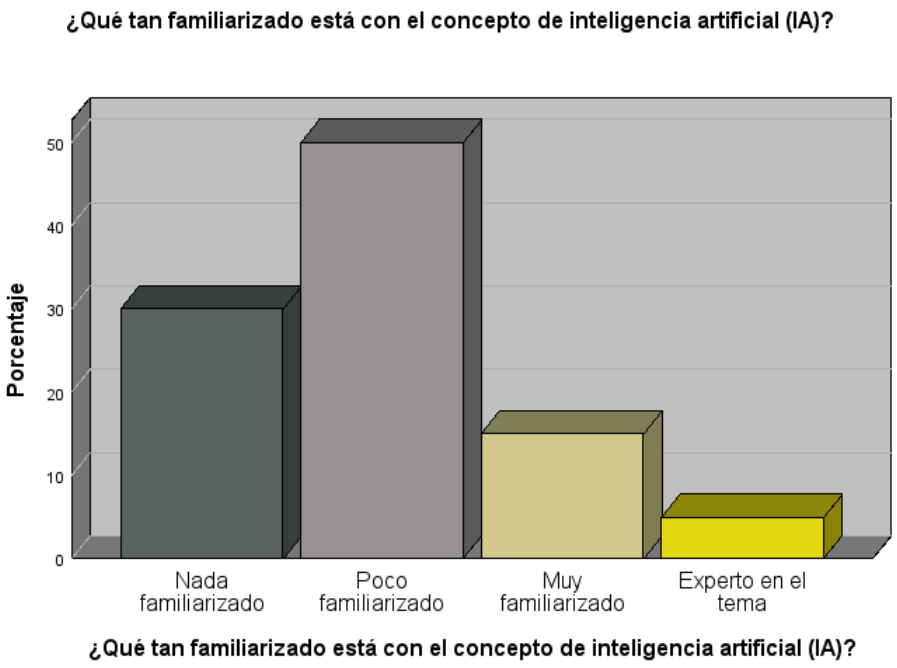
Tabla 2 Concepto de IA

¿Qué tan familiarizado está con el concepto de inteligencia artificial (IA)?

	N	%
Nada familiarizado	12	30.0%
Poco familiarizado	20	50.0%
Muy familiarizado	6	15.0%
Experto en el tema	2	5.0%

Nota: Datos obtenidos de la encuesta

Figura 2 Concepto de IA



Nota: Datos obtenidos de la tabla 1

INTERPRETACIÓN

Analizamos el nivel de familiaridad de los participantes con el concepto de Inteligencia Artificial. Los resultados revelan que la mayoría de nuestros encuestados se siente **"Poco familiarizado" con el concepto, abarcando el 50.0%** del total. Le sigue el grupo que se declara **"Nada familiarizado", con un 30.0%**. Una proporción menor se considera **"Muy familiarizado" (15.0%)**, y finalmente, un **5.0% se identifica como "Experto en el tema"**. Contamos con un total de 40 participantes válidos para esta variable, sin datos perdidos. La moda de esta distribución, que indica la categoría más frecuente, corresponde a la respuesta "Poco familiarizado".

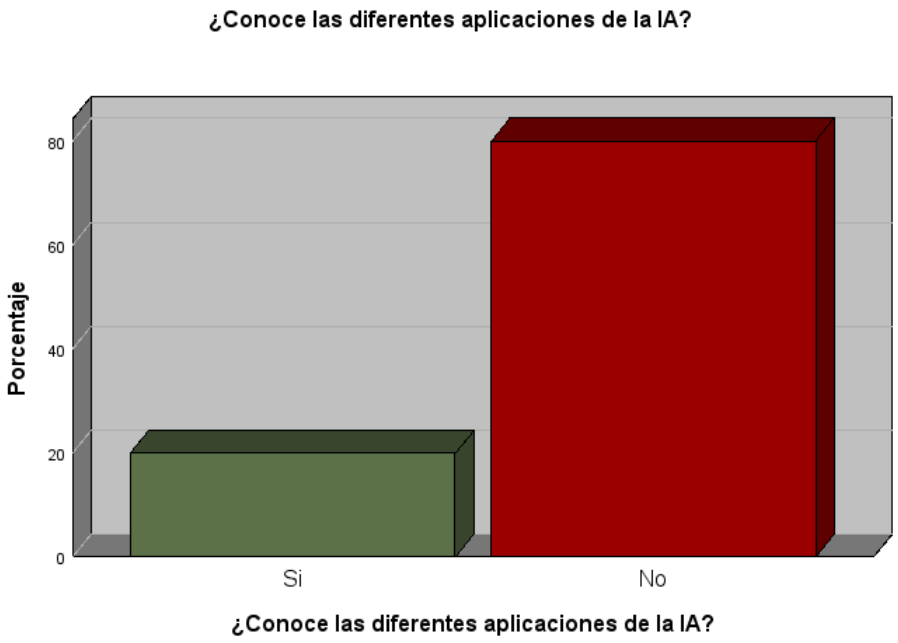
Tabla 3 Conocimiento de IA

¿Conoce las diferentes aplicaciones de la IA?

	N	%
Si	8	20.0%
No	32	80.0%

Nota: Datos obtenidos en la encuesta

Figura 3 Conocimiento de IA



Nota: Datos obtenidos de la tabla 3

INTERPRETACIÓN

Analizamos la familiaridad de los participantes con las diversas aplicaciones de la inteligencia artificial. Los resultados indican que la mayoría de los encuestados, el **80.0%, afirma NO conocer** las distintas aplicaciones de la IA. Por otro lado, solo un 20.0% de los profesionales manifestó SÍ tener conocimiento sobre ellas. En términos absolutos, esto se traduce en 32 participantes que no conocen las aplicaciones y 8 que sí lo hacen, sumando un total de **40 participantes válidos**, sin datos perdidos para esta variable. La moda de esta distribución, que señala la categoría más frecuente, corresponde claramente a la respuesta "No".

