UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

CARRERA DE SOFTWARE

TRABAJO DE INTEGRACIÓN CURRICULAR
PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERO EN SOFTWARE

FORMA: PROYECTO DE INVESTIGACIÓN

TEMA:

IMPACTO DE REDES NEURONALES PARA RECONOCIMIENTO FACIAL EN LA SEGURIDAD DE LA INFORMACIÓN

AUTOR:

EDWIN LEONEL BELDUMA BELDUMA

DIRECTOR:

LIC. EDGAR PATRICIO RIVADENEIRA RAMOS

GUARANDA – ECUADOR

2025

TEMA DEL PROYECTO DE INVESTIGACIÓN

IMPACTO DE REDES NEURONALES PARA RECONOCIMIENTO FACIAL EN LA SEGURIDAD DE LA INFORMACIÓN

AGRADECIMIENTO

La realización de este proyecto de investigación no solo representa un logro personal, sino también el fruto del inestimable apoyo de diversas personas e instituciones que, con su dedicación, compromiso y generosidad, han hecho posible su desarrollo.

Agradezco sinceramente al Lic. Edgar Rivadeneira, director de este trabajo, por su orientación académica, su compromiso constante y su disponibilidad para acompañarme en cada etapa del proceso de investigación. Sus acertados consejos, sus precisas observaciones y su rigor académico han sido fundamentales para la estructuración y solidez de este proyecto.

Expreso también mi profundo reconocimiento a los pares académico, Dr. Henry Vallejo y Fís. Rafael Medina, por su activa participación en la revisión de este trabajo. Su perspectiva crítica, sus constructivas aportaciones y su exigencia profesional han enriquecido la calidad y profundidad de este estudio.

Agradezco también a los profesores de la Universidad Estatal de Bolívar que, a lo largo de mis estudios universitarios, me transmitieron no solo conocimientos técnicos y teóricos, sino también valores y herramientas esenciales para la práctica profesional. Su vocación pedagógica y su dedicación contribuyeron a mi desarrollo académico y personal. A mis compañeros de clase, les agradezco sinceramente la colaboración, el diálogo constante y la camaradería que han caracterizado nuestra trayectoria universitaria. Compartir este camino con ustedes ha hecho que el aprendizaje sea más enriquecedor y humano.

Por último, expreso mi más profundo agradecimiento a todas las personas que, directa o indirectamente, han contribuido al desarrollo de esta investigación. Este trabajo también es testimonio de su apoyo y compromiso.

DEDICATORIA

Dedico este logro, con profunda gratitud y afecto, a mi familia, pilar fundamental en cada etapa de mi desarrollo académico y personal; a mis padres, por su compromiso, perseverancia y amor incondicional.

A mi padre, que con su sabiduría, sacrificio y apoyo constante me ha dado las herramientas necesarias para avanzar. A mi madre, por su ternura, sus enseñanzas y por creer en mí incluso en los momentos más difíciles. A mi hermana, por su compañía, su comprensión y su apoyo incondicional en cada etapa de este camino. Su presencia ha sido una fuente constante de motivación.

Gracias a todos por acompañarme a lo largo de este proceso, por vuestra paciencia, vuestro ánimo y vuestro apoyo cuando más lo necesitaba. Este trabajo no solo es el reflejo de mis esfuerzos, sino también del amor y la unidad familiar que me han impulsado a lograrlo.

CERTIFICADO DE VALIDACIÓN

Lic. Edgar Rivadeneira, Dr. Henry Vallejo e Fis. Rafael Medina, en su orden Director y Pares Académicos del Trabajo de Integración Curricular "IMPACTO DE REDES NEURONALES PARA RECONOCIMIENTO FACIAL EN LA SEGURIDAD DE LA INFORMACIÓN" desarrollado por el señor Edwin Leonel Belduma Belduma.

CERTIFICAN

Que, luego de revisado el Trabajo de Integración Curricular en su totalidad, cumple con las exigencias académicas de la carrera SOFTWARE, por lo tanto, autorizamos su presentación y defensa.

Guaranda, 12 del Agosto del 2025

Firmado electrónicamente por:
EDGAR PATRICIO RIVADENEIRA RAMOS
Validar únicamente con FirmaEC

Lic. Edgar Rivadeneira
Director

Firmado electrónicamente por:
SEGUNDO RAFAEL MEDINA VELASCO
Validar únicamente con FirmaEC

Fis. Rafael Medina
Par Académico

Firmado electrónicamente por:
HENRY FERNANDO VALLEJO BALLESTEROS
Validar únicamente con FirmaEC

Dr. Henry Vallejo
Par Académico

DERECHOS DE AUTOR

Yo Edwin Leonel Belduma Belduma portador de la Cédula de Identidad No 0750722258 en calidad de autor y titular de los derechos morales y patrimoniales del Trabajo de Titulación:
"IMPACTO DE REDES NEURONALES PARA RECONOCIMIENTO FACIAL EN LA SEGURIDAD DE LA INFORMACIÓN", modalidad Proyecto de investigación, de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, concedemos a favor de la Universidad Estatal de Bolívar, una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservamos a mi/nuestro favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizo/autorizamos a la Universidad Estatal de Bolívar, para que realice la digitalización y publicación de este trabajo de titulación en el Repositorio Digital, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

El autor declara que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.



Edwin Leonel Belduma Belduma
Firma

ÍNDICE DE CONTENIDO

TEMA DEL PROYECTO DE INVESTIGACIÓN i
AGRADECIMIENTO i
DEDICATORIA ii
INTRODUCCIÓN 1
RESUMEN 2
SUMILLA 3
ABSTRACT 4
CAPÍTULO I 5
1.1. Descripción del problema 5
1.2. Formulación del problema 6
1.3. Preguntas de investigación 6
1.4. Justificación 7
1.5. Objetivos: General Y Específicos 8
1.5.1. Objetivos General 8
1.5.2. Objetivos Específicos 8
1.7. VARIABLES 10
CAPÍTULO II 11
MARCO TEORICO 11
2.1. ANTECEDENTES 11
2.2. Científico 13
Redes Neuronales y su Aplicación en el Reconocimiento Facial 13
Privacidad y Protección de Datos en el Reconocimiento Facial 13
Aplicaciones y Desafíos del Reconocimiento Facial 14
2.3. Conceptual 16
2.4. Legal 18
Legislación Internacional 18
Leyes 18
Leyes 21
Reglamento 22
Decretos 22
Resoluciones 22
CAPÍTULO III 23
METODOLOGÍA 23
3.1. Tipo de investigación 23

3.2. Enfoque de la investigación 24
3.3. Métodos de investigación 24
3.4. Técnicas e instrumentos de recopilación de datos 24
3.5. Universo, Población y Muestra 25
3.6. Procesamiento de la Información 25
CAPÍTULO IV 26
RESULTADOS Y DISCUSIÓN 26
4.1 Análisis e Interpretación 26
Análisis de estudio en Ecuador 26
4.1.1 Categorización de estudios 26
4.1.2. Medidas de protección de datos aplicadas 29
4.1.3. Comparación de precisión entre entornos controladores y espacios públicos 31
4.1.4. Relación entre el enfoque del estudio y medidas propuestas 33
Análisis de estudio en el exterior 35
4.1.1. Categorización de estudios 35
4.1.2. Medidas de protección de datos aplicadas 38
4.1.3. Comparación de precisión entre entornos controladores y espacios públicos 40
4.2. Discusión de Resultados 44
ANALISIS COMPARATIVO 46
ANÁLISIS FODA 53
CAPÍTULO V 54
PROPUESTA 54
Desarrollo de propuesta con el estudios realizado 57
Componentes de la propuesta metodológica 57
Instrumentos de Apoyo 61
Fichas de Instrumento de apoyo 62
Validación práctica de la propuesta 65
RECOMENDACIONES 70
BIBLIOGRAFIA 71
ANEXOS 75

INDICE DE TABLAS

Tabla 1 Áreas de enfoque de los estudios 26
Tabla 2 Medidas de Protección de Datos 28
Tabla 3 Distribución de la precisión en estudios según el tipo de entorno 29
Tabla 4 Distribución de algoritmos utilizados en estudios de reconocimiento facial 31
Tabla 5 Número de estudios por combinación de variables 33
Tabla 6 Matriz de correlación entre variables clave del estudio 33
Tabla 7 Categorización de estudios sobre tecnologías emergentes y protección de datos 36
Tabla 8 Distribución de las Medidas de Protección de Datos Aplicadas según su Tipo 38
Tabla 9 Comparación de la Precisión de Modelos de Reconocimiento Facial en Entornos Controlados y Públicos 40
Tabla 10 Número de estudios por combinación de variables abordadas 42
Tabla 11 Matriz de similitud entre variables 42
Tabla 12 Comparación temática entre estudios de Ecuador y del exterior 45
Tabla 13 Comparación de leyes de protección de datos – Europa Occidental 46
Tabla 14 Comparación de leyes de protección de datos – América (Occidente) 47
Tabla 15 Comparación de leyes de protección de datos – América Latina 48
Tabla 16 Análisis FODA comparativo entre la metodología CLASP y la norma ISO/IEC 23894:2023 aplicada al reconocimiento facial 53
Tabla 17 Matriz de Riesgos Identificados en Estudios de Reconocimiento Facial 59
Tabla 18 Gestión de riesgos en el ciclo de vida de los datos según CLASP 60
Tabla 19 Evaluación Ética y Técnica 63
Tabla 20 Matriz de Cumplimiento 64
Tabla 21 Guía de Intervención ante Incidentes de Seguridad 64
Tabla 22 Modelo de Consentimiento Informado para Entornos Automatizados 65
Tabla 23 Resultados de riesgos técnico-normativos de la práctica experimental 67
Tabla 24 Propuesta para la elaboración del proyecto de titulación 82

INDICE DE FIGURAS

Gráfico 1 Distribución porcentual según enfoque principal 27
Gráfico 2 Medidas de protección de datos propuestas en los estudios..... 28
Gráfico 3 Comparación de precisión entre entornos controlados y espacios públicos..... 30
Gráfico 4 Tipos de algoritmo usados en reconocimiento facial..... 32
Gráfico 5 Correlación entre variables principales..... 34
Gráfico 6 Distribución porcentual de estudios según su categoría temática 36
Gráfico 7 Distribución de estrategias de protección de datos según su tipo de medida..... 38
Gráfico 8 Comparación de la precisión de modelos de reconocimiento facial en entornos controlados y espacios públicos 40
Gráfico 9 Comparación gráfica de similitud entre combinaciones de variables mediante curvas cerradas..... 43
Gráfico 10 Captura experimental en Python durante la práctica de validación 66
Gráfico 12 Reporte de similitud de Turnitin..... 78
Gráfico 13 Cronogramas de Actividades para la elaboración del Proyecto..... 80
Gráfico 14 Análisis de enfoques y medidas de protección en estudios de reconocimiento facial 84
Gráfico 15 Cálculo del índice de Jaccard aplicado a estudios sobre privacidad, precisión y regulación 85
Gráfico 16 Evidencia práctica de detección facial mediante programación 86
Gráfico 17 Evaluación práctica de riesgos técnico-normativos en el procesamiento de imágenes 87

INTRODUCCIÓN

En la era de la inteligencia artificial, los sistemas de reconocimiento facial, alimentados por redes neuronales y algoritmos de aprendizaje profundo, se han integrado ampliamente en los espacios públicos con fines de seguridad.

Esta tecnología permite una identificación muy precisa de los rostros humanos, pero también plantea serias preocupaciones sobre la privacidad, el uso de datos biométricos y los riesgos éticos asociados a la vigilancia masiva. Este estudio responde a la necesidad de analizar el impacto del rápido desarrollo de estas tecnologías en los derechos fundamentales, especialmente en contextos en los que la regulación es escasa o poco clara. El tratamiento de datos sensibles y los posibles sesgos algorítmicos hacen que sea esencial realizar una evaluación crítica y responsable de su aplicación.

Para ello, se adopta una metodología mixta que combina un análisis cualitativo de los principios éticos y los marcos normativos con un enfoque cuantitativo basado en estudios anteriores y datos estadísticos sobre las vulnerabilidades en materia de seguridad informática. La investigación es descriptiva y explicativa, con un diseño transversal no experimental, respaldado por un análisis documental. El objetivo principal es examinar el impacto de las redes neuronales en la privacidad dentro de los sistemas de reconocimiento facial en espacios públicos, identificando los retos técnicos y éticos más relevantes y proponiendo un marco de implementación responsable.

Se abordan los principales riesgos, se analizan las mejores prácticas en materia de ciberseguridad, como la metodología CLASP, y se proponen directrices para reducir los riesgos sin afectar a la funcionalidad del sistema.

El documento se organiza en cuatro capítulos: exposición y justificación del problema; marco teórico sobre redes neuronales, privacidad y regulación; metodología utilizada; y, por último, resultados, conclusiones y recomendaciones. Este trabajo tiene por objeto contribuir a la formulación de políticas y estrategias que permitan aprovechar las ventajas de estas tecnologías sin comprometer los derechos fundamentales de las personas. En un contexto en el que la tecnología avanza más rápido que la legislación, este análisis invita a la reflexión y a la acción responsable.

RESUMEN

Este estudio tuvo como objetivo analizar el impacto de las redes neuronales aplicadas al reconocimiento facial en espacios públicos, identificando los principales desafíos éticos, técnicos y regulatorios asociados con su implementación. Se aplicó una metodología mixta, combinando análisis cualitativos y cuantitativos en 100 estudios científicos (50 ecuatorianos y 50 internacionales), apoyados en técnicas estadísticas, matrices de riesgo, categorización de variables y herramientas gráficas.

Los resultados revelaron que la privacidad es la prioridad predominante en Ecuador (50%), mientras que la evaluación técnica es la prioridad a nivel internacional (44%). Las medidas más aplicadas fueron el cifrado (36%) y la combinación (20%). Se observó una mayor precisión de los sistemas en entornos controlados (90-100%) en comparación con los espacios públicos (75-90%).

Las redes neuronales convolucionales (CNN) fueron las más utilizadas (60%). Los hallazgos resaltan la poca integración entre precisión y regulación, la limitada aplicación de medidas de seguridad en estudios locales y la urgente necesidad de fortalecer la implementación de la LOPDP en Ecuador.

Se desarrolló una metodología basada en el enfoque CLASP y la norma ISO/IEC 23894:2023, acompañada de herramientas como hojas de evaluación, matrices normativas y plantillas de consentimiento. La conclusión es que es posible implementar tecnologías avanzadas respetando la privacidad, siempre que se integren principios éticos, técnicos y regulatorios desde la fase de diseño.

Palabras clave: Reconocimiento facial, redes neuronales, protección de datos personales, CLASP, ISO/IEC 23894:2023

SUMILLA

Kay yachay rimarin, ñawpa rikcharishka yachaykuna shina, riksichina imashina redes neuronales llamkashka riksishka ujllaykuna runakunapa uyay rikuna shimikunapi. Ñukanchik rimarirkani ima wakin ama shina alli kawsayta chinkachishka, mana allilla llankayta, ima llapa kamachiykuna riksina yuyaykunata ima chay tecnología llama kanaykuna.

Chay yachayta rurashka, ishkay yachaykunata tinkurirkani: shinallatak ima rurana ñawpakuna shutillatak tinkurishka 100 yachay (50 Ecuadorpi, 50 shuk llauta llaktakunapi), yachay ruraykuna rurashka rimaypi, shuyaypi, allikuykuna chaskiykipi, watakuykuna ruraykuna, ñawpa yuyaykuna.

Shina rikurirkani Ecuadorpi shuk ñawpa yuyay "privacy" ñawpakunata (50%) rurashka; shinallatak shuk llauta llaktakunapi alli llankay yuyaymi ñawpakuna (44%). Alli ruraykunata ima nishkakunata: cifrado (36%) y tukuykunata tinkurishka (20%). Alli rikchaykuna ñawpakunapi llankaymi alli kan (90% - 100%), shinallatak llakta wasi shina rikchaykuna mana shina alli (75% - 90%).

CNN (Convolutional Neural Networks) alli ushaykuna (60%) riksishka. Ñukanchik rikurirkani mana tinkuriy chakrata, mana chaskiy, mana alli kamachikuyta. Ecuadorpi ñawpakuna riksina LOPDP mana sinchi.

Ñukanchik rurarkani shuk ñawpak yachay: CLASP yachaykuna chaskiykuna, ISO/IEC 23894:2023 yuyay ruraykuna. Chaywan tinkurirkani yachaykunata: ñawpak riksichiykuna, kamachiykuna ñawpakunata watakuy, chaskikuy, riksiy, consentimiento ñawpakunata ima yachaykunawan.

Rimariy ñawpakunapi: Alli tecnología ruranakuy kashkanmi, shinallatak ñukanchikta yachaypika allikuykuna, sumak kawsaykuna, kamachiykuna yuyaywan tinkurishpa rurashka chaymanta riksiykuna.