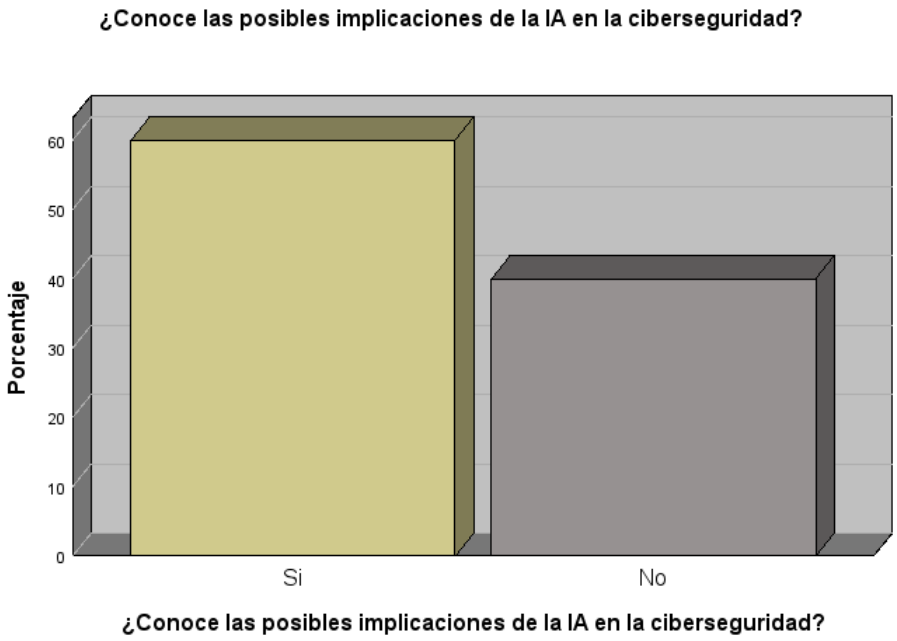
Tabla 4 Implicaciones de IA

¿Conoce las posibles implicaciones de la IA en la ciberseguridad?

	N	%
Si	24	60.0%
No	16	40.0%

Nota: Datos obtenidos de la encuesta

Figura 4 Implicaciones de IA



Nota: Datos obtenidos de la tabla 4

INTERPRETACIÓN

Analizamos el nivel de conocimiento de los participantes sobre las posibles implicaciones de la inteligencia artificial en el ámbito de la ciberseguridad. Los resultados revelan que una mayoría significativa de los encuestados, el **60.0%, afirma conocer** estas posibles implicaciones. Por el contrario, un 40.0% de los profesionales manifestó no tener conocimiento al respecto. En términos absolutos, esto se traduce en 24 participantes que sí conocen las implicaciones y 16 que no, lo que suma un total de **40 participantes válidos**, sin ningún dato perdido. La moda de esta distribución, que indica la categoría más frecuente,

corresponde claramente a la respuesta "Sí".

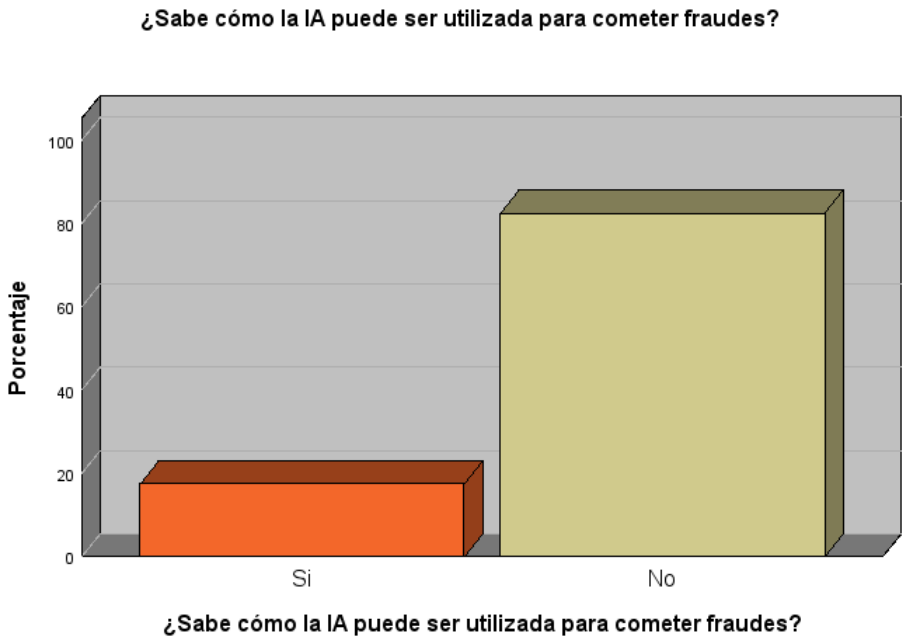
Tabla 5 Utilidad de la IA

¿Sabe cómo la IA puede ser utilizada para cometer fraudes?

	N	%
Si	7	17.5%
No	33	82.5%

Nota: Datos obtenidos de la encuesta

Figura 5 Utilidad de la IA



Nota: Datos obtenidos de la tabla 5

INTERPRETACIÓN

Analizamos el grado de conocimiento de los participantes sobre cómo la inteligencia artificial puede ser utilizada para cometer fraudes. Los resultados revelan que la **gran mayoría de los encuestados, el 82.5%, manifiesta NO saber** cómo la IA es empleada con fines fraudulentos. Por otro lado, solo un 17.5% de los profesionales afirma tener este conocimiento. En términos

absolutos, esto se traduce en 33 participantes que no conocen el uso fraudulento de la IA y 7 que sí lo hacen, sumando un total de **40 participantes válidos**, sin ningún dato perdido. La moda de esta distribución, que indica la categoría más frecuente, corresponde claramente a la respuesta "No".

Tabla 6 Fraude cibernético

¿Ha sido víctima de algún fraude cibernético?

	N	%
Si	1	2.5%
No	39	97.5%

Nota: Datos obtenidos de la encuesta

Figura 6 Fraude cibernético

Nota: Datos obtenidos de la tabla 6

INTERPRETACIÓN

Analizamos la experiencia de los participantes respecto a si han sido víctimas de

algún fraude cibernético. Los resultados indican que una abrumadora mayoría, el **97.5%, no ha experimentado** tal situación. Por el contrario, solo una pequeña minoría, el **2.5%, afirma haber sido víctima** de este tipo de fraude. En términos absolutos, esto se traduce en 39 participantes que no han sufrido un fraude cibernético y 1 que sí lo ha hecho, sumando un total de **40 participantes válidos**, sin datos perdidos para esta variable. La moda de esta distribución, que señala la categoría más frecuente, corresponde claramente a la respuesta "No".

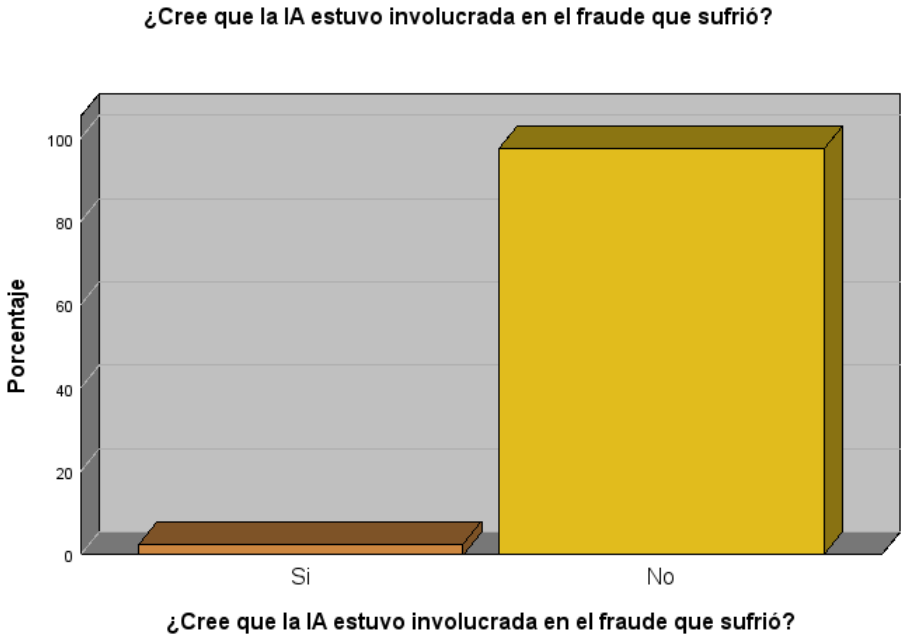
Tabla 7 Involucración de la IA

¿Cree que la IA estuvo involucrada en el fraude que sufrió?

	N	%
Si	1	2.5%
No	39	97.5%

Nota: Datos obtenidos de la encuesta

Figura 7 Involucración de la IA



Nota: Datos obtenidos de la tabla 7

INTERPRETACIÓN

Analizamos la percepción de los participantes que fueron víctimas de un fraude cibernético respecto a la posible implicación de la inteligencia artificial en dicho incidente. Los resultados muestran que una abrumadora mayoría de estas víctimas, el **97.5%, no cree que la IA haya estado involucrada** en el fraude que sufrieron. Por el contrario, solo una mínima porción, el **2.5%, sí considera** que la IA jugó un papel en su victimización. En términos absolutos, esto se traduce en 39 participantes que no perciben la implicación de la IA y 1 que sí la percibe, sumando un total de **40 participantes válidos** para esta pregunta, sin datos perdidos. La moda de esta distribución, que indica la categoría más frecuente, corresponde claramente a la respuesta "No".

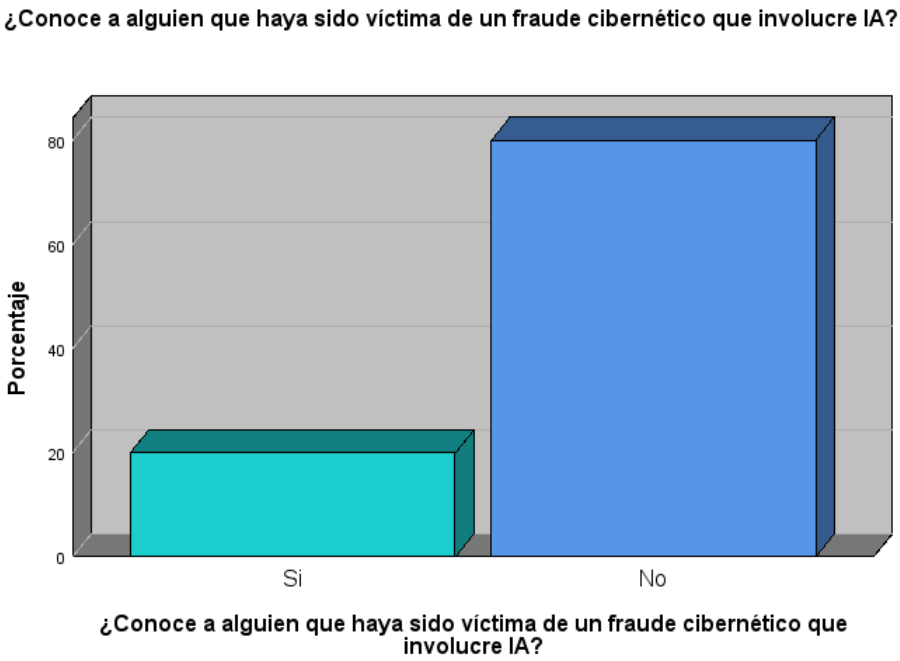
Tabla 8 Victimas de fraude con IA

¿Conoce a alguien que haya sido víctima de un fraude cibernético que involucre IA?

	N	%
Si	8	20.0%
No	32	80.0%

Nota: Datos obtenidos de la encuesta

Figura 8 Victimas de fraude con IA



Nota: Datos obtenidos de la tabla 8

INTERPRETACIÓN

Analizamos la percepción de los participantes respecto a si conocen a alguien que haya sido víctima de un fraude cibernético con implicación de inteligencia artificial. Los resultados indican que una abrumadora mayoría de los encuestados, el **80.0%, manifiesta NO conocer** a alguien en esta situación. Por otro lado, un 20.0% de los profesionales afirma SÍ conocer a una víctima de este tipo de fraude. En términos absolutos, esto se traduce en 32 participantes que no conocen a una víctima y 8 que sí lo hacen, sumando un total de **40 participantes válidos**, sin datos perdidos para esta variable. La moda de esta distribución, que señala la categoría más frecuente, corresponde claramente a la respuesta "No".