Shimikuna ñawpakunapi: Uyay rikuna, redes neuronales, datos personalespak allikuy, CLASP, ISO/IEC 23894:2023

ABSTRACT

This study aimed to analyze the impact of neural networks applied to facial recognition in public spaces, identifying the main ethical, technical, and regulatory challenges associated with their implementation. A mixed methodology was applied, combining qualitative and quantitative analyses in 100 scientific studies (50 Ecuadorian and 50 international), supported by statistical techniques, risk matrices, variable categorization, and graphical tools.

The results revealed that privacy is the predominant priority in Ecuador (50%), while technical evaluation is the priority internationally (44%). The most frequently applied measures were encryption (36%) and combination (20%). Greater system accuracy was observed in controlled environments (90-100%) compared to public spaces (75-90%).

Convolutional neural networks (CNNs) were the most frequently used (60%). The findings highlight the poor integration between accuracy and regulation, the limited application of security measures in local studies, and the urgent need to strengthen the implementation of the LOPDP (License for Personal Data Protection) in Ecuador.

A methodology based on the CLASP approach and the ISO/IEC 23894:2023 standard was developed, accompanied by tools such as assessment sheets, normative matrices, and consent templates. The conclusion is that it is possible to implement advanced technologies while respecting privacy, provided that ethical, technical, and regulatory principles are integrated from the design phase.

Keywords: Facial recognition, neural networks, personal data protection, CLASP, ISO/IEC 23894:2023

CAPÍTULO I

FORMULACIÓN GENERAL DEL PROYECTO

1.1. Descripción del problema

Los avances en inteligencia artificial han permitido la implementación de redes neuronales en los sistemas de reconocimiento facial en espacios públicos, lo que ha tenido un impacto significativo en la seguridad, la privacidad y la protección de los datos personales.

Las redes neuronales convolucionales se han convertido en herramientas esenciales para resolver problemas de seguridad en contextos controlados. Peñaherrera Plúa y Triviño Quiñonez (2024) explican que estas redes neuronales se distinguen por su capacidad para aprender patrones y características relevantes en grandes volúmenes de datos, lo que las convierte en una herramienta eficaz para abordar retos de seguridad, como la identificación de personas autorizadas y no autorizadas en entornos controlados.

Varios estudios destacan la importancia de aplicar los principios de seguridad informática en el diseño y desarrollo de estos sistemas.Gómez Cruz y Jiménez Valero (2020) explican que el reconocimiento facial destinado a la producción en un entorno IoT debe tener en cuenta la fase de análisis, ya que los requisitos deben evaluarse cuidadosamente para garantizar que se ajustan tanto a los objetivos del proyecto como a la realidad del desarrollo de software.

Sin embargo, el uso de esta tecnología plantea retos éticos y técnicos que deben abordarse con rigor para evitar la vigilancia masiva y el uso indebido de la información recopilada, lo que podría vulnerar los derechos fundamentales de las personas.

Además, el uso no regulado de esta tecnología podría crear un conflicto entre la seguridad de los ciudadanos y el derecho a la privacidad. Peñaherrera Plúa y Triviño Quiñonez (2024) las redes neuronales pueden entrenarse para reconocer los rasgos faciales de las personas autorizadas, impidiendo así cualquier acceso no autorizado a través de una cámara y un microcontrolador encargado del procesamiento.

Esta tecnología puede integrarse en los sistemas de seguridad automatizados y debe tener en cuenta el tratamiento ético de los datos, la reducción de sesgos y el respeto de los derechos fundamentales.

Desde un punto de vista científico y tecnológico, es necesario analizar el impacto de las redes neuronales en la privacidad y los mecanismos que pueden implementarse para mitigar los riesgos sin comprometer su funcionalidad. Este desafío justifica la relevancia de este estudio, cuyo objetivo es establecer un equilibrio entre el desarrollo tecnológico y la protección de los derechos fundamentales en el uso de los sistemas de reconocimiento facial.

1.2. Formulación del problema

¿Cómo pueden las redes neuronales en sistemas de reconocimiento facial implementarse en espacios públicos de manera responsable, garantizando la protección de datos y la seguridad ciudadana, a través de la identificación de retos éticos y técnicos, la aplicación de buenas prácticas de seguridad informática y la metodología CLASP?

1.3. Preguntas de investigación

- ¿Cuáles son los principales retos éticos, técnicos y de seguridad informática en el uso de redes neuronales en sistemas de reconocimiento facial en espacios públicos?
- ¿Cómo afecta la implementación de sistemas de reconocimiento facial a la privacidad y protección de datos personales, y qué estrategias pueden mitigar estos riesgos?
- ¿De qué manera puede lograrse un equilibrio entre la seguridad ciudadana y el respeto a los derechos fundamentales en la implementación de sistemas de reconocimiento facial?

1.4. Justificación

El reconocimiento facial basado en redes neuronales presenta sesgos importantes a la hora de identificar a determinados grupos demográficos, debido a bases de datos desequilibradas en términos de género y origen étnico. Aunque se han desarrollado modelos para mitigar este problema, persisten las desigualdades en términos de precisión del reconocimiento, lo que pone de relieve la necesidad de proponer soluciones que mejoren la equidad algorítmica mediante la biometría suave y estrategias de aprendizaje equilibradas, que benefician directamente a la sociedad en su conjunto, como demuestran diversos estudios sobre los sesgos y sus implicaciones técnicas y sociales (Simón Chico, 2021).

Esta investigación es necesaria porque la falta de medidas de ciberseguridad adecuadas y de metodologías de desarrollo responsables podría comprometer la integridad de los datos personales.

En este sentido, Gutiérrez (2021) señala que la metodología CLASP ofrece un enfoque estructurado, basado en la experiencia práctica, para integrar medidas de seguridad que permiten identificar vulnerabilidades, lo que beneficia directamente a los equipos de desarrollo y a las organizaciones usuarias, y beneficia indirectamente a los usuarios finales al reforzar la protección de los sistemas contra los riesgos cibernéticos.

Este estudio es relevante porque tiene como objetivo elaborar un marco para la implementación responsable de los sistemas de reconocimiento facial, garantizando un equilibrio entre la seguridad y la privacidad. Contribuirá a la elaboración de directrices técnicas y éticas que orientarán a las instituciones públicas y privadas en el desarrollo y el uso de esta tecnología, previniendo los abusos y garantizando la transparencia de su funcionamiento.

Los beneficiarios directos de esta investigación son los desarrolladores de software, las entidades gubernamentales y las organizaciones que utilizan sistemas de reconocimiento facial. Indirectamente, la sociedad en su conjunto se beneficiará de mecanismos reforzados de protección de datos y de mejores garantías de respeto de los derechos fundamentales.

En el ámbito académico y científico, este estudio contribuye a la investigación en materia de ciberseguridad, inteligencia artificial y ética de las tecnologías, proporcionando una base para futuras investigaciones y la elaboración de normativas que regulen el uso de redes neuronales en el ámbito del reconocimiento facial.

También se inscribe en la línea de las experiencias de otros países, donde la implementación incontrolada de esta tecnología ha suscitado debates y regulaciones específicas destinadas a mitigar sus riesgos. En definitiva, esta investigación representa un paso crucial para garantizar que la inteligencia artificial y el reconocimiento facial se utilicen de forma equitativa, transparente y segura, favoreciendo así el desarrollo tecnológico sin comprometer la privacidad ni los derechos fundamentales de las personas.

1.5. Objetivos: General Y Específicos

1.5.1. Objetivos General:

Analizar el impacto de las redes neuronales en el reconocimiento facial en espacios públicos, identificando los principales retos éticos y técnicos asociados a su implementación.

1.5.2. Objetivos Específicos

- Identificar y categorizar los retos éticos y técnicos asociados al uso de redes neuronales en sistemas de reconocimiento facial en espacios públicos.
- Evaluar la aplicación de buenas prácticas de seguridad informática y la metodología CLASP en el diseño de sistemas de reconocimiento facial basados en redes neuronales.
- Proponer un marco de diseño responsable para sistemas de reconocimiento facial

1.6. Hipótesis

La implementación de redes neuronales en los sistemas de reconocimiento facial en espacios públicos tiene un impacto significativo en la privacidad y la protección de los datos personales, y este impacto puede mitigarse aplicando las mejores prácticas y metodologías de ciberseguridad, como CLASP, que garantizan un equilibrio entre la seguridad de los ciudadanos y el respeto de los derechos fundamentales.

1.7. VARIABLES

Variable	Definición	Dimensión	Indicadores	Técnicas
Redes neuronales	Son modelos computacionales inspirados en el funcionamiento del cerebro humano.	Aplicaciones en IA	• Uso en reconocimiento de patrones. • Aplicaciones en visión artificial y procesamiento de lenguaje natural.	Revisión documental, análisis de casos de uso.
		Precisión y rendimiento	• Tasa de aciertos en clasificación de datos. • Comparación con otros modelos de aprendizaje automático.	Evaluación de reportes de precisión en modelos de IA.
Privacidad de los datos	Es el derecho y la capacidad de controlar cómo se recopilan, almacenan, procesan y comparten los datos personales	Protección de datos personales	• Existencia de normativas de privacidad. • Medidas de seguridad en bases de datos biométricas.	Revisión documental, análisis de contenido.
		Normativa	• Políticas de acceso. • Legislación regional y local • cumplimiento de normativas	
Reconocimiento facial	Es una tecnología de inteligencia artificial que identifica o verifica la identidad de una persona mediante el análisis de sus rasgos faciales a partir de imágenes o videos.	Uso y seguridad de la tecnología	• Tasa de error en identificación. • Riesgos de hackeos y suplantaciones.	Evaluación de informes de ciberseguridad, revisión de legislaciones.
		Regulación y normativas	• Legislación vigente sobre el uso del reconocimiento facial en espacios públicos y privados. • Normativas sobre almacenamiento y uso de datos biométricos.	Revisión de marcos legales nacionales e internacionales.

CAPÍTULO II

MARCO TEORICO

2.1. ANTECEDENTES

Gárate Briones (2020) en su tesis, defendida en la Escuela Superior Politécnica del Litoral, diseñó un sistema de reconocimiento facial en línea para el control de acceso utilizando inteligencia artificial. Se utilizaron redes neuronales y herramientas como Tensor Flow y OpenCV para identificar rostros en tiempo real. Se obtuvo una gran precisión en condiciones controladas, lo que demostró la eficacia de estos sistemas en entornos seguros. Sin embargo, se identificaron limitaciones debido a bases de datos desequilibradas, lo que generó sesgos de reconocimiento. Esto demuestra a escala internacional la necesidad de integrar la diversidad de datos para mejorar la equidad algorítmica de los sistemas de reconocimiento facial. (Gárate Briones, 2020).

En la ciudad de Guayaquil, el proyecto desarrollado en la Universidad Politécnica Salesiana respondía a la necesidad de mejorar la seguridad institucional mediante el reconocimiento facial. Se diseñó un sistema basado en redes neuronales convolucionales para controlar el acceso a las zonas restringidas. El modelo se entrenó con imágenes reales de profesores y obtuvo buenos resultados. Esta propuesta demuestra que es posible aplicar la inteligencia artificial en contextos educativos locales con recursos accesibles. (Peñaherrera Plúa & Triviño Quiñonez, 2024).

El reconocimiento facial se utiliza ampliamente en todo el mundo en sectores como los aeropuertos, la seguridad ciudadana y el transporte público. En países como China, esta tecnología se utiliza en estaciones de tren y sistemas de videovigilancia para identificar a delincuentes mediante sensores faciales conectados a bases de datos gubernamentales. En Europa, Londres y Madrid han implementado el reconocimiento facial en espacios públicos y transportes, con resultados positivos en términos de reducción de la delincuencia y optimización de los servicios. Del mismo modo, el aeropuerto de Canberra, en Australia, ha sustituido el pasaporte físico por una identificación biométrica. Estos avances demuestran el alcance global del reconocimiento facial y su integración en los sistemas IoT en diferentes contextos. (Gómez Cruz & Jiménez Valero, 2020).

Análisis a Nivel Local - Cantón Guaranda

No se ha identificado ningún estudio específico sobre el impacto de las redes neuronales en la confidencialidad y la protección de datos en los sistemas de reconocimiento facial en el cantón de Guaranda. Sin embargo, la implementación de esta tecnología podría representar un avance significativo en la seguridad y la digitalización de los procesos administrativos y comerciales en la región.

Guaranda, capital de la provincia de Bolívar, cuenta con instituciones públicas y privadas que podrían beneficiarse de la automatización de los controles de acceso y la protección de datos mediante el reconocimiento facial.

El uso de sistemas de reconocimiento facial en entidades gubernamentales, empresas y centros educativos del cantón mejoraría la seguridad del acceso a las instalaciones, optimizaría la gestión de la información sensible y garantizaría la confidencialidad de los ciudadanos. Teniendo en cuenta la transformación digital emergente en la región, la adopción de estas tecnologías podría contribuir a modernizar la administración pública y reforzar la protección de datos personales en el contexto local.

2.2. Científico

La investigación se basa en teorías establecidas del procesamiento de señales y el aprendizaje automático, utilizando técnicas como el transformado coseno discreta (DCT), la transformada wavelet discreta (DWT), el análisis de componentes principales (ACP) y el análisis de componentes independientes (ACI). Estas herramientas permiten reducir la dimensión del vector de características de las imágenes faciales, conservando al mismo tiempo su poder discriminatorio. El estudio se basa en el uso de clasificadores como las máquinas de vectores de soporte (SVM) y las redes neuronales, en un marco científico destinado a optimizar el rendimiento y la eficacia de los sistemas de reconocimiento facial (Travieso et al., 2008).

Redes Neuronales y su Aplicación en el Reconocimiento Facial

Las redes neuronales convolucionales (CNN) han revolucionado el procesamiento de imágenes al imitar la capacidad del cerebro humano para reconocer patrones visuales. Este modelo se basa en capas de procesamiento que detectan características específicas en una imagen, lo que permite una identificación facial extremadamente precisa. Según Peñaherrera Plúa y Triviño Quiñonez (2024) la implementación de CNN en los sistemas de seguridad mejora la eficacia de la detección de personas autorizadas y no autorizadas.

Uno de los principales enfoques del reconocimiento facial mediante redes neuronales es Eigenface, desarrollado por Sirovich y Kirby, cuyo objetivo es representar los rostros en un espacio de menor dimensión. Esta técnica se ha mejorado mediante el uso de métodos como la transformada de Fisher y las redes neuronales siamesas, que optimizan la correspondencia de las imágenes faciales.

Privacidad y Protección de Datos en el Reconocimiento Facial

La implementación del reconocimiento facial ha suscitado debates sobre la confidencialidad y el tratamiento de los datos biométricos. Según Gárate Briones, (2020) el 90% los encuestados considera que el reconocimiento facial tiene un impacto en la privacidad, lo que pone de relieve la necesidad de una regulación estricta de su uso.

A nivel internacional, organizaciones como el Instituto Nacional de Estándares y Tecnología (NIST) han establecido directrices para evaluar la precisión y la seguridad de los sistemas de reconocimiento facial, garantizando que cumplan con las normativas en materia de confidencialidad y protección de datos.

Aplicaciones y Desafíos del Reconocimiento Facial

El reconocimiento facial se utiliza en muchos sectores, desde el control de acceso a instituciones hasta los sistemas de identificación y vigilancia de aeropuertos. Sin embargo, su implementación se enfrenta a retos como los sesgos algorítmicos, que pueden afectar a la precisión en determinadas poblaciones, y el riesgo de ataques de phishing.

La mejora continua de estas tecnologías requiere la implementación de enfoques híbridos que combinen redes neuronales y técnicas de criptografía para garantizar la seguridad de los datos biométricos.

Técnicas de Vivacidad como Componente Científico en la Verificación Biométrica

La base científica de esta investigación se complementa con el estudio de las técnicas de vivacidad, que permiten verificar si el rostro presentado al sistema de reconocimiento facial proviene de una persona real o de una representación artificial (como una fotografía o un vídeo). Estas técnicas, como el parpadeo y la orientación de la mirada, se basan en la detección de puntos clave del rostro mediante modelos de redes neuronales convolucionales como MediaPipe.

De acuerdo con Rodriguez Ponce et al. (2024), estas estrategias refuerzan el proceso de autenticación biométrica al integrarlo como segundo factor de seguridad, lo que reduce la posibilidad de robo de identidad y ofrece un enfoque sólido y reproducible del procesamiento visual en tiempo real.

Aprendizaje profundo y el procesamiento de datos no estructurados

Se basa en el aprendizaje profundo, un subcampo del aprendizaje automático que permite a los sistemas de inteligencia artificial resolver problemas complejos utilizando datos no estructurados, como imágenes, voz o vídeos, elementos esenciales para el reconocimiento facial.