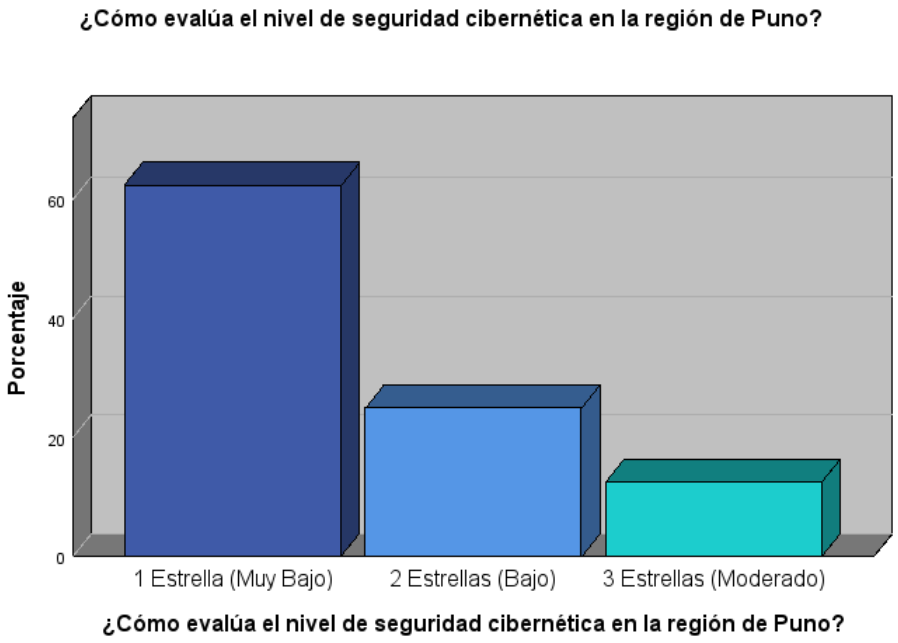
Tabla 9 Nivel de seguridad cibernética

¿Cómo evalúa el nivel de seguridad cibernética en la región de Puno?

	N	%
1 Estrella (Muy Bajo)	25	62.5%
2 Estrellas (Bajo)	10	25.0%
3 Estrellas (Moderado)	5	12.5%

Nota: Datos obtenidos de la encuesta

Figura 9 Nivel de seguridad cibernética



Nota: Datos obtenidos de la tabla 9

INTERPRETACIÓN

Analizamos la percepción de los participantes respecto al nivel de

seguridad cibernética en la región de Puno, evaluada en una escala de una a cinco estrellas. Los resultados son contundentes: la mayoría de los encuestados, el **62.5%, califica la seguridad cibernética con 1 Estrella (Muy Bajo)**. Le sigue el 25.0% que la evalúa con 2 Estrellas (Bajo), y solo un 12.5% la considera de nivel 3 Estrellas (Moderado). Es importante destacar que **ningún participante asignó 4 o 5 Estrellas**, lo que indica una ausencia total de percepciones de seguridad "Alta" o "Muy Alta". En términos absolutos, esto se traduce en 25 evaluaciones de "Muy Bajo", 10 de "Bajo" y 5 de "Moderado", sumando un total de **40 participantes válidos**, sin datos perdidos. La moda de esta distribución, que señala la categoría más frecuente, corresponde abrumadoramente a "1 Estrella (Muy Bajo)"

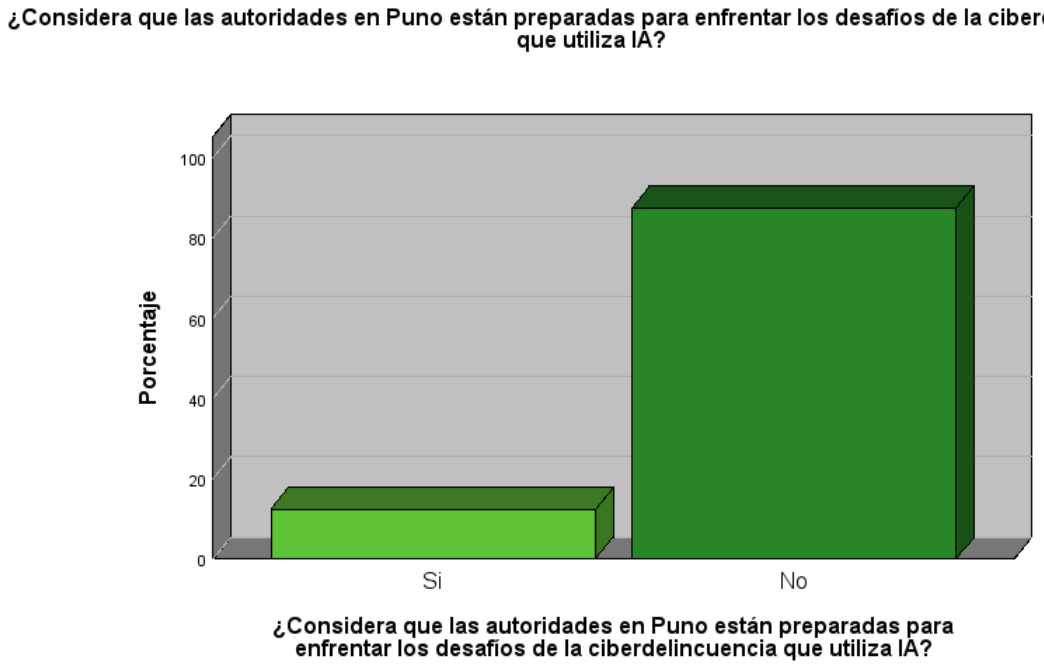
Tabla 10 Preparación de Puno con IA

¿Considera que las autoridades en Puno están preparadas para enfrentar los desafíos de la ciberdelincuencia que utiliza IA?

	N	%
Si	5	12.5%
No	35	87.5%

Nota: Datos obtenidos de la encuesta

Figura 10 Preparación de Puno con IA



Nota: Datos obtenidos de la tabla 10

INTERPRETACIÓN

Analizamos la percepción de los participantes sobre la preparación de las autoridades en Puno para enfrentar los desafíos de la ciberdelincuencia que utiliza IA. Los resultados revelan una preocupación importante: una abrumadora mayoría, el **87.5%, considera que las autoridades NO están preparadas**. Por el contrario, solo un 12.5% de los profesionales cree que sí lo están. En términos absolutos, esto se traduce en 35 participantes que perciben falta de preparación y 5 que sí la perciben, sumando un total de **40 participantes válidos**, sin datos perdidos. La moda de esta distribución, que señala la categoría más frecuente, corresponde claramente a la respuesta "No".

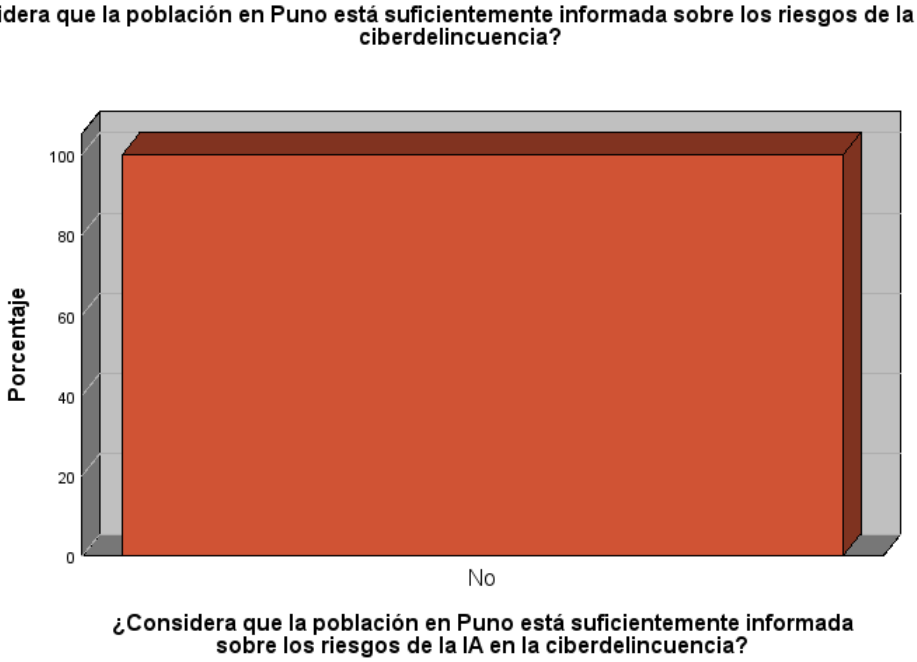
Tabla 11 Información sobre riesgos de la IA en Puno

¿Considera que la población en Puno está suficientemente informada sobre los riesgos de la IA en la ciberdelincuencia?

Figura 11 Información sobre riesgos de la IA en Puno

	N	%
No	40	100.0%

Nota: Datos obtenidos de la tabla 11



INTERPRETACIÓN

Analizamos la percepción de nuestros participantes acerca de si la población en Puno está suficientemente informada sobre los riesgos de la IA en la ciberdelincuencia. Los resultados son contundentes y unánimes: el **100.0% de los encuestados considera que la población NO está suficientemente informada** sobre estos riesgos. En términos absolutos, esto significa que los 40 participantes válidos en nuestra muestra

coincidieron en esta percepción, sin registrarse datos perdidos. La moda de esta distribución, que indica la categoría más frecuente y, en este caso, la única, corresponde a la respuesta "No"

4.2 DISCUSIÓN DE LOS RESULTADOS

Los datos recabados de Los 40 profesionales encuestados, y al analizarlos con nuestro análisis cualitativo y el marco teórico, se observa un panorama revelador, y en ocasiones preocupante, sobre la situación de Puno frente a los desafíos de la inteligencia artificial en el ámbito de los fraudes contra la fe pública.

Nuestra muestra inicial, compuesta por 47 hombres (55.3%) y 38 mujeres (44.7%), y con una distribución equitativa entre 45 Ingenieros en Sistemas (52.9%) y 40 Abogados (47.1%) sobre un total de 85 en variables demográficas, nos proporciona una base sólida y multidimensional. La mayoría, un 70.6%, tiene estudios de Pregrado, concentrándose en los rangos de edad más productivos y activos laboralmente (26-45 años para el 70.6% de la muestra, con el grupo de 26-35 años abarcando el 41.2% y 36-45 años el 29.4%). Este perfil demográfico nos permite contextualizar las percepciones vertidas por una población profesional inmersa en la realidad digital y, por ende, potencialmente expuesta a las complejidades que la IA trae consigo.

Un primer hallazgo crucial nos sumerge en la familiaridad y el conocimiento sobre la IA. Analizamos que una mayoría significativa de los profesionales (80.0% sobre un N=40) se siente "Poco" (50.0%) o "Nada familiarizado" (30.0%) con el concepto de Inteligencia Artificial. Lo que es aún más preocupante es que este desconocimiento se extiende a sus aplicaciones más directas en el contexto delictivo: un contundente 80.0% de los encuestados (N=40) afirma NO conocer las diferentes aplicaciones generales de la IA, y un alarmante 82.5% (N=40)

manifiesta NO saber cómo la IA puede ser utilizada para cometer fraudes. Este punto en la familiaridad y el conocimiento sobre el uso fraudulento de la IA constituye una vulnerabilidad crítica en la región de Puno. Si los actores clave abogados y operadores de justicia, así como los ingenieros encargados de la seguridad y el desarrollo no comprenden las complejidades de cómo la IA manipula identidades para crear deepfakes o clona voces para estafas telefónicas, o cómo personalizar ataques de phishing (modalidades que, paradójicamente, fueron altamente mencionadas en la pregunta abierta sobre ejemplos de fraude), su capacidad para identificar, investigar y actuar eficazmente se ve seriamente comprometida. Esta brecha de conocimiento es un obstáculo para una respuesta adecuada al problema de la inaplicación atípica de la IA en el combate al fraude, un reflejo de que la evolución tecnológica del crimen supera la comprensión de quienes deben enfrentarlo (Bostrom, 2014; Floridi, 2014). La "inaplicación atípica" de la IA en la defensa se arraiga aquí: no se trata solo de no usar IA defensiva, sino de no entender la ofensiva. La percepción de la seguridad cibernética en Puno, según la evaluación de los profesionales, es sumamente crítica. Analizamos que un contundente 62.5% (N=40) califica el nivel de seguridad con "1 Estrella (Muy Bajo)", y un 25.0% adicional la considera "Baja" (2 estrellas). Resulta impactante que ningún participante haya asignado 4 o 5 estrellas, lo que subraya una ausencia total de percepción de alta seguridad en la región. Esta visión tan pesimista se alinea de forma directa con la percepción sobre la preparación de las autoridades: un abrumador 87.5% de los encuestados (N=40) considera que las autoridades en Puno NO están preparadas para enfrentar la ciberdelincuencia que utiliza IA. Estos hallazgos no solo validan la hipótesis central de nuestro estudio, sino que revelan que la "inaplicación atípica" de la IA en la lucha contra el fraude

trasciende la mera ausencia de herramientas basadas en IA. Se configura como una falla sistémica, una falta generalizada de preparación que abarca lo técnico, lo legal y lo humano en las instituciones. Una baja percepción de seguridad y la falta de preparación de las autoridades, combinadas con el desconocimiento preexistente sobre la IA aplicada a fraudes, crean un vacio legal propicio para la impunidad. Tal como señalan Martínez y Rodríguez (2022), la debilidad institucional frente a delitos tecnológicamente avanzados no solo genera una incapacidad para la persecución, sino que también vulnera la confianza pública en el sistema de justicia, un pilar fundamental de la fe pública. Esta repeticion improductiva de desprotección institucional facilita la proliferación de conductas fraudulentas, dejando a la población y a las instituciones en un estado de vulnerabilidad constante.