Según Rouhiainen (2018), el aprendizaje profundo permite a los algoritmos identificar patrones visuales complejos, optimizando así la precisión de tareas como la detección de gestos y la verificación biométrica. Combinado con amplios conjuntos de datos y capacidades computacionales avanzadas, este enfoque refuerza las bases científicas para el desarrollo de sistemas biométricos fiables, adaptables y escalables en contextos de alta seguridad.

Detección facial en tiempo real mediante OpenCv y Clasificadores Haar

Un elemento científico esencial para el desarrollo de los sistemas de reconocimiento facial es el uso de bibliotecas especializadas como OpenCv, que permiten la captura, segmentación y análisis faciales en tiempo real. Los clasificadores Haar Cascade, en particular, ofrecen una técnica eficaz para detectar rostros a partir de imágenes o vídeos animados.

Este enfoque se basa en modelos reentrenados que identifican las estructuras faciales clave, como los ojos, la nariz y la boca. Según Pérez Lorenzo (2023) se utilizó esta metodología se ha utilizado para desarrollar un sistema de control de acceso, demostrando su eficacia en entornos con baja latencia y sujetos a limitaciones de hardware. Este trabajo refuerza la facilidad de uso y la seguridad del reconocimiento facial, permitiendo una identificación rápida gracias a recursos informáticos accesibles.

Validación de identidad mediante documentos y visión artificial

El reconocimiento facial mejora cuando se integra en los mecanismos de validación de documentos, añadiendo una segunda capa de autenticación. En la propuesta de Molina (2022) se emplean modelos como VGG y Caffe, así como bibliotecas como OpenCV, permiten comparar el rostro capturado por la cámara con la fotografía que figura en el documento de identidad del usuario. Esta técnica garantiza un alto nivel de seguridad y cumple con los requisitos normativos y políticos en materia de confidencialidad de los datos. Desde un punto de vista científico, representa una fusión entre la visión por ordenador y los mecanismos jurídicos de verificación de identidad.

Prevención de suplantación facial mediante estrategias Antispoofing

El auge de los ataques de suplantación de identidad facial ha llevado al desarrollo de modelos anti suplantación diseñados para detectar intentos de fraude mediante el análisis de micro expresiones, profundidad y comportamiento dinámico del rostro. Estos modelos, entrenados con grandes volúmenes de datos, distinguen un rostro real de una representación fraudulenta mediante un análisis temporal y textural. Este enfoque mejora la precisión y el rendimiento de la variable de la red neuronal, así como la protección de los datos personales, minimizando los accesos no autorizados y los falsos positivos en los sistemas biométricos (Martínez Guerrero, 2018).

2.3. Conceptual

Aprendizaje profundo: "Es un subconjunto de la inteligencia artificial que imita las redes neuronales del cerebro para aprender de grandes volúmenes de datos, lo que permite a las maquinas resolver problemas complejos" (O que é deep learning?, 2024).

Ataques de suplantación: Se trata de una técnica utilizada por los ciberdelincuentes para acceder sin autorización a sistemas informáticos haciéndose pasar por usuarios legítimos. Este tipo de ataque consiste en manipular datos, comunicaciones de red u otros elementos digitales creando identidades falsas, ocultando así el verdadero origen del ataque («What Is a Spoofing Attack?», s. f.).

Autenticación biométrica: Se trata de un mecanismo de seguridad que utiliza las características físicas o conductuales únicas de una persona para verificar su identidad. Consiste en generar un modelo basado en los datos biométricos del individuo, lo que permite a los sistemas de seguridad autenticar el acceso a las aplicaciones y los recursos digitales. (¿Qué es la autenticación biométrica?, s. f.).

CLASP: Se trata de un modelo desarrollado por OWASP que establece las mejores prácticas de seguridad basadas en funciones y actividades, con el objetivo de integrar la seguridad en todo el ciclo de vida del desarrollo de software de forma estructurada, medible y reproducible (Santos Chavez, 2024).

Datos biométricos: “Son los datos personales relativos a las características única del ser humano, sean físicas, fisiológicas o asociadas al comportamiento, que faciliten y garanticen la identificación de un individuo (persona física), mediante sistemas o procedimiento tecnológicos” (Monforte, 2022).

Equidad algorítmica: “Se refiere a la imparcialidad y la falta de sesgo en los algoritmos que rigen los procesos de toma de decisiones, particularmente en áreas como la contratación, el otorgamiento de préstamos y la aplicación de la ley”(¿Qué es la Equidad Algorítmica? - Términos y Definiciones de Ciberseguridad, s. f).

Inteligencia artificial: “Es una tecnología que permite ordenadores y máquinas simular las capacidades humanas de aprendizaje, como comprensión y soluciones de problemas, toma de decisiones, creatividad y autonomía” (Stryker & Kavlakoglu, 2024).

ISO/IEC 23894:2023: Es un estándar internacional que proporciona pautas para la gestión de riesgos en sistemas de inteligencia artificial, ayudando a las organizaciones a integrar procesos efectivos para identificar, evaluar y abordar los riesgos relacionados con la IA (ISO, 2023).

Protección de datos personales: “Se refiere a los derechos de las personas cuyos datos se recogen, se mantienen y se procesan, de saber que datos están siendo retenidos y usados y de corregir las inexactitudes” (Vilches, 2024).

Redes neuronales convolucionales: Se trata de un tipo de red neuronal profunda especializada en el procesamiento de datos mallados, como las imágenes. Utilizan capas convolucionales para identificar automáticamente patrones y características en las imágenes, lo que facilita tareas como la clasificación y el reconocimiento de objetos *(*¿Qué son las redes neuronales convolucionales?, 2021).

Reconocimiento facial: “Es una forma de identificar o confirmar la identidad de una persona mediante de una imagen de su rostro. Los sistemas de reconocimiento facial se pueden utilizar para identificar a las personas en tiempo real o para identificar a las personas en foto o vídeos” (¿Qué es el reconocimiento facial?, s. f.)**.**

Seguridad biométrica: Se trata de un sistema de autenticación que utiliza las características físicas o conductuales únicas de una persona para conceder acceso, sustituyendo o complementando los métodos tradicionales, como las contraseñas o los códigos PIN (Biometric Security, 2019).

Sesgo algorítmico: Se trata de un error sistemático en los resultados generados por un algoritmo, que favorece o perjudica injustamente a determinados grupos de personas. Este sesgo es consecuencia de datos de entrenamiento de mala calidad y de los prejuicios de quienes diseñan, recopilan los datos y entrenan los algoritmos (Verma, 2024).

Vigilancia biométrica: "Es una tecnología que facilita la identificación de un individuo a partir de sus características físicas, bilógicas y/o comportamiento. Dado que estos datos son únicos y permanentes, no pueden falsificarse" (El equipo de Veesion, 2023).

Vivacidad facial: "Garantiza que los estafadores no puedan utilizar impresiones o fotos de alta resolución, mascaras o videos para falsificar los sistemas de reconocimiento fácil utilizados para la autenticación y verificación de identidad" («Facial Liveness Detection Whitepaper Spanish», s. f.).

2.4. Legal

Legislación Internacional

Leyes

Reglamento general de protección de datos (RGPD): Se trata de la norma jurídica de la Unión Europea del 27 de abril de 2016 que regula la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y la libre circulación de los mismos, y tiene por objeto establecer un marco jurídico uniforme, coherente y reforzado que garantice los derechos fundamentales de los ciudadanos, permitiéndoles controlar sus datos personales (Diario Oficial de la Unión Europea, 2016).

Ley Estadounidense de Privacidad y Protección de Datos (ADPPA) es una propuesta federal que busca unificar las leyes de privacidad en Estados Unidos. Establece requisitos como el consentimiento informado, las evaluaciones de impacto, la notificación de infracciones con 72 horas de anticipación y el derecho de los ciudadanos a acceder, corregir o eliminar sus datos. Si bien aún no se ha aprobado, representa un paso

significativo hacia un marco legal integral para la protección de datos.(«Conoce la Ley Estadounidense de Privacidad y Protección de Datos», s. f.)

Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), que regula el tratamiento legítimo, informado y controlado de datos personales para garantizar la confidencialidad y el derecho a la autodeterminación informativa. Esta ley reconoce los derechos ARCO (acceso, rectificación, cancelación y oposición), exige el consentimiento del titular de los datos para el tratamiento de sus datos (artículo 8) y establece la obligación de publicar una declaración de privacidad (artículo 16). Asimismo, prevé sanciones administrativas y penales en caso de incumplimiento (artículo 63) y designa al INAI como la autoridad responsable de su vigilancia y cumplimiento (ASAMBLEA LEGISLATIVA DEL DISTRITO FEDERAL, 2021).

La Ley de Protección de la Información Personal y de los Documentos Electrónicos de Canadá (PIPEDA), vigente desde el año 2000, rige el procesamiento de datos personales en el sector privado y se basa en diez principios clave, entre ellos el consentimiento, las restricciones de uso y la transparencia. Su aplicación es relevante para esta investigación, ya que establece obligaciones claras para el procesamiento ético y seguro de datos, en particular en contextos tecnológicos como el reconocimiento facial («PIPEDA», s. f.).

Ley de Protección de Datos de Francia, Aprobada en 1978 y actualizada para alinearse con el RGPD, esta ley protege los datos personales de los ciudadanos franceses. Establece principios como la legalidad, la minimización de datos y la rendición de cuentas, exigiendo el consentimiento explícito y medidas de seguridad. Su aplicación está supervisada por la CNIL (Comisión Nacional para la Protección de Datos Personales), que puede imponer sanciones severas. Esta ley es relevante para la investigación debido a su enfoque en el control del procesamiento de datos en sistemas automatizados como el reconocimiento facial («Ley de Protección de Datos de Francia», s. f.).

Ley Federal de Protección de Datos de Alemania (Bundesdatenschutzgesetz – BDSG), Alemania ha armonizado su legislación con el Reglamento General de Protección de Datos (RGPD) mediante la Ley Federal de Protección de Datos (BDSG), que entró en vigor el 25 de mayo de 2018. Esta ley se basa en las cláusulas de apertura del RGPD para adaptar ciertos requisitos a nivel nacional, especialmente en sectores

como las telecomunicaciones, la energía y las finanzas (*Leyes de protección de datos en Alemania - Leyes de protección de datos del mundo*, 2018)

Código de Privacidad Italiano (Decreto Legislativo 196/2003, modificado por el Decreto Legislativo 101/2018), Italia adaptó su legislación al RGPD mediante el Decreto Legislativo 101/2018, que modificó el anterior Código de Privacidad (Decreto Legislativo 196/2003). Este marco regula el tratamiento de datos personales en los sectores público y privado, garantizando derechos como el consentimiento, el acceso, la rectificación y la supresión. La autoridad de control es responsable de la protección de datos personales. Esta ley es esencial para esta investigación debido a su enfoque en el cumplimiento normativo y la protección de datos en entornos digitales complejos, como el reconocimiento facial (Leyes de protección de datos en Italia - Leyes de protección de datos del mundo, 2018).

Ley General de Protección de Datos de Brasil (LGPD – Ley n.º 13.709/2018) En vigor desde septiembre de 2020, la LGPD es la primera normativa integral de protección de datos en Brasil y comparte similitudes con el RGPD europeo. Se aplica a todo tratamiento de datos personales realizado en Brasil o relativo a personas físicas dentro de su territorio, independientemente de la ubicación del responsable. Reconocida como un derecho fundamental desde 2022, esta ley garantiza principios como el consentimiento, la transparencia y la seguridad, bajo la supervisión de la Autoridad Nacional de Protección de Datos (ANPD). Su enfoque es esencial en esta investigación debido a su alcance extraterritorial y su aplicación a entornos digitales (Leyes de protección de datos en Brasil - Leyes de protección de datos del mundo, 2020).

Ley Orgánica 1581 de 2012 – Colombia La Ley 1581 de 2012 establece el régimen general de protección de datos personales en Colombia. Reconoce el derecho de toda persona a conocer, actualizar y rectificar su información recopilada en bases de datos, y regula su tratamiento por entidades públicas y privadas. La ley establece principios como la licitud, la finalidad, la libertad, la seguridad y la confidencialidad, e impone obligaciones a los responsables del tratamiento de datos. Su aplicación está supervisada por la Superintendencia de Industria y Comercio. Esta ley es relevante para esta investigación debido a su clara regulación del uso de datos sensibles y biométricos, esenciales para los sistemas de reconocimiento facial (Gestor Normativo, 2012).

Reglamento de la Ley N.° 29733 – Perú (Decreto Supremo N.° 016-2024-JUS) El nuevo reglamento de la Ley de Protección de Datos Personales del Perú, publicado en noviembre de 2024, fortalece los estándares de protección al armonizarlos con las normas internacionales. Introduce obligaciones como el nombramiento progresivo de un Delegado de Datos Personales (DDP), el reconocimiento del derecho a la portabilidad de datos, la evaluación del impacto del tratamiento sensible y la notificación de incidentes con 48 horas de antelación. También establece criterios para las transferencias internacionales, medidas específicas para la protección de menores y actualiza los requisitos de seguridad de acuerdo con las normas ISO. Este reglamento es relevante para la investigación debido a su enfoque actualizado y preventivo en contextos automatizados como el reconocimiento facial(Gallo & Egas, 2024).

Legislación Nacional (Ecuador)

Leyes

Ley de comercio electrónico, firmas electrónicas y mensaje de datos: Establece las responsabilidades de los proveedores y los usuarios, exige mecanismos de seguridad para proteger la información sensible y prohíbe el envío de mensajes electrónicos no solicitados sin consentimiento (Ley de comercio electrónico, firmas electrónicas y mensajes de datos, s. f.).

Ley Orgánica de Protección de Datos Personales del Ecuador: Su objetivo es garantizar el ejercicio del derecho a la protección de los datos personales de forma libre, informada y segura. Esta ley protege la recopilación, el almacenamiento, el uso, la circulación y la eliminación de datos personales, tanto en soportes físicos como digitales, estableciendo principios como el consentimiento, la finalidad, la proporcionalidad y la confidencialidad (Asamblea Nacional, 2021).

Reglamento

Código orgánico económico social de los conocimientos: Regula la producción, la gestión, el acceso y el uso del conocimiento, la creatividad y la innovación en el país, estableciendo disposiciones sobre propiedad intelectual, ciencia, tecnología, conocimientos ancestrales, educación superior e investigación. Esta normativa promueve un modelo de economía social del conocimiento, centrado en un desarrollo inclusivo, sostenible y soberano (Reglamento codigo organico economia docial de los conocimiento, 2017).

Decretos

Reglamento de la ley Orgánica de protección de datos personales: Decreto N° 904 detalla las disposiciones clave de su aplicación, entre los aspectos más relevantes se encuentran el tratamiento a gran escala de los datos personales, los criterios de tratamiento legítimo, el contenido mínimo que deben tener las notificaciones de fallos de seguridad y la obligación de nombrar a un delegado de protección de datos (BPONE, 2023).

Resoluciones

Protección de datos personales: Resolución N.º SPDP-SPD-2025-0002-R tiene como su objetivo es establecer las normas técnicas y jurídicas necesarias para garantizar una aplicación eficaz. Su finalidad es garantizar la seguridad jurídica, uniformizar los procedimientos y armonizar el marco normativo nacional con las normas internacionales en materia de protección de datos (Peralta-Díaz, 2025).

CAPÍTULO III

METODOLOGÍA

3.1. Tipo de investigación

En términos de profundidad, esta investigación es tanto descriptiva como explicativa. Descriptiva porque documenta los retos técnicos y éticos de estas tecnologías, ofreciendo una visión detallada de sus implicaciones para la confidencialidad y la seguridad de los datos. Explicativa porque analiza las relaciones de causa y efecto entre la implementación de sistemas de reconocimiento facial y las vulnerabilidades en materia de seguridad de los datos.

De acuerdo con Hernández Sampieri y Fernández Collado (2014), la investigación explicativa busca establecer relaciones entre variables y comprender fenómenos complejos mediante la identificación de factores determinantes.

En cuanto a la metodología de recopilación de datos, el estudio adopta un enfoque mixto, combinando datos cualitativos, como el análisis de normativas y principios éticos, con datos cuantitativos procedentes de estudios anteriores sobre los impactos en materia de seguridad. La combinación de estos enfoques permite un análisis más completo del fenómeno estudiado (Hernández Sampieri & Fernández Collado, 2014).

Se trata de un estudio no experimental, ya que no se manipula ninguna variable, sino que se analizan los datos existentes. Para la inferencia se utiliza un enfoque inductivo y deductivo: el análisis de casos particulares permitirá formular conclusiones generales, y los principios teóricos se confrontarán con los datos empíricos, según la metodología propuesta por Hernández Sampieri y Fernández Collado (2014).

Por último, el estudio es transversal, ya que los datos se analizarán en un momento concreto sin seguimiento a lo largo del tiempo, lo que permite obtener una “instantánea” del estado actual de la problemática objeto de investigación (Hernández Sampieri & Fernández Collado, 2014).