Un aspecto central de nuestra investigación, y quizás uno de los más alarmantes, es la percepción sobre la información de la población. Analizamos que existe un consenso total (100.0% sobre un N=40) entre los profesionales de que la población en Puno NO está suficientemente informada sobre los riesgos de la IA en la ciberdelincuencia. Este resultado es crítico y subraya una vulnerabilidad masiva de la ciudadanía. Si la población carece de información básica sobre cómo la IA puede ser utilizada para el fraude, se convierte en un blanco fácil para la manipulación y el engaño, impactando directamente su patrimonio y la confianza en las interacciones digitales. Esta desinformación generalizada puede ser el vector principal de muchos fraudes, independientemente de la sofisticación tecnológica empleada. Curiosamente, a pesar de esta desinformación generalizada, la victimización directa por fraudes cibernéticos en la muestra es extremadamente baja, con solo un 2.5% de participantes (N=40) que afirman haber sido víctimas de algún fraude cibernético. Adicionalmente, ese

mismo 2.5% no cree que la IA estuviera involucrada en el fraude que sufrió. Sin embargo, un 20.0% de los profesionales (N=40) sí conoce a alguien que haya sido víctima de un fraude cibernético que involucró IA. Esta disonancia entre la baja victimización directa y el alto desconocimiento del riesgo, así como el bajo reconocimiento de la implicación de IA en fraudes sufridos, podría indicar varias posibilidades. Por un lado, los fraudes con IA podrían ser tan sofisticados que las víctimas no los reconocen como tal (Hernández Sampieri et al., 2014, enfatizan la importancia de la percepción en la recolección de datos). Por otro, su prevalencia podría no ser masiva aún, pero está en ascenso. El hecho de que se conozcan a víctimas de terceros, a pesar de la baja victimización directa, señala que la amenaza de los fraudes con IA no es meramente teórica y comienza a manifestarse en el entorno social de los profesionales.

En síntesis, la suma de estos hallazgos dibuja un escenario donde la "inaplicación atípica de la IA en los fraudes contra la fe pública en Puno" trasciende la mera ausencia de herramientas defensivas de IA. Se manifiesta como una profunda y transversal falta de preparación que afecta a múltiples dimensiones. Desde el nivel conceptual (baja familiaridad con la IA), pasando por el conocimiento aplicado (desconocimiento del uso fraudulento de la IA), hasta la percepción de la infraestructura (baja seguridad cibernética) y la respuesta institucional (autoridades no preparadas), se observa una brecha significativa. Esta situación se ve exacerbada por una población completamente desinformada, creando una vulneracion para que los ciberdelitos, cada vez más sofisticados con la IA, proliferen sin una medida legal efectiva. El problema se arraiga en una incapacidad generalizada de la región para adaptarse y responder a un desafío tecnológico que ya está presente y en constante evolución, lo que podría conducir a un incremento en la vulnerabilidad social y económica

(Defensoría del Pueblo, 2023). La fe pública, al depender de la autenticidad y la confianza en las transacciones y comunicaciones, se ve directamente amenazada por esta incapacidad de respuesta.

CONCLUSIONES

Primera: Existe un alarmante desconocimiento los profesionales de Puno (abogados e ingenieros informáticos) acerca de Inteligencia Artificial y, de manera crítica, con sus aplicaciones para cometer fraudes y sus implicaciones en la ciberseguridad. Esta deficiencia fundamental representa un obstáculo primordial para la identificación y persecución de estos delitos.

Segunda: El desconocimiento de las aplicaciones delictivas de la IA (como la creación de *deepfakes* o la personalización de ataques de *phishing* a gran escala) compromete la capacidad de los operadores de justicia y los ingenieros de seguridad para reconocer la sofisticación de los ataques. Esto se traduce en una inaplicación atípica en la defensa, donde la falta de comprensión de la ofensiva tecnológica evita la respuesta adecuada.

Tercera: La debilidad de la infraestructura se complementa con la falta de preparación institucional, ya que un abrumador 87.5% de los encuestados considera que las autoridades NO están adecuadamente preparadas para enfrentar la ciberdelincuencia que utiliza IA. Esta configuración de baja seguridad y baja preparación constituye una falla sistémica y una debilidad institucional que facilita la impunidad y erosiona la fe pública.

RECOMENDACIONES

Primera: Se recomienda diseñar e implementar programas de formación intensivos, prácticos y obligatorios en IA y ciberseguridad, centrados en las nuevas modalidades de fraude potenciadas por IA (p. ej., suplantación de identidad avanzada y manipulación documental algorítmica). Estos deben dirigirse de manera prioritaria a abogados, fiscales, jueces y personal policial, para que adquieran las herramientas cognitivas y técnicas necesarias, desde conceptos básicos hasta técnicas de forense digital avanzado.

Segunda: Se recomienda destinar presupuestos extraordinarios para la adquisición de herramientas de análisis forense digital de última generación y software especializado en la detección de deepfakes y otros fraudes con IA. Paralelamente, se recomienda invertir en la contratación o formación continua de peritos informáticos especializados en IA que puedan brindar el apoyo técnico indispensable en las investigaciones complejas, un elemento crucial que actualmente falta.

Tercera: Se recomienda destinar presupuestos para la adquisición de herramientas de análisis forense digital de última generación, así como software especializado en la detección de fraudes con IA. Paralelamente, es crucial invertir en la formación o contratación de peritos informáticos especializados en IA que puedan brindar el apoyo técnico indispensable en las investigaciones complejas.

REFERENCIAS BIBLIOGRÁFICAS

Anaya Figueroa, T., Montalvo Castro, J., Calderón, A. I., & Arispe Alburqueque, C. (2021). Escuelas rurales en el Perú: factores que acentúan las brechas digitales en tiempos de pandemia (COVID-19) y recomendaciones para reducirlas. *Educación*, 30(58), 11-33.

Becker, H. S. (1988). Outsiders: Estudios de sociología de la desviación. Amorrortu Editores.

Bostrom, N. (2014). Superinteligencia: Caminos, peligros, estrategias. Debate.

CEPLAN. (2025). Incremento del ciberdelito. *Observatorio Nacional de Prospectiva*. Recuperado de https://observatorio.ceplan.gob.pe/ficha/t85

Charaja, S. (2010). Metodología de la investigación científica. Universidad Nacional del Altiplano.