3.2. Enfoque de la investigación

Según un enfoque mixto, se utilizarán los siguientes métodos:

- Cualitativos, para el análisis de normas, reglamentos y estudios de casos sobre redes neuronales en el reconocimiento facial.
- Cuantitativos, para evaluar el impacto y las vulnerabilidades de seguridad mediante datos estadísticos y estudios específicos.

El análisis combinará métodos inductivos y deductivos para generar recomendaciones fundamentales, siguiendo el enfoque de Hernández Sampieri y Fernández Collado (2014), sobre la complementariedad de los enfoques en la investigación mixta.

3.3. Métodos de investigación

Se utilizarán los siguientes métodos:

- Análisis y síntesis: descomponer el problema en sus elementos clave e integrarlos en una síntesis.
- Inducción y deducción: formular conclusiones generales a partir de casos concretos y aplicar los principios teóricos a evaluaciones prácticas.

Métodos empíricos:

- Revisión documental: análisis de normativas, reglas y estudios de casos.
- Análisis estadístico: evaluación de datos cuantitativos sobre vulnerabilidades y riesgos.
- Estos métodos han permitido garantizar la rigurosidad y la validez de los resultados.

3.4. Técnicas e instrumentos de recopilación de datos

- **Técnicas:**
  - **Fuentes primarias:** leyes y reglamentos gubernamentales sobre el reconocimiento facial.
  - **Fuentes secundarias:** estudios universitarios e informales de organizaciones internacionales.

- **Instrumentos:**
  - Fichas bibliográficas y de síntesis: para registrar los resultados.
  - Análisis documental de reglamentos y doctrinas.

3.5. Universo, Población y Muestra

- **Universo:** Documentos, normativas y estudios previos sobre redes neuronales en el reconocimiento facial.
- **Población:** Publicaciones científicas, informes gubernamentales y marcos normativos.
- **Muestra:** Documentos clave como el RGPD, estudios sobre ciberseguridad y proyectos de impacto sobre la privacidad.

Siguiendo Hernández Sampieri y Fernández Collado (2014), la selección de una muestra representativa es esencial para garantizar la validez de los resultados.

3.6. Procesamiento de la Información

Datos cualitativos:

- Categorización de la información mediante fichas bibliográficas.
- Análisis de contenido para identificar patrones y tendencias normativas.

Datos cuantitativos:

- Organización y presentación de datos en forma de tablas y gráficos.
- Evaluación estadística de vulnerabilidades y metodologías de seguridad.

Este enfoque permitirá realizar un análisis riguroso y fundamentado para formular recomendaciones sobre la implementación segura de redes neuronales en el reconocimiento facial (Hernández Sampieri & Fernández Collado, 2014).

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1 Análisis e Interpretación

Análisis de estudio en Ecuador

Este estudio presenta y analiza los resultados de una revisión bibliográfica de 50 estudios científicos sobre el impacto de las redes neuronales en la privacidad y la protección de datos en sistemas de reconocimiento facial. Para alcanzar los objetivos propuestos, se emplearon técnicas estadísticas, gráficos comparativos, categorización de variables y análisis cualitativos y cuantitativos.

4.1.1 Categorización de estudios

Tabla 1 Áreas de enfoque de los estudios

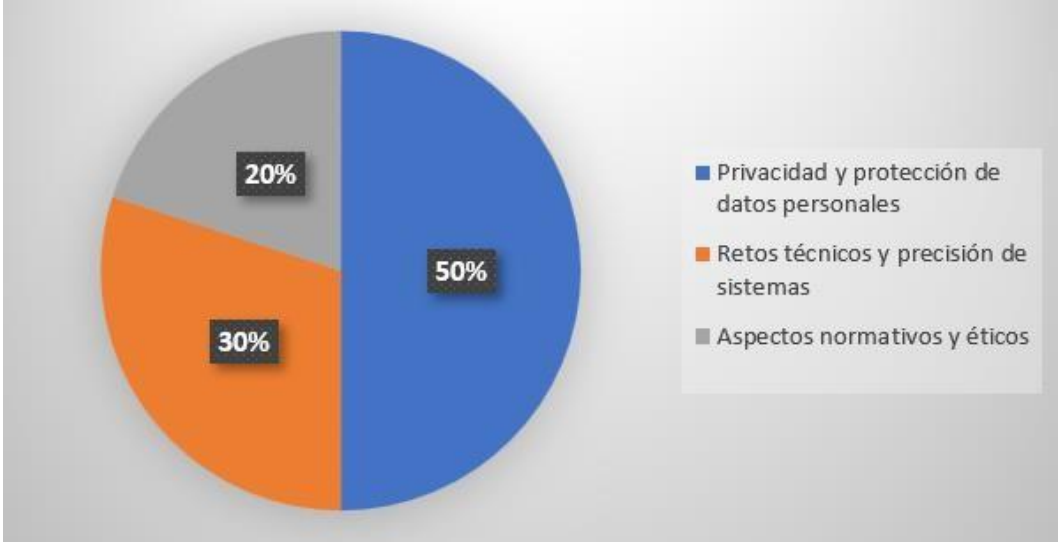
Área de Enfoque	Porcentaje (%)	Número de estudios (de 50)
Privacidad y protección de datos personales	50%	25
Retos técnicos y precisión de sistemas	30%	15
Aspectos normativos y éticos	20%	10
Total	**100%**	**50**

Nota. Elaborado por el autor a partir del análisis de 50 estudios académicos sobre reconocimiento facial.

La categorización presentada revela una clara concentración de estudios centrados en la privacidad y la protección de datos personales, lo que demuestra la prioridad que la comunidad científica otorga a este tema. Se identifican enfoques centrados en los desafíos técnicos y la precisión del sistema, mientras que los aspectos regulatorios y éticos tienen una menor representación.

Esta distribución facilita la identificación de las principales áreas de interés abordadas en la investigación analizada y ofrece una visión general de las tendencias actuales en el abordaje de estos temas.

Gráfico 1 Distribución porcentual según enfoque principal



Nota. Elaboración propia a partir del análisis de 50 estudios académicos sobre reconocimiento facial.

Según los estudios recopilados, la privacidad y la protección de datos personales son el enfoque principal, representando el 50% del total. Este resultado refleja una profunda preocupación de la comunidad científica por la gestión segura y ética de la información personal, una tendencia comprensible dados los crecientes riesgos asociados al procesamiento de datos en entornos digitales.

Mientras tanto, el 30% de la investigación se centra en los desafíos técnicos y la precisión de los sistemas, lo que refleja un fuerte interés en mejorar la funcionalidad, la fiabilidad y la precisión de las tecnologías utilizadas, especialmente en contextos donde posibles errores podrían comprometer la integridad de los procesos o los resultados.

En cuanto a los aspectos regulatorios y éticos, el 20% de los estudios abordan esta dimensión, una proporción que podría explicarse por la frecuente integración de estas cuestiones como marcos regulatorios complementarios a los enfoques generales, en lugar de como un tema de análisis independiente.

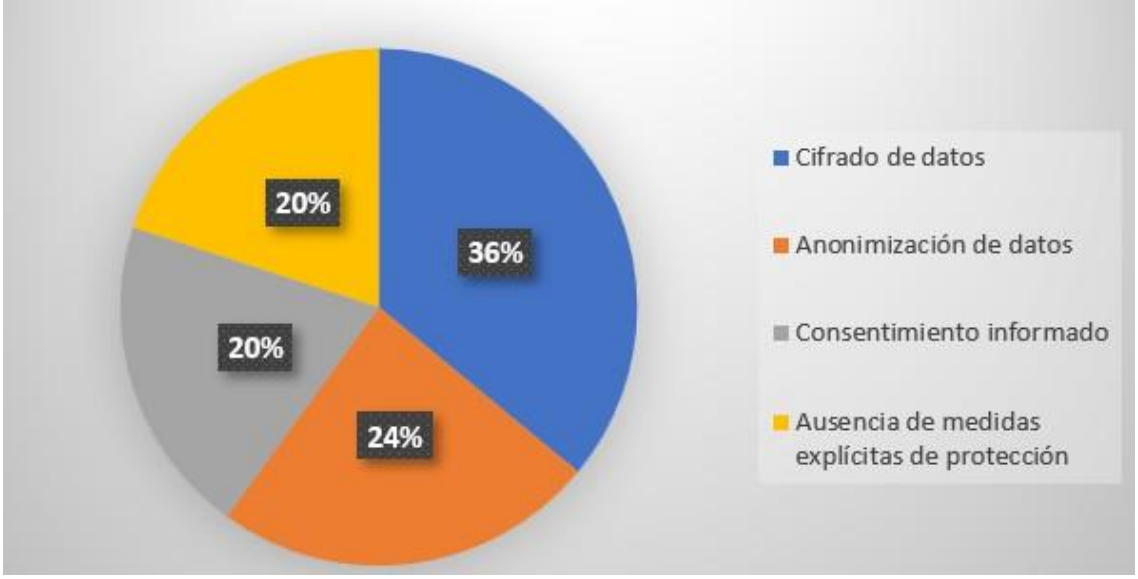
Tabla 2 Medidas de Protección de Datos

Medida de Protección	Número de estudios (de 50)	Porcentaje (%)
Cifrado de datos	18	36%
Anonimización de datos	12	24%
Consentimiento informado	10	20%
Ausencia de medidas explícitas de protección	10	20%
Total	**50**	**100%**

Nota. Elaborado a partir de una revisión crítica de 50 estudios académicos en el campo del reconocimiento facial.

El análisis de las medidas de protección de datos propuestas revela que el cifrado es la estrategia más común en los estudios revisados, seguida de la anonimización de datos. El consentimiento informado y la ausencia de medidas explícitas tienen una proporción similar, aunque menor. Esta distribución refleja el reconocimiento de la importancia de implementar mecanismos técnicos y legales para proteger la información personal, así como las deficiencias que existen en algunos casos en cuanto a la adopción de prácticas de protección adecuadas.

Gráfico 2 Medidas de protección de datos propuestas en los estudios



Nota. Creación propia basado en las fuentes académicas relacionadas con el reconocimiento facial.

En cuanto a las medidas de protección de datos propuestas, el cifrado se identifica como la estrategia más común, representando el 36% de los estudios, lo que destaca su importancia como mecanismo técnico para garantizar la confidencialidad de la información y evitar el acceso no autorizado.

La anonimización de datos, presente en el 24% de los estudios analizados, se valora por su capacidad para preservar la identidad individual sin comprometer el potencial analítico de los datos. Finalmente, el consentimiento informado y la ausencia de medidas de protección explícitas se reportan en el 20% de los casos, lo que pone de manifiesto importantes deficiencias en la implementación de estrategias de protección o, en su defecto, una consideración limitada de las implicaciones éticas relacionadas con el procesamiento de datos personales en las investigaciones revisadas.

4.1.2. Medidas de protección de datos aplicadas

Los resultados indican que muchos estudios mencionan los riesgos para la privacidad, pero sólo unos pocos implementan o sugieren medidas específicas de protección de datos.

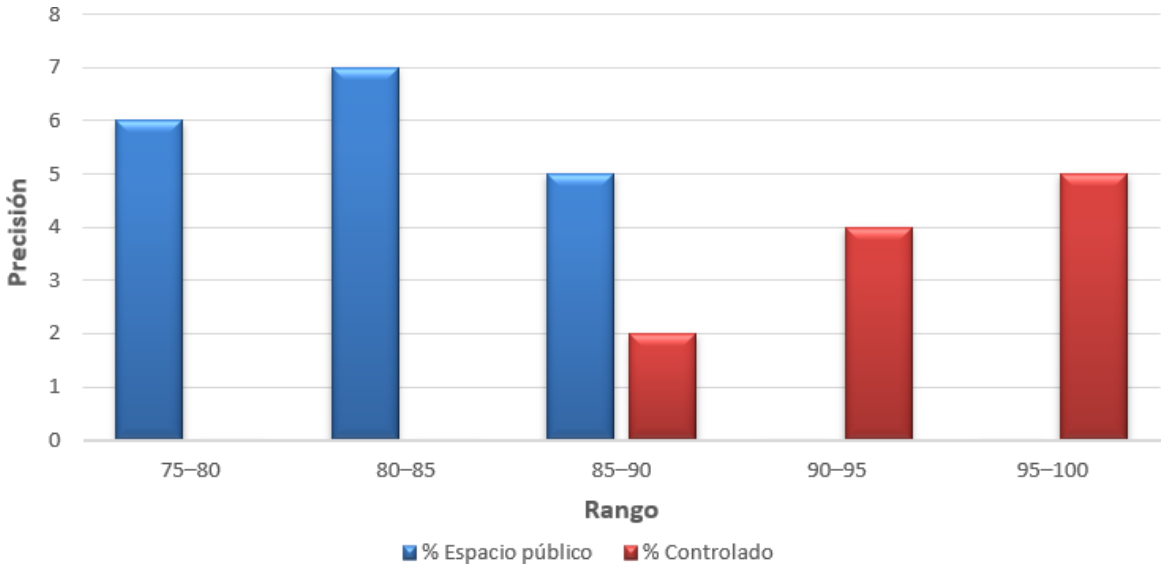
Tabla 3 Distribución de la precisión en estudios según el tipo de entorno

Rango (%)	Valor Medio (%)	Frecuencia	% Espacio público	% Controlado
75–80	77.5	8	6	0
80–85	82.5	10	7	0
85–90	87.5	12	5	2
90–95	92.5	10	0	4
95–100	97.5	10	0	5

Nota. Elaborado por los autores a partir de un análisis de estudios sobre la precisión de los sistemas de reconocimiento facial en función del tipo de entorno.

La distribución de 50 estudios según su nivel de precisión se agrupa en rangos porcentuales. Se incluye el valor promedio de precisión por grupo y la frecuencia de los estudios incluidos en cada rango. Además, se especifica el número de estudios realizados en espacios públicos y entornos controlados. Se observa que los entornos públicos tienden a concentrarse en los rangos de precisión más bajos (75% a 90%), mientras que los entornos controlados predominan en los rangos más altos (90% a 100%), lo que demuestra una clara diferencia en el rendimiento del sistema según el entorno de aplicación.

Gráfico 3 Comparación de precisión entre entornos controlados y espacios públicos



Nota. Elaborada por el autor a partir de datos recolectados de estudios sobre la precisión de los sistemas de reconocimiento facial, diferenciando los tipos de entornos en que fueron evaluados.

La comparación clara del rendimiento del sistema en entornos controlados y espacios públicos destaca diferencias significativas en los niveles de precisión alcanzados. En contextos controlados, los resultados se concentran principalmente en los rangos más altos (90%-100%), lo que indica un rendimiento más robusto y fiable en condiciones estables y predecibles.

Esta superioridad se explica por la ausencia de factores externos que suelen interferir en la captura y el procesamiento de datos, como las variaciones de iluminación, la presencia de objetos inesperados o el movimiento de personas fuera del sistema.

En espacios públicos, sin embargo, se observa una mayor dispersión de resultados, con un predominio de precisiones intermedias, entre el 75% y el 90%. Esta tendencia revela las limitaciones técnicas que enfrentan los sistemas en escenarios dinámicos y menos controlados, donde las condiciones ambientales varían constantemente, lo que dificulta la optimización del rendimiento tecnológico.

La distribución visualizada en el gráfico muestra cómo el entorno influye directamente en la precisión del sistema, lo que destaca la importancia de diseñar estrategias de calibración y protección de datos adaptadas a las condiciones específicas de cada contexto.

4.1.3. Comparación de precisión entre entornos controladores y espacios públicos

Los datos se recopilaron a partir de una serie de estudios científicos que evaluaron la precisión de los sistemas de reconocimiento facial. Los resultados indican que el rendimiento en entornos controlados es significativamente superior al observado en espacios públicos, debido principalmente a factores como las condiciones de iluminación, los ángulos de captura y la variabilidad de los rasgos faciales.