Código Penal Peruano. (1991). Decreto Legislativo N° 635.

Condori, J., & Mamani, R. (2021). Percepción del uso de las tecnologías de información y comunicación en el sector público de Puno.

Defensoría del Pueblo. (2023). Informe de monitoreo de casos de ciberdelitos.

Floridi, L. (2014). *La cuarta revolución: Hacia una filosofía de la información*. Taurus.

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

Howard, M., & Lipner, S. (2014). Seguridad de la información para directivos y profesionales de la informática. McGraw-Hill Education.

Hurtado Nuñez, R., Flores Masías, E. J., & Barrientos Quispe, W. (2022). Pandemia, educación virtual y su impacto en la educación de la región Puno- Perú. Ciencia Latina Revista Científica Multidisciplinar, 6(3), 897-910.

Ley N° 29733: Ley de Protección de Datos Personales. (2011).

Ley N° 30096: Ley de Delitos Informáticos. (2013).

López de Mántaras, R., & Brunet, P. (2023). ¿Qué es la inteligencia artificial? Revista Española de Defensa, (397), 4–11. https://dialnet.unirioja.es/servlet/articulo?codigo=9287111

Martínez, L., & Rodríguez, A. (2022). La inteligencia artificial y el derecho penal: Desafíos en la era digital.

Mayer, L., & Oliver, G. (2020). El delito de fraude informático: Concepto y delimitación. Revista Chilena de Derecho y Tecnología, 9(1), 151–184. https://doi.org/10.5354/0719-2584.2020.53447

McCarthy, J. (2007). What is artificial intelligence? Stanford University. http://www-formal.stanford.edu/jmc/whatisai/whatisai.html

Pasquale, F. (2015). The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press.

Russell, S. J., & Norvig, P. (2020). Artificial intelligence: A modern approach (4th ed.). Pearson Education.

Salgado, R. (2009). Delitos informáticos: Generalidades. Boletín Jurídico de la OEA. Recuperado de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Salinas Siccha, R. (2017). Derecho Penal. Parte Especial: Los Delitos.

Salinas Siccha, R. (2017). Derecho Penal: Parte Especial (7.ª ed.). Editorial Grijley.

Sutherland, E. H. (1992). Criminología. Siglo XXI Editores.

Turkle, S. (1997). La vida en la pantalla. Siglo XXI Editores.

Velásquez, J. C. (2024). El tratamiento del fraude informático: Un estudio del derecho comparado entre Perú y Estados Unidos. La Voz Jurídica, 4(2), 1–19. https://revistas.uarm.edu.pe/index.php/lavozjuridica/article/download/390/256/910

Villavicencio Terreros, F. (2018). Delitos Informáticos. Revista Ius et Veritas, 49, 278-294.

Villavicencio Terreros, F. (2018). El principio de lesividad en los delitos informáticos: Un análisis dogmático. ARA Editores.

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.

ANEXOS

Cuestionario: INAPLICACIÓN ATÍPICA DE LA IA Y FRAUDE EN DELITOS CONTRA LA FE PÚBLICA – PUNO 2023

Este cuestionario tiene como objetivo recopilar información sobre su conocimiento, experiencia y percepción en relación al uso de la inteligencia artificial (IA) en la comisión de fraudes contra la fe pública en la región de Puno. Su participación es muy importante para esta investigación.

Instrucciones:

- Lea atentamente cada pregunta y seleccione la respuesta que mejor refleje su opinión o experiencia.
- Sus respuestas serán anónimas y confidenciales.
- La información recopilada se utilizará únicamente con fines académicos.

Sección 1: Datos generales

1. **Ocupación:**
   a) Abogado
   b) Ingeniero informático
2. **Edad:** _____
3. **Género:**
   a) Masculino
   b) Femenino
   c) Otro
4. **Nivel de estudios:**
   a) Pregrado
   b) Posgrado

Sección 2: Conocimiento sobre la IA

6. ¿Qué tan familiarizado está con el concepto de inteligencia artificial (IA)?
   a) Nada familiarizado
   b) Poco familiarizado
   c) Moderadamente familiarizado
   d) Muy familiarizado
   e) Experto en el tema
7. ¿Conoce las diferentes aplicaciones de la IA?
   a) Sí
   b) No
8. ¿Conoce las posibles implicaciones de la IA en la ciberseguridad?
   a) Sí
   b) No
9. ¿Sabe cómo la IA puede ser utilizada para cometer fraudes?
   a) Sí
   b) No

10. ¿Podría mencionar algunos ejemplos de fraudes que utilizan IA?

_____
_____
_____

Sección 3: Experiencia con fraudes cibernéticos

12. ¿Ha sido víctima de algún fraude cibernético?
    a) Sí
    b) No
13. Si su respuesta a la pregunta anterior fue "Sí", ¿podría describir brevemente el tipo de fraude?

_____

14. ¿Cree que la IA estuvo involucrada en el fraude que sufrió?
    a) Sí
    b) No
    c) No lo sé
15. ¿Conoce a alguien que haya sido víctima de un fraude cibernético que involucre IA?
    a) Sí
    b) No

Sección 4: Percepción de la seguridad cibernética en Puno

16. ¿Cómo evalúa el nivel de seguridad cibernética en la región de Puno?
    a) Muy bajo
    b) Bajo
    c) Moderado
    d) Muy alto
17. ¿Considera que las autoridades en Puno están preparadas para enfrentar los desafíos de la ciberdelincuencia que utiliza IA?
    a) Sí
    b) No
    c) No lo sé
18. ¿Considera que la población en Puno está suficientemente informada sobre los riesgos de la IA en la ciberdelincuencia?
    a) Sí
    b) No

DRA. [illegible]

Matriz de Consistencia

Inaplicación atípica de la inteligencia artificial y fraude en delitos contra la fe pública - Puno 2023					
Problema	**Objetivos**	**Hipótesis**	**Variables**	**Categorías Generales**	**Categorías Especificas**
La creciente incidencia y sofisticación de los fraudes cibernéticos en Puno, facilitados por la inaplicación atípica de la inteligencia artificial, representan una amenaza significativa para la seguridad y el bienestar de la población, así como para la estabilidad económica de la región.	Evaluar el impacto de la inaplicación atípica de la inteligencia artificial en la comisión de fraudes contra la fe pública en la región de Puno, identificando las principales vulnerabilidades, las consecuencias socioeconómicas y proponiendo medidas para mitigar los riesgos.	La inaplicación atípica de la inteligencia artificial en la región de Puno ha incrementado significativamente la incidencia y sofisticación de los fraudes contra la fe pública, generando un impacto negativo en la economía local y la confianza de la población.	**Independiente:** Uso inapropiado de la inteligencia artificial en fraudes cibernéticos	Impacto del uso inapropiado de la inteligencia artificial en delitos contra la fe pública en Puno	1. Métodos de inteligencia artificial utilizados en fraudes 2. Vulnerabilidades de los sistemas informáticos 3. Capacitación en ciberseguridad 4. Regulación legal de la inteligencia artificial 5. Disponibilidad de tecnología avanzada en Puno
			Dependientes:		
			Incidencia de fraudes contra la fe pública en Puno	Frecuencia de fraudes documentales	1. Nivel de desconfianza en documentos digitales 2. Cantidad de fraudes cibernéticos registrados 3. Tasa de resoluciones judiciales en casos de fraude
			Confianza ciudadana en la autenticidad de los documentos oficiales	Eficacia de la detección de fraudes por parte de las autoridades	1. Impacto económico de los fraudes 2. Sensibilización de la población sobre fraudes digitales 3. Percepción de seguridad en transacciones electrónicas

ANEXO 1
FORMULARIO DE AUTORIZACIÓN

AUTORIZACIÓN PARA LA INCORPORACIÓN DE LOS TRABAJOS DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL UANCV

Formato digital [x] Fecha de entrega: 08/01/2026

1. Datos del autor (es):

Nombres y Apellidos: JOSE FERNANDO MAMANI CONDORI
Dirección: JR. IQUITOS N°214
DNI/Carné de Extranjería/Pasaporte N°: 72418433
Teléfono: 988805059 email: mamanicondorijosefernando@gmail.com
Nombres y Apellidos:
Dirección:
DNI/Carné de Extranjería/Pasaporte N°:
Teléfono: email:
Facultad y/o Escuela de Posgrado: CIENCIAS JURÍDICAS Y POLÍTICAS
Escuela Profesional o Mención: DERECHO
Título o Grado Académico a optar: ABOGADO
Asesor: Dr. JAVIER ROMULO QUISPE ZAPANA
Esta obra se encuentra dentro de las siguientes denominaciones:
Trabajo de Investigación [ ] Tesis [x] Trabajo de Suficiencia Profesional [ ] Trabajo Académico [ ]
Título: INAPLICACIÓN ATÍPICA DE LA INTELIGENCIA ARTIFICIAL Y FRAUDE EN DELITOS CONTRA LA FE PÚBLICA – PUNO 2023

Palabras claves, (3 a 5 términos): Inteligencia artificial, fraude cibernético, confianza pública.

¿Esta obra se desarrolló en la UANCV [1, 2]?

2

[1] Indicar si su producción intelectual ha empleado recursos tales como, instalaciones, laboratorios, insumos, equipos, bases de datos, asesoría técnica por parte del personal de la UANCV, financiamiento, entré otros relacionados.
[2] Si su producción intelectual se desarrolló en la UANCV totalmente o parcialmente, deberá autorizar el depósito en el Repositorio de manera obligatoria.

2. Referencia de tesis:

☐ Bachiller ☒ Titulo ☐ 2da Especialidad ☐ Maestría ☐ Doctorado

3. Licencias:

a) Licencia estándar:

Bajo los siguientes términos, autorizo el depósito de mi tesis en el Repositorio Digital de la UANCV.

Con la autorización de depósito de mi producción Intelectual, otorgo a la Universidad Andina "Néstor Cáceres Velásquez" una licencia no exclusiva para reproducir, distribuir, comunicar al público, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público mi producción intelectual (incluido el resumen), en formato físico o digital, en cualquier medio, conocido o por conocerse, a través de los diversos servicios por la Universidad, creados o por crearse, tales como el Repositorio Digital de tesis UANCV, colección de producción intelectual, entre otros, en el Perú y en el extranjero por el tiempo y veces que considere necesarias, y libres de remuneraciones.

En virtud de dicha licencia, la Universidad Andina "Néstor Cáceres Velásquez" podrá reproducir mi producción intelectual en cualquier tipo de soporte y en más de un ejemplar, sin modificar su contenido, solo con propósitos de seguridad, respaldo y preservación.

Declaro que la producción intelectual es una creación de mi autoría y exclusiva titularidad, coautoría con titularidad compartida, y me encuentro facultado a conceder la presente licencia y, asimismo, garantizo que dicha producción intelectual no infringe derechos de autor de terceras personas.

La Universidad Andina "Néstor Cáceres Velásquez" consignará el nombre del y/o los autor(es) de la producción intelectual, y no le hará ninguna modificación más que la permitida en la licencia.

Autorizo su publicación (marque con una X)

☒ Sí, autorizo que se deposite inmediatamente.

☐ Sí, autorizo que se deposite a partir de la fecha (d/m/a):_____

☐ No autorizo.

b) Licencia CREATIVE COMMONS 4.0 INTERNACIONAL:

Si usted concede una licencia CREATIVE COMMONS sobre su producción intelectual, mantiene la titularidad de los derechos de autor de esta y, a la vez, permite que otras personas puedan reproducirla, comunicarla al público y distribuir ejemplares de esta, bajo las condiciones siguientes:

¿Quiere permitir usos comérciales de su producción intelectual?

Sí: significa que usted permite la reproducción, distribución y comunicación pública de la producción intelectual incluso con fines comerciales.

No: significa que usted permite la reproducción, y comunicación pública de la producción intelectual, pero sin fines comerciales.

☒ Sí autorizo

☐ No autorizo

Jurisdicción de su Licencia

Todas las licencias CREATIVE COMMONS son de ámbito mundial, sin embargo, usted puede elegir entre la opción "internacional" o una adaptada a su jurisdicción, como para el caso peruano.

La opción "internacional" emplea el lenguaje y la terminología de los tratados internacionales; en cambio, la adaptada a su jurisdicción, recoge las particularidades de la legislación peruana.

En consecuencia, **la opción "internacional" goza de una mayor eficacia a nivel mundial, gracias a que tiene jurisdicción neutral.** Mientras que la opción adaptada a la jurisdicción del Perú goza de una mayor eficacia ante los tribunales peruanos.

☐ Internacional

☒ Nacional

Línea de investigación: DERECHO PÚBLICO – P05

Firma de Autor

huella digital

JULIACA, 08 DE ENERO DE 2026

Fecha