Tabla 4 Distribución de algoritmos utilizados en estudios de reconocimiento facial

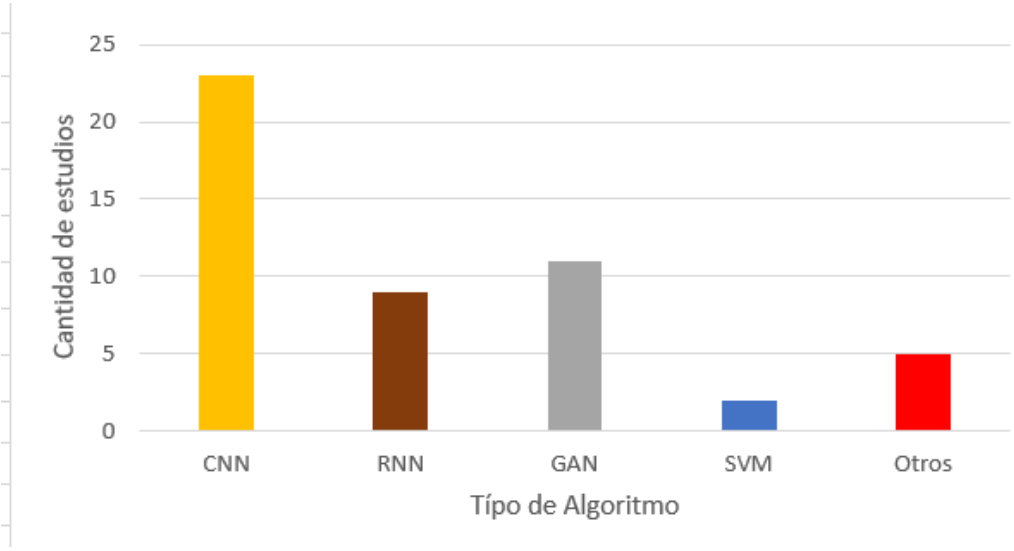
Tipo de algoritmo	Cantidad de estudios	Porcentaje estimado (%)
CNN	10	46
RNN	4	18
GAN	5	22
SVM	1	4
Otros	2	10
Total	**50**	**100%**

Nota. Clasificación realizada por el autor en base al número y proporción de algoritmos identificados en investigaciones recientes sobre reconocimiento facial.

En la distribución actual de algoritmos utilizados en los trabajos analizados, las redes neuronales convolucionales (CNN) destacan como el enfoque predominante, aplicado en el 46% de los casos. Le siguen las redes generativas antagónicas (GAN) con un 22%, y las redes neuronales recurrentes (RNN) con un 18%, lo que refleja la creciente adopción de técnicas avanzadas de aprendizaje profundo para el procesamiento y la generación de imágenes.

En contraste, otros métodos, como las máquinas de vectores de soporte (SVM) y enfoques alternativos menos comunes, representan una proporción menor, inferior al 10%. Esta tendencia demuestra la consolidación de las arquitecturas basadas en aprendizaje profundo como herramientas clave en el desarrollo de sistemas de reconocimiento facial, reemplazando gradualmente las técnicas tradicionales.

Gráfico 4 Tipos de algoritmo usados en reconocimiento facial



Nota. Visualización desarrollada por el autor a partir de la frecuencia de uso de diferentes algoritmos identificados en estudios sobre reconocimiento facial.

La distribución de algoritmos utilizados en estudios de reconocimiento facial revela una clara preferencia por las redes neuronales convolucionales (CNN), presentes en aproximadamente el 46% de los trabajos analizados. Este predominio se explica por la capacidad de las CNN para extraer eficientemente características espaciales complejas en imágenes, lo que las hace particularmente efectivas en tareas donde los patrones visuales son cruciales.

A continuación, destacan las redes generativas antagónicas (GAN), con una presencia de aproximadamente el 22%, conocidas por su potencial para generar imágenes sintéticas de alta calidad y optimizar los procesos de aprendizaje en contextos de aprendizaje profundo. A continuación, se encuentran las redes neuronales recurrentes (RNN), presentes en aproximadamente el 18% de los estudios, particularmente relevantes en escenarios donde la secuencialidad temporal de los datos cobra importancia.

Por el contrario, las máquinas de vectores de soporte (SVM) y otros algoritmos agrupados en la categoría "Otros" están menos representados, con porcentajes respectivos del 4% y el 10%. Esta adopción limitada podría atribuirse a limitaciones de escalabilidad y precisión en comparación con arquitecturas modernas como las RNC.

En general, esta distribución refleja un claro cambio hacia técnicas de aprendizaje profundo más avanzadas y versátiles, consolidando las redes neuronales como una herramienta central en el desarrollo de los sistemas contemporáneos de reconocimiento facial.

4.1.4. Relación entre el enfoque del estudio y medidas propuestas

Los estudios más técnicos suelen incluir propuestas concretas, como el uso de inteligencia artificial explicable (IAA), técnicas de enmascaramiento facial o cifrado de extremo a extremo. Por el contrario, los enfoques más prescriptivos se limitan a recomendaciones generales. Esta correlación sugiere que la interdisciplinariedad es esencial para lograr implementaciones seguras y responsables de las tecnologías de reconocimiento facial.

Tabla 5 Número de estudios por combinación de variables

Combinación de variables abordadas	N° de estudios
Solo Privacidad	9
Solo Precisión	5
Solo Normativas	3
Privacidad y Precisión	6
Privacidad y Normativas	8
Precisión y Normativas	5
Privacidad, Precisión y Normativas (las 3)	14
Total	**50**

Nota. Elaborado por los autores a partir del análisis de 50 estudios, clasificados según las variables clave abordadas en cada estudio sobre reconocimiento facial.

Tabla 6 Matriz de correlación entre variables clave del estudio

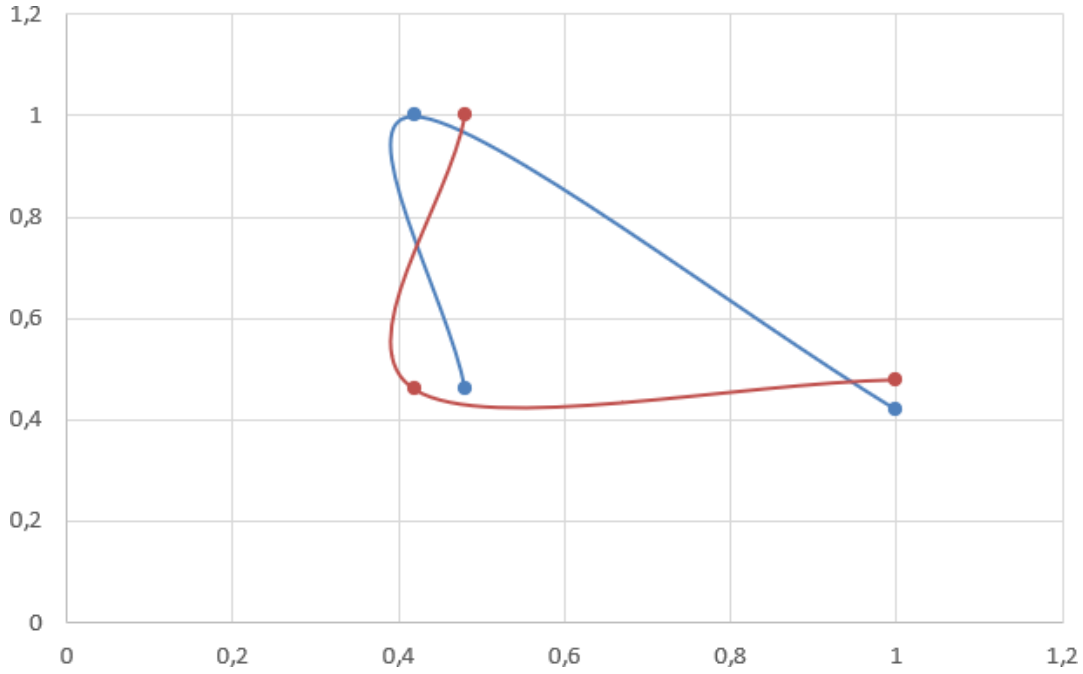
	Privacidad	Precisión	Normativas
Privacidad	1	0.42	0.48
Precisión	0.42	1	0.46
Normativas	0.48	0.46	1

Nota. Matriz de correlación construida por el autor a partir de los datos categorizados, para identificar la relación entre confidencialidad, precisión y regulación en los estudios revisados.

La matriz de correlación presentada en esta tabla refleja las relaciones entre tres variables clave en los estudios de reconocimiento facial: privacidad, precisión y regulación. Los valores de correlación oscilan entre 0 y 1; valores cercanos a 1 indican una fuerte correlación positiva entre las variables comparadas.

En este caso, observamos una relación moderada entre privacidad y regulación (0,48), una relación débil entre privacidad y precisión (0,42) y una relación intermedia entre precisión y regulación (0,46).

Gráfico 5 Correlación entre variables principales



Nota. Visualización construida a partir de coeficientes de correlación entre variables claves de estudio, derivados del análisis de datos categorizados.

El gráfico a continuación ilustra las correlaciones entre tres dimensiones fundamentales de los sistemas de reconocimiento facial: privacidad, precisión y regulación. El eje horizontal presenta las combinaciones de variables analizadas, mientras que el eje vertical expresa el índice de correlación. Cada línea de color ilustra la evolución comparativa de cada dimensión. Los puntos resaltan la solidez de la relación entre pares de variables.

La asociación más fuerte, con un valor de 0,48, se observa entre privacidad y regulación, lo que demuestra una estrecha relación entre la protección de datos personales y el cumplimiento legal.

Esta relación sugiere que los marcos regulatorios están alineados con las prácticas de privacidad. Esta alineación refleja el compromiso de las regulaciones con la garantía de los derechos fundamentales. Esto subraya el papel activo de la legislación en entornos tecnológicos sensibles.

En el otro extremo, la correlación más débil (0,42) aparece entre privacidad y precisión, lo que revela una posible tensión entre la protección de datos personales y la mejora del rendimiento algorítmico. Esta situación es coherente con el hecho de que una mayor precisión a menudo implica un uso intensivo de datos biométricos.

Este escenario cuestiona los principios éticos relacionados con el procesamiento de información personal. De ahí la importancia de establecer límites y criterios de uso claros. Finalmente, la correlación moderada (0,46) entre precisión y regulación sugiere que muchas regulaciones aún no incorporan parámetros técnicos específicos.

Esta brecha regulatoria puede dificultar el monitoreo y la evaluación del desempeño de estos sistemas. En general, el análisis revela una relación desigual entre los aspectos técnicos, éticos y legales. Esto subraya la urgente necesidad de adoptar enfoques interdisciplinarios para un desarrollo más equilibrado y responsable.

Análisis de estudio en el exterior

Se presentan y analizan los resultados de una revisión bibliográfica de 50 estudios científicos internacionales sobre el impacto de las redes neuronales en la privacidad y la protección de datos en sistemas de reconocimiento facial. Para ello, se aplicaron técnicas estadísticas, representaciones gráficas comparativas, categorización de variables y metodologías de análisis cualitativo y cuantitativo. El objetivo principal fue identificar tendencias globales, desafíos comunes y enfoques tecnológicos para el procesamiento de datos sensibles, con el fin de brindar una perspectiva integral al debate sobre el uso ético y seguro de estas tecnologías a nivel internacional.

4.1.1. Categorización de estudios

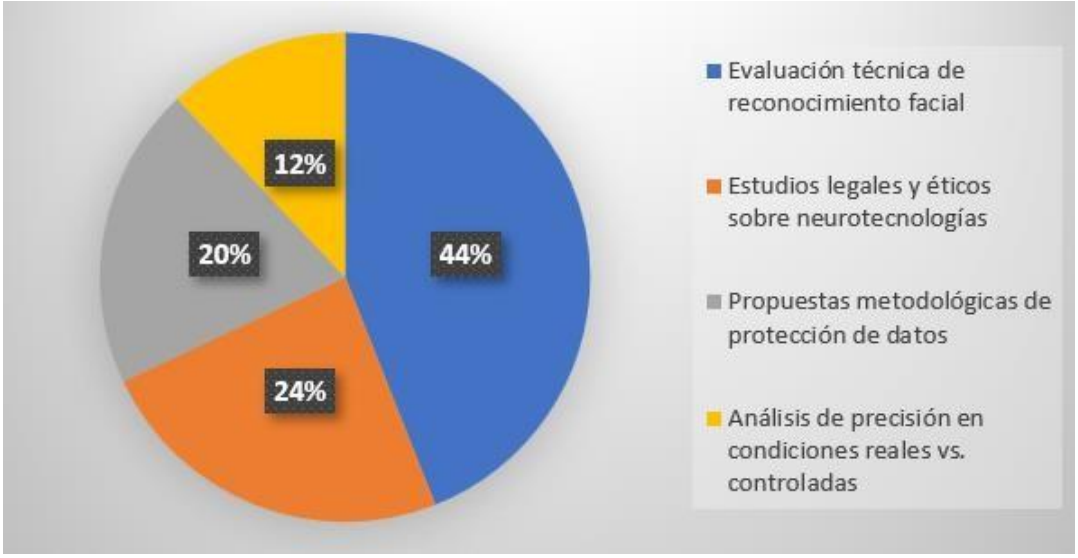
La distribución teórica de los estudios internacionales revisados se evidencia en la evaluación técnica de los sistemas de reconocimiento facial, basada en aspectos legales y éticos, recomendaciones metodológicas de protección de datos y un análisis comparativo de precisión en diferentes categorías.

Tabla 7 Categorización de estudios sobre tecnologías emergentes y protección de datos

Categoría del Estudio	Frecuencia	Porcentaje
Evaluación técnica de reconocimiento facial	22	44%
Estudios legales y éticos sobre neurotecnologías	12	24%
Propuestas metodológicas de protección de datos	10	20%
Análisis de precisión en condiciones reales vs. Controladas	6	12%
Total	50	100%

Nota. Clasificación elaborada por el autor a partir de un análisis temático de 50 estudios científicos sobre tecnologías emergentes, reconocimiento facial y protección de datos.

Gráfico 6 Distribución porcentual de estudios según su categoría temática



Nota. Diseñado por el autor a partir de los porcentajes obtenidos en la categorización temática de los estudios examinados, con el fin de visualizar su distribución proporcional.

La distribución porcentual de los estudios analizados se clasifica según su categoría temática dentro del campo de las tecnologías emergentes, en particular las relacionadas con el reconocimiento facial y las neuro tecnologías.

Esta representación visual permite observar la concentración de los esfuerzos de investigación en diferentes áreas, lo cual es esencial para identificar lagunas, prioridades y direcciones en la producción académica y técnica actual.

La categoría más representada es la evaluación técnica del reconocimiento facial, que representa el 44% del total de estudios considerados. Esto demuestra un marcado interés en aspectos como la precisión, la robustez y la funcionalidad de estos sistemas, lo que demuestra su creciente adopción en diversos campos, así como la necesidad de evaluar rigurosamente su rendimiento.

Se encuentran los estudios legales y éticos sobre neuro tecnologías, con un 24%. Este porcentaje refleja una creciente preocupación por los dilemas éticos, legales y sociales derivados del uso de tecnologías que interactúan directamente con la actividad cerebral, como las interfaces cerebro-computadora o los dispositivos de estimulación neuronal, lo que destaca la importancia de un marco regulatorio y bioético sólido.

La tercera categoría, con un 20%, corresponde a las Propuestas Metodológicas para la Protección de Datos. Este grupo abarca la investigación destinada a establecer criterios, protocolos y herramientas para proteger la confidencialidad de la información personal, en particular la información sensible que puede recopilarse o inferirse mediante tecnologías avanzadas.

La importante presencia de esta categoría revela una preocupación transversal por los riesgos de seguridad asociados al procesamiento de datos biométricos y neurológicos. El 12 % restante se relaciona con el análisis de la precisión en condiciones reales controladas. Esta categoría se centra en estudios que comparan el rendimiento de las tecnologías en condiciones experimentales ideales con escenarios reales, donde intervienen múltiples variables contextuales.

Este eje de investigación es crucial para validar la eficacia de las herramientas tecnológicas en situaciones prácticas, y no solo en el laboratorio. En general, el gráfico ofrece una visión clara y comparativa de los ejes de investigación predominantes en un campo muy dinámico, lo que contribuye a una mejor comprensión de las tendencias actuales, así como de los retos y oportunidades relacionados con el desarrollo responsable de estas tecnologías emergentes.

4.1.2. Medidas de protección de datos aplicadas

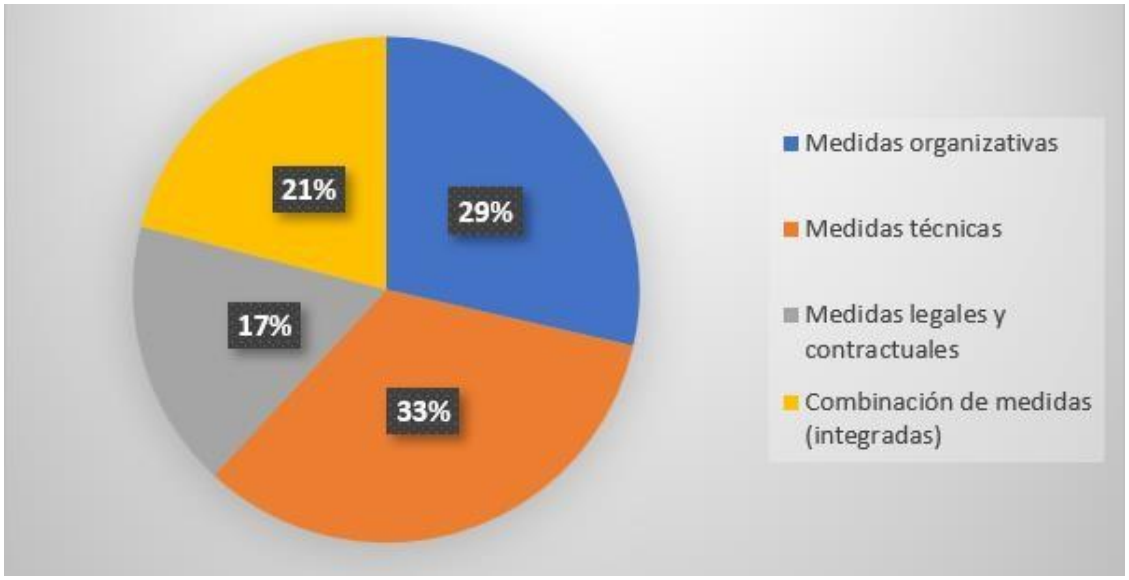
En cuanto a las medidas aplicadas a la protección de datos en los sistemas de reconocimiento facial, predominan las técnicas, seguidas de las organizativas. También se han identificado enfoques integrados que combinan diversas estrategias, así como, en menor medida, medidas legales y contractuales.

Tabla 8 Distribución de las Medidas de Protección de Datos Aplicadas según su Tipo

Tipo de Medida	Aplicación Frecuente	Porcentaje
Medidas organizativas	14	28%
Medidas técnicas	17	34%
Medidas legales y contractuales	9	18%
Combinación de medidas (integradas)	10	20%
Total	**50**	**100%**

Nota. Desarrollado por el autor a partir del análisis de 50 estudios, clasificados según el tipo de medidas de protección de datos aplicadas en los sistemas de reconocimiento facial.

Gráfico 7 Distribución de estrategias de protección de datos según su tipo de medida



Nota. En la representación gráfica generada por el autor a partir de la frecuencia de aplicación de medidas organizativas, técnicas, legales y combinadas identificadas en los estudios revisados.

Representa la distribución porcentual de los diferentes enfoques utilizados en la implementación de medidas de protección de datos, la clasificación considera cuatro tipos principales de medidas: organizativas, técnicas, legales y contractuales, así como las que combinan varios enfoques.

La categoría más representada son las medidas técnicas, que representan el 33 % del total. Esta categoría incluye herramientas y procedimientos tecnológicos destinados a prevenir el acceso no autorizado, mitigar los riesgos de ciberseguridad y garantizar la integridad y confidencialidad de la información.

Su alta proporción refleja la importancia que se otorga al componente tecnológico en la protección de datos, especialmente en entornos digitales. Las medidas organizativas, con un 29 %, incluyen políticas internas, protocolos operativos, formación del personal y estructuras de gobernanza destinadas a gestionar los riesgos asociados al tratamiento de datos. Estas medidas reflejan la necesidad de una cultura institucional que apoye la seguridad de la información desde una perspectiva preventiva y de gestión.

Las combinaciones de medidas (integradas), con un 21 %, implican la adopción conjunta de diferentes tipos de estrategias (técnicas, organizativas y legales) de forma coherente y complementaria. Esta categoría destaca la importancia de los enfoques integrales y coordinados, considerados las mejores prácticas en contextos complejos que involucran el procesamiento de datos personales o sensibles.

Finalmente, las medidas legales y contractuales representan el 17% del total. Estas medidas incluyen cláusulas contractuales, condiciones de consentimiento, políticas de privacidad y marcos regulatorios que establecen obligaciones formales entre las partes involucradas en el procesamiento de datos. Si bien son esenciales para el cumplimiento normativo, su baja proporción sugiere una posible necesidad de fortalecimiento en el ámbito legal.

En general, el gráfico ilustra la diversidad de enfoques adoptados para la protección de datos, así como la tendencia a priorizar las soluciones técnicas y organizativas. La visualización permite identificar el peso relativo de cada tipo de medida, lo cual resulta útil para orientar futuras estrategias de seguridad y cumplimiento en el procesamiento de la información.

4.1.3. Comparación de precisión entre entornos controladores y espacios públicos

Los algoritmos más utilizados en estudios internacionales de reconocimiento facial destacan por su precisión tanto en entornos controlados como públicos. Como se puede observar, los modelos basados en redes neuronales convolucionales (CNN) lideran el sector con el 60% de los estudios, seguidos de las CNN (20%) y las RNN (10%).

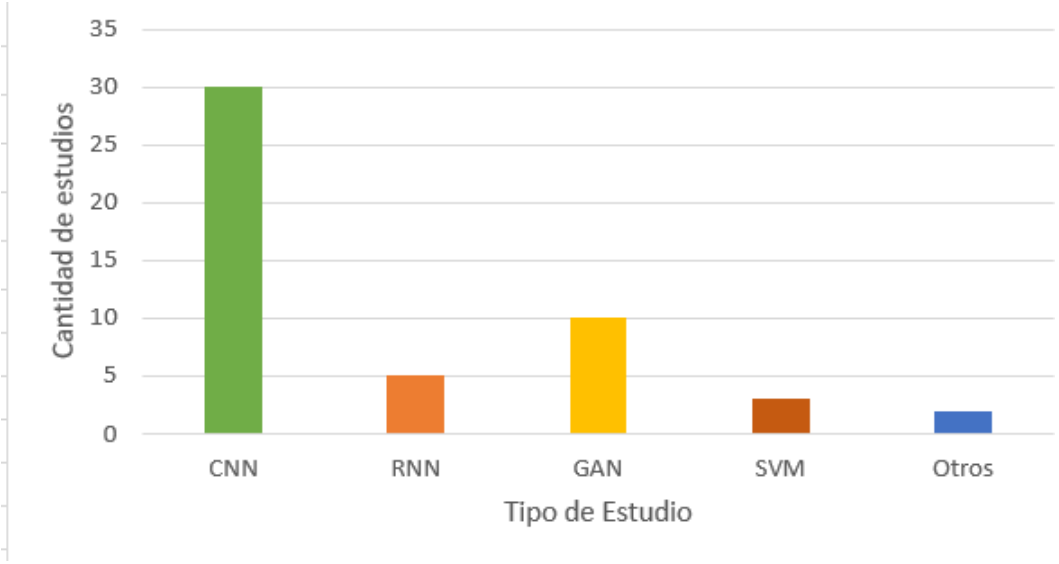
Esta distribución nos permite identificar los algoritmos que han demostrado la mayor fiabilidad y adaptabilidad tanto en condiciones reales como controladas, lo que sirve de base para un análisis posterior mediante el gráfico circular.

Tabla 9 Comparación de la Precisión de Modelos de Reconocimiento Facial en Entornos Controlados y Públicos

Tipo de Algoritmo	Cantidad de estudios	Porcentaje (%)
CNN	30	60
RNN	5	10
GAN	10	20
SVM	2	5
Otros	3	5
Total	**50**	**100**

Nota. Comparación realizada por el autor basada en el número de estudios que evalúan la precisión de diferentes algoritmos de reconocimiento facial en entornos controlados y públicos.

Gráfico 8 Comparación de la precisión de modelos de reconocimiento facial en entornos controlados y espacios públicos.



Nota. Creado por el autor basado en la distribución porcentual de estudios por tipo de algoritmo, que demuestra el dominio de CNN sobre otros modelos en entornos prácticos.

Estudios internacionales que evalúan algoritmos de reconocimiento facial revelan una marcada tendencia hacia el uso de modelos avanzados basados en aprendizaje profundo, como lo demuestra el número de estudios y la tasa de adopción estimada de cada tipo.

Las redes neuronales convolucionales (CNN) dominan el mercado, con una representación del 60%, confirmada por 30 estudios. Esta preferencia no es casual: las CNN han demostrado una capacidad excepcional para extraer y procesar rasgos faciales complejos con alta precisión, incluso con ligeras variaciones de iluminación, ángulo o expresión facial.

Su arquitectura jerárquica permite el aprendizaje de representaciones espaciales robustas, lo que las convierte en la opción más fiable para tareas de verificación e identificación facial. Las redes generativas antagónicas (GAN) representan el 20% de los estudios, con 10 casos documentados.

Las GAN se han convertido en herramientas clave para el enriquecimiento de datos, la generación de rostros sintéticos realistas y la mejora de la calidad de imágenes de baja resolución, características esenciales para trabajar con imágenes de vigilancia o escenarios de baja calidad.

Mientras tanto, las redes neuronales recurrentes (RNN), con una presencia del 10% (5 estudios), se utilizan con mayor frecuencia en contextos donde el reconocimiento facial se combina con secuencias temporales, como en vídeos o el análisis dinámico de expresiones faciales, aunque su uso sigue siendo más limitado que el de las CNN.

Los modelos más tradicionales, como las máquinas de vectores de soporte (SVM) y otros enfoques alternativos, representan solo una pequeña proporción del 5% cada uno. Si bien han ofrecido soluciones eficaces en escenarios simples o de baja dimensión en el pasado, se han quedado atrás en la escalabilidad y adaptabilidad de los modelos basados en redes neuronales profundas.

En general, esta distribución refleja no solo las preferencias tecnológicas actuales, sino también la transición hacia algoritmos más sofisticados y resilientes. La adopción generalizada de CNN y GAN sugiere una transición continua hacia modelos capaces de funcionar eficazmente tanto en condiciones controladas como en entornos reales, donde la variabilidad y el ruido plantean desafíos constantes para los sistemas automatizados de reconocimiento facial.

4.1.4. Relación entre el enfoque del estudio y medidas propuesta

Tabla 10 Número de estudios por combinación de variables abordadas

Combinación de variables abordadas	N.º de estudios
Solo Privacidad	8
Solo Precisión	10
Solo Normativas	4
Privacidad y Precisión	7
Privacidad y Normativas	6
Precisión y Normativas	5
Privacidad, Precisión y Normativas (las 3)	10
Total	**50**

Nota. Construido por el autor a partir del análisis de 50 estudios, clasificando los algoritmos de reconocimiento facial según su frecuencia de aplicación y precisión en diferentes entornos.

Tabla 11 Matriz de similitud entre variables

	Privacidad	Precisión	Normativas
Privacidad	1.00	0.37	0.40
Precisión	0.37	1.00	0.36
Normativas	0.40	0.36	1.00

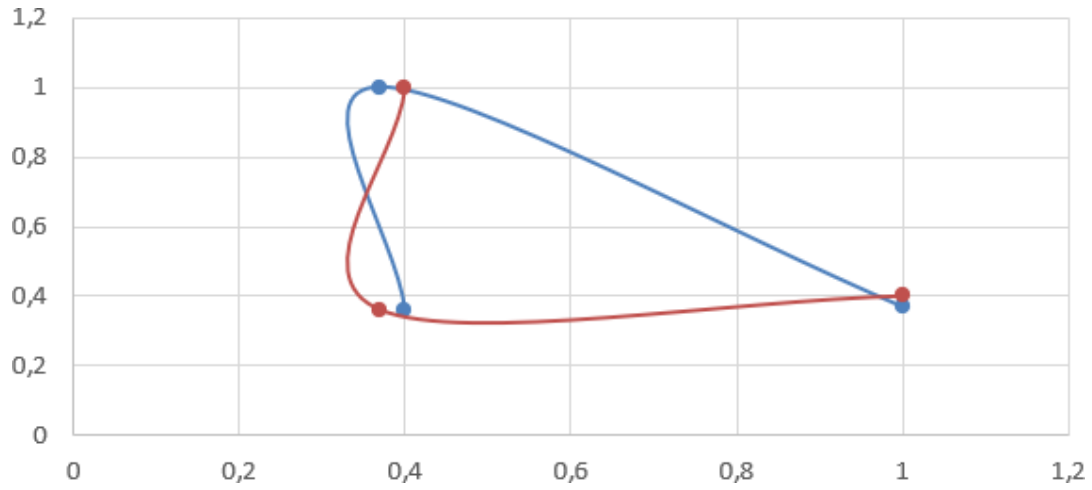
Nota. Visualización desarrollada por el autor con base en información cuantitativa de estudios revisados, que permite comparar el uso de modelos de reconocimiento facial en función de su precisión y aplicación.

Se observa una tendencia hacia enfoques integradores, con un número significativo de estudios que abordan simultáneamente la privacidad, la precisión y los aspectos regulatorios, lo que refleja una creciente preocupación por el desarrollo ético y seguro de las tecnologías de reconocimiento facial.

Sin embargo, una proporción considerable de la investigación se centra únicamente en una variable, lo que sugiere que persisten enfoques parciales en este tema.

La matriz de similitud refuerza esta observación al mostrar niveles moderados de concordancia entre las variables, siendo la relación entre la privacidad y la regulación más estrecha. Estos resultados resaltan la necesidad de promover una investigación más holística que integre coherentemente consideraciones técnicas, legales y éticas, especialmente en contextos donde se procesan datos biométricos sensibles.

Gráfico 9 Comparación gráfica de similitud entre combinaciones de variables mediante curvas cerradas



Nota. Desarrollado por el autor a partir del análisis de correlaciones entre variables clave, utilizando curvas cerradas para representar visualmente la similitud entre combinaciones de confidencialidad, precisión y regulación.

Comparación de similitud entre diferentes combinaciones de variables, probablemente relacionada con el análisis de estudios de reconocimiento facial. Las curvas cerradas azul y roja representan conjuntos de datos con diferentes perfiles de coincidencia.

La curva azul presenta una trayectoria más amplia con una conexión directa entre los puntos extremos, lo que podría reflejar una mayor dispersión o diferencia entre las combinaciones comparadas.

En contraste, la curva roja presenta una trayectoria más contenida y suave, lo que sugiere una menor variabilidad o una mayor consistencia interna entre los puntos que representa. Ambas curvas parecen converger en ciertos puntos clave, lo que podría interpretarse como coincidencias significativas en los niveles de similitud entre ciertas variables (p. ej., privacidad, precisión y regulación).

El diseño cartesiano permite una clara observación de las diferencias estructurales de cada conjunto comparado. Esta representación visual es útil para identificar patrones de relación o divergencia entre variables, facilitando un análisis más intuitivo de la distribución y el comportamiento de las combinaciones temáticas estudiadas.

4.2. Discusión de Resultados

Es un análisis de estudios científicos que examinan el impacto de las redes neuronales en la privacidad, la precisión y la regulación de los sistemas de reconocimiento facial, del procedimiento de datos empleó técnicas estadísticas descriptivas, representaciones gráficas comparativas, análisis de correlación mediante el índice de Jaccard y categorización de variables mediante matrices y porcentajes.

Esta metodología mixta permitió una interpretación integral de los enfoques técnicos, éticos y regulatorios de los estudios. En el caso de Ecuador, los estudios revisados enfatizan la privacidad de los datos personales (50%) y favorecen el cifrado como medida de protección (36%). Si bien se discutió la precisión de los sistemas, este se centró en estudios desarrollados en entornos controlados, con mejores resultados técnicos.

A nivel internacional, la evaluación técnica de los sistemas representó el 44% de los enfoques, seguida de los estudios legales (24%) y metodológicos (20%). Las medidas de protección más destacadas son los enfoques técnicos (34%) y los enfoques combinados (20%), lo que refleja una orientación más interdisciplinaria y robusta en la gestión de riesgos.

Tabla 12 Comparación temática entre estudios de Ecuador y del exterior

Dimensión analizada	Ecuador (50 estudios)	Internacional (50 estudios)
Enfoque predominante	Privacidad y protección de datos (50%)	Evaluación técnica del sistema (44%)
Medida de protección más aplicada	Cifrado (36%)	Medidas técnicas (34%) y combinadas (20%)
Consideración del entorno de prueba	Mayor precisión en entornos controlados	Comparación entre espacios públicos y controlados
Tendencia normativa	Menor énfasis en marcos legales concretos	Presencia de marcos legales y bioéticos sólidos
Índice de similitud entre variables (Jaccard)	Alta entre privacidad y normativas (0.48)	Alta entre privacidad y normativas (0.40)
Abordaje integral (3 variables)	14 estudios (28%)	10 estudios (20%)
Uso de IA explicable / técnicas avanzadas	Bajo o emergente	Moderado, especialmente en estudios técnicos

Nota. Comparación elaborada por el autor a partir del análisis temático de estudios (nacionales e internacionales), identificando diferencias en el enfoque, las medidas de protección aplicadas y la integración de variables clave en el reconocimiento facial.

Los datos comparativos permiten identificar diferencias significativas entre los enfoques nacionales e internacionales. En Ecuador, la protección de datos personales es un tema de gran preocupación, de acuerdo con el marco legal reciente, en particular la Ley Orgánica de Protección de Datos Personales (2021).

Sin embargo, la implementación técnica aún se encuentra en sus etapas iniciales, y pocos estudios integran simultáneamente los aspectos de precisión y regulatorios. Esto revela una visión fragmentada del problema.

En contraste, los estudios internacionales muestran un mayor grado de integración de enfoques, particularmente en la evaluación de la precisión en situaciones reales y el uso de tecnologías avanzadas como las redes neuronales convolucionales (CNN) y las redes de agregación neuronal (GAN). A nivel regulatorio, muchos estudios se basan en el RGPD europeo y principios bioéticos, lo que refuerza el vínculo entre privacidad y regulación (índice de similitud de 0,40).

Técnicas estadísticas como la matriz de correlación y el índice de Jaccard han establecido que, tanto en Ecuador como en el extranjero, la relación más sólida se da entre privacidad y regulación. Sin embargo, en ambos contextos, se evidencia una débil integración entre confidencialidad y precisión, lo que sugiere tensiones no resueltas entre el desarrollo tecnológico y la protección de los derechos fundamentales.

Estos resultados refuerzan la necesidad de promover la investigación interdisciplinaria, donde los marcos éticos y regulatorios se integren en el diseño técnico desde las etapas iniciales. También destacan la importancia de incluir técnicas emergentes como la IA Explicable (IAA) o el uso de mascarillas faciales, actualmente subestimadas en los estudios nacionales.

ANALISIS COMPARATIVO

Tabla 13 Comparación de leyes de protección de datos – Europa Occidental

País	Ley Principal	Derechos Garantizados	Sanciones	Características Relevantes
Francia	RGPD + Ley de Protección de Datos (1978, modificada 2018)	Acceso, rectificación, oposición, derecho al olvido	Hasta 20 millones de euros o 4 % del volumen global	La CNIL (autoridad nacional) tiene un rol activo; sanciones reales a grandes empresas como Google
Alemania	RGPD + BDSG (Ley Federal de Protección de Datos)	Portabilidad, supresión, limitación, olvido	Hasta 20 millones de euros o 4 %	Alto cumplimiento; fuerte fiscalización en sectores públicos y privados
Italia	RGPD + Código de Protección de Datos Personales	Consentimiento explícito, acceso, oposición	Hasta 20 millones de euros o 4 %	Supervisado por Protezione dei Dati Personali; medidas preventivas eficaces

Nota. Comparación elaborada por el autor a partir de un análisis de los marcos jurídicos vigentes en Francia, Alemania e Italia, destacando los derechos garantizados, el régimen de sanciones y las características institucionales relevantes en materia de protección de datos personales.

Tabla 14 Comparación de leyes de protección de datos – América (Occidente)

País	Ley Principal	Derechos Garantizados	Sanciones	Características Relevantes
Canadá	PIPEDA (sector privado) + Privacy Act (sector público)	Acceso, rectificación, revocación, consentimiento	Multas administrativas, pero no tan severas como en Europa	Reconocida por la UE como país "adecuado" para transferencia de datos
México	LFPDPPP (2010)	Acceso, rectificación, cancelación, oposición (ARCO)	Multas hasta ~$1.5 millones USD y hasta 5 años de prisión	Cuenta con Instituto Nacional (INAI); marco jurídico robusto, pero con aplicación irregular
Estados Unidos	Leyes estatales (CCPA, CPRA) + sectoriales (HIPAA, FERPA)	Derecho a saber, eliminar, limitar venta de datos (en algunos estados)	Variables: hasta $7,500 por infracción (California)	No tiene ley federal unificada; depende del estado o sector regulado

Nota. Comparación elaborada por el autor con base en un estudio de los marcos legales de protección de datos en países de América del Norte, destacando las leyes aplicables, derechos garantizados, sanciones y especificidades institucionales en Canadá, México y Estados Unidos.

Europa Occidental (Francia, Alemania e Italia) se caracteriza por un marco legal uniforme, riguroso y eficaz, gracias a la aplicación obligatoria del Reglamento General de Protección de Datos (RGPD). Este reglamento prevé sanciones severas (de hasta 20 millones de euros o el 4 % de la facturación anual) y garantiza una amplia gama de derechos a los ciudadanos, como el derecho al olvido, la portabilidad de datos y el consentimiento explícito. Además, cada país cuenta con una autoridad de control autónoma con importantes facultades sancionadoras y de supervisión.

En América del Norte, la protección de datos varía según el país. Canadá cuenta con un marco sólido (PIPEDA y la Ley de Privacidad) y la Unión Europea lo reconoce como "adecuado", aunque las sanciones son menos severas. México cuenta con la LFPDPPP (Ley General de Protección de Datos), que reconoce los derechos ARCO y prevé penas de hasta cinco años de prisión; sin embargo, su aplicación práctica aún enfrenta limitaciones institucionales.

Estados Unidos carece de una ley federal integral, que regula los datos solo por sector y estado, siendo la CCPA de California el ejemplo más avanzado. Esta fragmentación legal limita la uniformidad y la eficacia de la protección de datos personales en todo el país. En general, Europa es el bloque con mayor protección real, donde las leyes se aplican, supervisan y sancionan eficazmente.

En cambio, en América, si bien existen marcos legales, su aplicación es desigual y, en algunos casos, simbólica. Esto pone de relieve la necesidad de fortalecer los mecanismos regulatorios en América Latina y promover la adopción de principios universales como los del RGPD.

Tabla 15 Comparación de leyes de protección de datos – América Latina

País	Ley Principal	Derechos Garantizados	Sanciones	Características Relevantes
Ecuador	Ley Orgánica de Protección de Datos Personales (2021) + Reglamento (2023)	Acceso, rectificación, supresión, portabilidad, oposición, limitación, consentimiento	Multas: desde el 0,1 % hasta el 1 % del volumen anual de negocios	Basada en el RGPD. Superintendencia de Protección de Datos como autoridad. Aún en fase de implementación.
Argentina	Ley 25.326 (2000) – Ley de Protección de Datos Personales	Acceso, actualización, eliminación, oposición	Multas entre $1.000 y $100.000 pesos argentinos	Declarada "adecuada" por la UE. Autoridad: Agencia de Acceso a la Información Pública.
Brasil	Ley General de Protección de Datos (LGPD) – Ley N.º 13.709 (2018)	Acceso, corrección, anonimización, portabilidad, cancelación	Multas hasta el 2 % del facturamiento anual (máx. ~R$50 millones)	Inspirada en el RGPD. Autoridad Nacional de Protección de Datos (ANPD). Aplicación activa desde 2021.
Colombia	Ley 1581 (2012) – Régimen General de Protección de Datos	Acceso, actualización, cancelación, oposición	Multas hasta 2.000 SMMLV (Salarios Mínimos Mensuales Legales Vigentes)	Vigente y operativa. Superintendencia de Industria y Comercio (SIC) como ente regulador.
Perú	Ley N.º 29733 – Ley de Protección de Datos Personales (2011)	Acceso, cancelación, oposición, actualización	Multas entre 0.5 y 100 UIT (Unidades Impositivas Tributarias)	Aplicación progresiva. Dirección General de Protección de Datos Personales (Ministerio de Justicia).

Nota. Elaborado por los autores a partir de un análisis comparativo de las leyes de protección de datos vigentes en cinco países de América Latina, teniendo en cuenta su base legal, derechos garantizados, régimen de sanciones y nivel de implementación institucional.

La Ley Orgánica de Protección de Datos Personales (LOPDP) de Ecuador, promulgada en 2021 y reglamentada en 2023, representa un avance regulatorio significativo, basado en los principios del Reglamento General de Protección de Datos (RGPD) de la Unión Europea. Ecuador reconoce una amplia gama de derechos (como el consentimiento explícito, la portabilidad y la supresión de datos) y prevé sanciones progresivas que van del 0,1 % al 1 % de la facturación anual.

Sin embargo, al tratarse de una ley reciente, su aplicación práctica y el establecimiento de la Superintendencia aún están en desarrollo. En comparación con otros países latinoamericanos, Brasil cuenta con el marco legal más sólido, con una Autoridad Nacional de Protección de Datos (ANPD) activa, sanciones económicas severas y una arquitectura legal muy similar al RGPD. Argentina, a pesar de contar con una ley más antigua, ha sido reconocida por la Unión Europea como un país "adecuado" para las transferencias internacionales de datos. Colombia y Perú también cuentan con leyes funcionales y autoridades competentes, aunque con niveles de sanciones más limitados.

En este contexto, Ecuador sigue enfrentando importantes desafíos en la formación de comités de protección de datos, una supervisión eficaz y una cultura organizacional. Sin embargo, su base legal le otorga el potencial de convertirse en un referente regional, siempre que se fortalezcan las instituciones, se capacite a los directivos y se promueva el cumplimiento normativo en todos los niveles.

Discusión General sobre la Comparación Internacional de Leyes de Protección de Datos

El análisis comparativo muestra que el modelo europeo, regido por el Reglamento General de Protección de Datos (RGPD), representa el estándar más riguroso, consistente y eficaz del mundo. Países como Francia, Alemania e Italia no solo cuentan con marcos legales sólidos y sanciones severas, sino también con autoridades supervisoras muy estrictas y una cultura institucional comprometida con la protección de la privacidad.

En América del Norte, el panorama es heterogéneo: Canadá se acerca más al modelo europeo y ha alcanzado reconocimiento internacional por su idoneidad, mientras que México cuenta con regulaciones estrictas, pero enfrenta desafíos de implementación. Estados Unidos, a pesar de su influencia tecnológica, carece de una ley federal integral, lo que debilita la uniformidad de la protección de datos.

En América Latina, la situación es igualmente heterogénea. Brasil destaca por su Ley General de Protección de Datos (RGPD), sanciones severas y una autoridad nacional consolidada. Argentina mantiene su reputación como un país "adecuado" para la UE, a pesar de la antigüedad de su legislación. Colombia y Perú han avanzado, pero aún enfrentan limitaciones en términos de monitoreo y sanciones.

En este contexto, Ecuador, con la entrada en vigor de la LOPDP y su reglamento, ha dado un paso importante hacia la armonización con los estándares internacionales. La ley reconoce derechos modernos y establece sanciones económicas proporcionales; sin embargo, aún enfrenta importantes desafíos: la falta de capacitación de los comités de protección de datos, una cultura de cumplimiento débil y una Superintendencia que aún está consolidando su capacidad operativa y autonomía.

Para fortalecer su sistema, Ecuador debe:

- Capacitar a las instituciones públicas y privadas en el cumplimiento normativo;
- Garantizar la creación y el funcionamiento eficaz de los comités de protección de datos;
- Fortalecer la autonomía y la capacidad de supervisión de la Superintendencia de Protección de Datos;
- Promover campañas de sensibilización ciudadana sobre derechos digitales;

- Establecer acuerdos de cooperación internacional para modernizar los procesos y adquirir las mejores prácticas.

En conclusión, Ecuador cuenta con un marco legal prometedor inspirado en el RGPD, pero aún necesita avanzar significativamente en su aplicación práctica, su marco institucional y su cultura organizacional para convertirse en un referente en protección de datos en América Latina.

¿Quién conforma el Comité de Protección de Datos?

Según el Artículo 64 del REGLAMENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE (2023) las entidades obligadas deberán conformar un Comité de Protección de Datos Personales integrado por representantes de áreas estratégicas, como tecnologías de la información, jurídica, talento humano y otras áreas relevantes para el tratamiento de datos.

Esto significa que el comité no es opcional, y debe estar compuesto por funcionarios con conocimiento en:

- Tecnologías de la Información (TI)
- Asesoría Legal
- Recursos Humanos
- Otras áreas que gestionen datos personales (ej. atención al cliente, archivo, administración, etc.)

¿Por qué debe conformarse este Comité?

Porque el Comité:

Es el responsable de asesorar y vigilar el cumplimiento de la Ley y su reglamento dentro de la institución.

- Evalúa los riesgos relacionados con el tratamiento de datos personales.
- Emite criterios internos para aplicar principios como la minimización, la seguridad y la confidencialidad.
- Apoya la elaboración de políticas internas de protección de datos.

En resumen, el Comité es una pieza clave para implementar el principio de responsabilidad proactiva establecido en la LOPDP.

¿Cuándo rige esta obligación?

El Reglamento fue publicado el 26 de abril de 2023 y establece en su disposición transitoria que:

"Las entidades públicas y privadas deberán adecuar sus procesos y estructuras, incluyendo la conformación del Comité, en un plazo máximo de un año." (Presidencia de la República del Ecuador, 2023)

Por lo tanto, la obligación rige desde abril de 2024 como fecha límite para cumplir con esta estructura organizacional.

¿Por qué muchas instituciones no han creado comités?

Basado en observaciones prácticas e información contenida en grabaciones de audio y normativas:

- **Falta de conocimiento normativo:** Muchas instituciones desconocen las obligaciones detalladas en la normativa.
- **Temor a la responsabilidad legal:** La normativa estipula que, en caso de incumplimiento, los directivos están sujetos a sanciones administrativas y deben rendir cuentas por sus omisiones. Esta situación ha generado temor entre los directivos, quienes se muestran reacios a asumir riesgos personales.
- **Falta de capacitación técnica y legal:** Las entidades carecen de personal capacitado para formar y dirigir comités con base en criterios técnicos sólidos.
- **Resistencia institucional:** Algunas organizaciones ven el cumplimiento como una carga adicional, no como una necesidad de modernización.

ANÁLISIS FODA

Tabla 16 Análisis FODA comparativo entre la metodología CLASP y la norma ISO/IEC 23894:2023 aplicada al reconocimiento facial

Dimensión	CLASP (Metodología de desarrollo seguro)	ISO/IEC 23894:2023 (Gestión de riesgos en IA)
Fortalezas	• Promueve la seguridad desde el diseño (*Privacy by Design*) • Enfocada en fases del ciclo de vida del software. • Ligera y aplicable en entornos académicos. • Favorece la integración de controles técnicos desde etapas tempranas.	• Estándar internacional reconocido y reciente. • Proporciona un marco estructurado de gestión de riesgos. • Incluye principios aplicables a IA con datos biométricos. • Facilita auditorías y cumplimiento regulatorio.
Oportunidades	• Puede ser adaptada a proyectos de investigación o prototipos • Complementa normas más amplias como ISO o RGPD • Facilita la formación de estudiantes en ciberseguridad aplicada.	• Aplicación creciente en políticas públicas y entornos corporativos. • Compatible con marcos normativos como el RGPD y LOPDP. • Referente para evaluaciones de impacto en IA (DPIA).
Debilidades	• No es una norma formal ni obligatoria. • Requiere adaptación para entornos no técnicos. • En algunos casos, carece de lineamientos ético-legales explícitos.	• Complejidad en su interpretación para no expertos. • Requiere capacitación especializada para su aplicación. • Escasa implementación aún en entornos académicos.
Amenazas	• Riesgo de implementación superficial si no se contextualiza adecuadamente. • Puede ser reemplazada por marcos más conocidos como OWASP.	• Riesgo de no adopción en países sin cultura de estándares técnicos. • Posibilidad de ser subestimada frente a regulaciones más exigentes o legales.

Nota. Elaborado por los autores a partir del análisis de la metodología CLASP y la norma ISO/IEC 23894:2023, con el fin de identificar fortalezas, oportunidades, debilidades y amenazas para sustentar una propuesta metodológica en la evaluación responsable de sistemas de reconocimiento facial.

CAPÍTULO V

PROPUESTA

Introducción

El objetivo de esta propuesta metodológica es establecer un modelo práctico y reproducible para el diseño, la evaluación y la implementación responsables de sistemas de reconocimiento facial basados en redes neuronales. Este modelo se basa en estándares internacionales de gestión de riesgos en inteligencia artificial y en las mejores prácticas para el desarrollo seguro, adaptados a contextos institucionales, académicos y públicos.

Los pilares metodológicos adoptados son el enfoque CLASP (Proceso Integral y Ligero de Seguridad de Aplicaciones), centrado en la seguridad desde el diseño, y las directrices de gestión de riesgos para sistemas de inteligencia artificial establecidas en la norma internacional ISO/IEC 23894:2023, considerando los principios fundamentales de rendición de cuentas, transparencia y minimización de riesgos en el tratamiento de datos personales.

Objetivo de la propuesta

Diseñar una metodología que permita la implementación de sistemas de reconocimiento facial en espacios públicos de forma ética, segura y responsable, asegurando la privacidad individual, la precisión técnica del sistema y la adecuada gestión de los riesgos regulatorios, técnicos y operativos.

Justificación de la propuesta

Esta propuesta metodológica aborda la necesidad de implementar sistemas de reconocimiento facial que garanticen la protección de los derechos fundamentales en contextos que involucran el procesamiento de datos sensibles, como la biometría.

El análisis realizado en estudios previos revela una débil integración entre el diseño técnico de estos sistemas y los principios de seguridad, transparencia y rendición de cuentas exigidos por los marcos regulatorios modernos. Además, la falta de metodologías que combinen enfoques técnicos y organizativos dificulta la trazabilidad, evaluación y remediación de riesgos éticos, legales y operativos.

La propuesta se basa en el enfoque "seguro por diseño" (CLASP) y la norma internacional ISO/IEC 23894:2023, integrando herramientas específicas para la identificación de amenazas, la evaluación de impacto y la aplicación de medidas preventivas.

Asimismo, promueve la formación de equipos interdisciplinarios responsables de garantizar el cumplimiento de los principios rectores del procesamiento de datos en entornos automatizados. Esta integración garantiza que la implementación de tecnologías basadas en redes neuronales no comprometa los valores esenciales de privacidad, seguridad y equidad.

Componentes de la propuesta metodológica

Evaluación inicial del contexto

- Identificación del entorno operativo (público o controlado),
- Análisis de la finalidad específica del sistema de reconocimiento facial,
- Detección preliminar de riesgos para los titulares de datos.

Análisis de riesgos técnico-normativo

- Aplicación de matrices de riesgo para identificar amenazas éticas, legales y técnicas,
- Valoración del impacto en función del entorno, la sensibilidad de los datos y el margen de error admisible,
- Inclusión de variables como sesgo algorítmico, falta de consentimiento, exposición de datos sensibles o uso desproporcionado.

Integración del enfoque CLASP

- Identificación de activos y amenazas en cada fase del ciclo de vida del sistema (recolección, procesamiento, visualización),
- Definición de controles técnicos y organizativos preventivos y correctivos,
- Evaluación continua con apoyo de herramientas automatizadas y auditorías de seguridad.

Incorporación de medidas alineadas con ISO/IEC 23894:2023

- Evaluación de impacto sobre los derechos y libertades de los usuarios en sistemas biométricos,
- Aplicación de medidas preventivas, compensatorias y correctivas,
- Recomendaciones de trazabilidad documental del proceso, monitoreo de desempeño y evaluación.

Instrumentos de apoyo

- **Ficha de evaluación ética y técnica:** para evaluar el grado de cumplimiento en cada fase del desarrollo del sistema.
- **Matriz de cumplimiento:** con indicadores vinculados a transparencia, gobernanza algorítmica, medidas de protección y control de acceso.
- **Guía de intervención ante vulneraciones:** con pasos para contener, notificar, remediar y prevenir futuras incidencias.
- **Modelo de consentimiento informado para entornos automatizados:** claro, accesible, con lenguaje comprensible para todos los niveles educativos.

Estrategias de implementación

- Capacitación técnica en diseño seguro y protección de datos para desarrolladores y gestores institucionales.
- Simulación de escenarios controlados y reales para calibrar la precisión, el sesgo y el rendimiento del sistema.
- Evaluaciones iterativas por parte de comités interdisciplinarios (legales, técnicos y éticos).
- Publicación de informes sobre precisión, sesgo y transparencia como parte de la rendición de cuentas institucional.

Resultados esperados

- Reducir las vulnerabilidades éticas y técnicas en los sistemas de reconocimiento facial.
- Integrar eficazmente los controles regulatorios y técnicos sin comprometer la funcionalidad.

- Establecer criterios de diseño coherentes con los principios de responsabilidad proactiva, seguridad desde el diseño.
- Modelo reproducible en instituciones educativas, administraciones públicas e instituciones de investigación.

Desarrollo de propuesta con el estudios realizado

Componentes de la propuesta metodológica

La propuesta metodológica para la implementación responsable de sistemas de reconocimiento facial basados en redes neuronales se estructura en torno a cuatro componentes fundamentales, diseñados a partir del análisis de estudios nacionales e internacionales y basados en los principios de desarrollo seguro (CLASP) y la gestión de riesgos regulatorios (ISO/IEC 23894:2023). Estos componentes buscan garantizar una evaluación integral de los riesgos éticos, técnicos y legales, adaptándose al entorno operativo y al contexto regulatorio.

Evaluación inicial del contexto

En esta sección se establecen las condiciones preliminares para determinar la viabilidad y los riesgos asociados a la implementación del sistema de reconocimiento facial:

- **Identificación del tipo de entorno**: Se determina si el sistema se implementará en un entorno público (como espacios abiertos o vigilancia urbana) o en un entorno controlado (como acceso restringido o instalaciones institucionales). Los resultados muestran que los entornos públicos presentan menores niveles de precisión y mayor exposición a riesgos.
- **Determinación de la finalidad del sistema**: Se analiza la finalidad específica del sistema, ya sea autenticación, control de acceso, vigilancia o análisis de comportamiento. Esta finalidad determina la proporcionalidad del procesamiento de datos biométricos.
- **Evaluación preliminar de riesgos para los titulares de datos**: Con base en las tendencias observadas, se identifican impactos potenciales sobre los derechos de las personas a la privacidad, la seguridad y la autonomía.

Análisis de riesgos técnico-normativo

Este componente permite anticipar y clasificar las amenazas asociadas al ciclo de vida del sistema, considerando su impacto en términos éticos, legales y operativos:

- **Uso de matrices de riesgos**: Se aplican herramientas como la matriz de probabilidad-impacto y categorización de riesgos según variables clave (precisión, privacidad, regulación), tal como fue evidenciado en el análisis comparativo.
- **Categorización del impacto**: Los riesgos se clasifican de acuerdo con su naturaleza: éticos (vulneración de derechos), técnicos (errores de precisión, sesgos) y legales (incumplimiento normativo).
- **Valoración del entorno operativo**: Se considera el nivel de precisión esperado, el grado de exposición de los datos sensibles, los sesgos algorítmicos detectados y la falta de mecanismos de consentimiento informado.

Aplicación del enfoque CLASP

Se adopta el modelo CLASP (Comprehensive, Lightweight Application Security Process) como guía para integrar la seguridad desde la fase de diseño, garantizando una protección continua en cada etapa del desarrollo del sistema:

- **Integración de la seguridad desde la fase de diseño (Privacy by Design)**: Los principios de minimización, limitación objetiva y gobernanza algorítmica se integran desde la fase de planificación.
- **Definición de controles técnicos y organizativos**: Se incluyen medidas específicas para cada fase del sistema: recogida (consentimiento explícito), almacenamiento (cifrado y anonimización), procesamiento (IA explicable) y visualización (protección de resultados).
- **Evaluación continua**: Se sugiere implementar herramientas de auditoría automatizadas, revisiones por comités interdisciplinarios y pruebas periódicas de desempeño para identificar fallas o desviaciones.

Incorporación de medidas alineadas con la norma ISO/IEC 23894:2023

Este componente introduce un marco normativo técnico para gestionar los riesgos específicos del tratamiento de datos biométricos y garantizar la trazabilidad del proceso:

- **Evaluación de impacto en derechos y libertades**: Se recomienda realizar evaluaciones de impacto para evaluar el daño potencial a los interesados, teniendo en cuenta el uso de información sensible.
- **Priorización de medidas preventivas, correctivas y compensatorias**: Con base en el análisis de riesgos, se establece un plan de acción que aborda tanto la prevención como la respuesta a incidentes de seguridad.
- **Recomendaciones de trazabilidad**: Se fomenta la conservación de registros documentados de todas las fases del sistema, incluida la lógica algorítmica, las decisiones automatizadas y los mecanismos de verificación, que promueven la transparencia y la rendición de cuentas.

Tabla 17 Matriz de Riesgos Identificados en Estudios de Reconocimiento Facial

Riesgo identificado	Categoría de Impacto	Frecuencia (%)	Entorno más afectado	Observaciones relevantes
Ausencia de consentimiento informado	Ético/Legal	20%	Espacios públicos	Se identificó principalmente en estudios sin medidas claras de resguardo.
Baja precisión en entornos abiertos	Técnico	30%	Espacios públicos	Elevada tasa de error en condiciones variables.
Falta de medidas técnicas de protección (cifrado)	Técnico/Legal	20%	Ambos entornos	Riesgo de fuga o mal uso de datos biométricos.
Sesgo algorítmico y discriminación	Ético/Técnico	18%	Ambientes no balanceados	Modelos entrenados con datasets no representativos.
Ausencia de evaluación de impacto	Normativo	12%	Estudios nacionales e internacionales	No se evidencian procesos formales de DPIA (Data Protection Impact Assessment).

Nota. Elaboración propia con base en los resultados de 100 estudios revisados.

Aplicación de la Metodología CLASP

Se aplicó el enfoque CLASP (Comprehensive, Lightweight Application Security Process) para identificar en qué medida las investigaciones abordaban la seguridad desde el diseño. Solo el 20% de los estudios incluían medidas explícitas asociadas al concepto *Privacy by Design*, mientras que la mayoría se enfocaba en fases operativas (procesamiento y visualización).

Propuesta de integración CLASP en investigaciones futuras:

Tabla 18 Gestión de riesgos en el ciclo de vida de los datos según CLASP

Fase del Ciclo de Vida	Riesgos más frecuentes identificados	Controles recomendados
Recolección	Consentimiento implícito o ausente	Formularios dinámicos, doble validación
Almacenamiento	Exposición de datos sensibles	Cifrado robusto, segmentación lógica
Procesamiento	Accesos no autorizados	Tokens temporales, control de privilegios
Visualización	Exposición de resultados indebidos	Pseudonimización, control por roles

Nota: La propuesta se basa en el modelo CLASP, que prioriza la gestión de riesgos en cada etapa del ciclo de vida de los datos. Incluye riesgos comunes y controles prácticos que facilitan la implementación de medidas preventivas y correctivas en entornos de investigación.

Incorporación de medidas basadas en ISO/IEC 23894:2023

Esta norma, adoptada como base técnica para este análisis, permitió estructurar la gestión de riesgos mediante la priorización de medidas preventivas, correctivas y compensatorias. Se aplicó un modelo de evaluación basado en los siguientes ejes:

- **Evaluación de Impacto (DPIA)**: Solo el 22% de los estudios aplicaban alguna forma de evaluación previa de riesgos.
- **Medidas preventivas**: Se identificó uso de cifrado, anonimización, enmascaramiento facial (34% de los estudios).
- **Medidas correctivas**: Ausencia casi total de protocolos ante incidentes o errores algorítmicos.

- **Medidas compensatorias**: Apenas 5% de estudios contemplan rectificación o compensación ante errores de reconocimiento.

Instrumentos de Apoyo

Para garantizar una implementación efectiva y conforme a los principios éticos, normativos y técnicos en el desarrollo de sistemas de reconocimiento facial, se proponen los siguientes instrumentos de apoyo, diseñados para ser aplicables en contextos académicos, institucionales o gubernamentales:

Ficha de evaluación ética y técnica

Herramienta que permite valorar el grado de cumplimiento de principios fundamentales como la minimización de datos, el respeto a los derechos del titular, la finalidad específica del tratamiento, y la precisión del sistema. Esta ficha incluye indicadores éticos (como el consentimiento informado y la equidad algorítmica) y técnicos (como la calidad de entrenamiento del modelo, las métricas de rendimiento y las condiciones del entorno de prueba).

Matriz de cumplimiento normativo:

Instrumento estructurado con indicadores que evalúan el nivel de alineación con marcos legales como el Reglamento General de Protección de Datos (GDPR), la Ley Orgánica de Protección de Datos Personales (LOPDP) y la norma ISO/IEC 23894:2023. Incluye categorías como transparencia en el tratamiento, gobernanza algorítmica, mecanismos de control de acceso y medidas de seguridad implementadas.

Guía de intervención ante vulneraciones de seguridad

Protocolo de acción para casos en los que se identifiquen filtraciones, accesos no autorizados o vulneraciones éticas en los sistemas.

La guía contempla cuatro fases:

- contención del incidente,
- notificación a las autoridades competentes y a los titulares de los datos
- remediación técnica y organizativa,
- revisión y prevención futura mediante auditoría y actualización del sistema.

Modelo de consentimiento informado para entornos automatizados:

Documento estandarizado, claro y comprensible, orientado a garantizar que los titulares de los datos comprendan el uso, alcance, riesgos y derechos asociados al tratamiento de su información biométrica. Este modelo está diseñado para ser accesible a diversos niveles educativos y puede presentarse en formatos multimodales (texto, audio, visual) según el contexto de implementación.

Fichas de Instrumento de apoyo

Las herramientas que se presentan a continuación constituyen un conjunto de instrumentos destinados a facilitar la evaluación ética, técnica y regulatoria de los sistemas de reconocimiento facial desarrollados mediante redes neuronales. Su construcción se basa en un análisis comparativo de los estudios científicos revisados en el Capítulo IV, integrando resultados empíricos y directrices metodológicas.

El objetivo de estos instrumentos es permitir una evaluación estructurada y objetiva del grado de cumplimiento de principios esenciales como la confidencialidad, la transparencia, la minimización de datos y la seguridad, así como proporcionar orientación para la respuesta a incidentes y la obtención del consentimiento informado en contextos automatizados.

En conjunto, estas contribuciones buscan fortalecer los procesos de diseño, auditoría y supervisión institucional, proporcionando así una base práctica para la implementación de sistemas biométricos que respeten los derechos de los interesados y cumplan con los estándares éticos y técnicos reconocidos internacionalmente.

Tabla 19 Evaluación Ética y Técnica

Dimensión	Indicador / Evaluación
Privacidad de los datos personales	¿El sistema emplea cifrado y anonimización? • Cifrado (36%) • Anonimización (24%)
Consentimiento informado	¿Se informa y obtiene consentimiento de los titulares? • Sólo en 20% de estudios
Justificación del tratamiento biométrico	¿Se valida la necesidad del uso de datos biométricos? • En estudios internacionales predominan medidas técnicas justificadas (34%)
Entorno de aplicación	¿Es un entorno controlado o público? • Controlado: mayor precisión (90–100%) • Público: menor precisión (75–90%)
Evaluación técnica	¿Qué algoritmos se utilizan y qué precisión se alcanza? • CNN (60%), GAN (20%), RNN (10%)

Nota. Elaborada por los autores a partir de un análisis comparativo de los estudios científicos nacionales e internacionales, esta tabla ofrece una visión estructurada del nivel de cumplimiento ético y técnico de los sistemas de reconocimiento facial, destacando aspectos como la aplicación de técnicas de anonimización, la obtención del consentimiento informado y la precisión en función del entorno de uso.

Tabla 20 Matriz de Cumplimiento

Principio / Criterio	Cumplimiento	Justificación según estudios	Observaciones
Minimización de datos	Media	24% aplica anonimización	Debe fortalecerse en estudios locales
Seguridad técnica	Alta	36% utiliza cifrado de datos	Estudios internacionales tienen mejores prácticas
Transparencia	Baja	Pocas referencias al consentimiento informado	Necesidad de informar al usuario
Evaluación de impacto	Media	En propuestas metodológicas del 20%	Incipiente en Ecuador
Responsabilidad proactiva	Baja	Débil adopción de mecanismos de revisión	Se sugiere guía técnica de verificación

Nota. Elaborada por el autor a partir de la sistematización de los criterios observados en los estudios analizados, esta matriz permite evaluar el nivel de cumplimiento de los principios fundamentales relativos a la protección de datos personales en los sistemas de reconocimiento facial, incluyendo los aspectos de minimización, seguridad, transparencia y rendición de cuentas institucional. La evaluación cualitativa y cuantitativa refleja tanto los avances logrados a nivel internacional como las brechas regulatorias y técnicas en el contexto local.

Tabla 21 Guía de Intervención ante Incidentes de Seguridad

Fase	Acciones sugeridas
Detección	Monitorear precisión del sistema en entornos dinámicos (controlado vs. público)
Contención	Desconectar acceso a bases biométricas ante incidentes
Análisis	Verificar si el sistema tenía medidas de cifrado activas
Notificación	Informar a los titulares si hay brecha de seguridad (según índice de impacto)
Corrección	Ajustar configuración del algoritmo o cambiar modelo (CNN → GAN si es necesario)

Nota. Elaborada por los autores con base en las mejores prácticas para la gestión de riesgos en sistemas biométricos, esta guía establece un protocolo de respuesta ante

incidentes de seguridad relacionados con sistemas de reconocimiento facial, estructurado en cinco fases clave: detección, contención, análisis, notificación y remediación. Su objetivo es minimizar el impacto de las brechas, proteger los derechos de los titulares de los datos y fortalecer la resiliencia de los sistemas.

Tabla 22 Modelo de Consentimiento Informado para Entornos Automatizados

Elemento	Contenido mínimo sugerido
Identificación del responsable	Nombre institucional, datos de contacto
Finalidad del tratamiento	Reconocimiento facial con fines de control o autenticación
Tipo de datos tratados	Imagen facial, metadatos contextuales
Derechos del titular	Acceso, rectificación, oposición, eliminación
Medidas de protección	Cifrado, anonimización, revisión de precisión

Nota. Elaborada por los autores con base en el análisis de las mejores prácticas regulatorias y técnicas descritas los elementos mínimos que debe contener un formulario de consentimiento informado apto para entornos automatizados que utilizan reconocimiento facial. El objetivo es garantizar que los interesados comprendan claramente la finalidad del tratamiento, sus derechos, el tipo de datos recopilados y las garantías implementadas, promoviendo así la transparencia y el respeto a la autodeterminación informativa.

Validación práctica de la propuesta

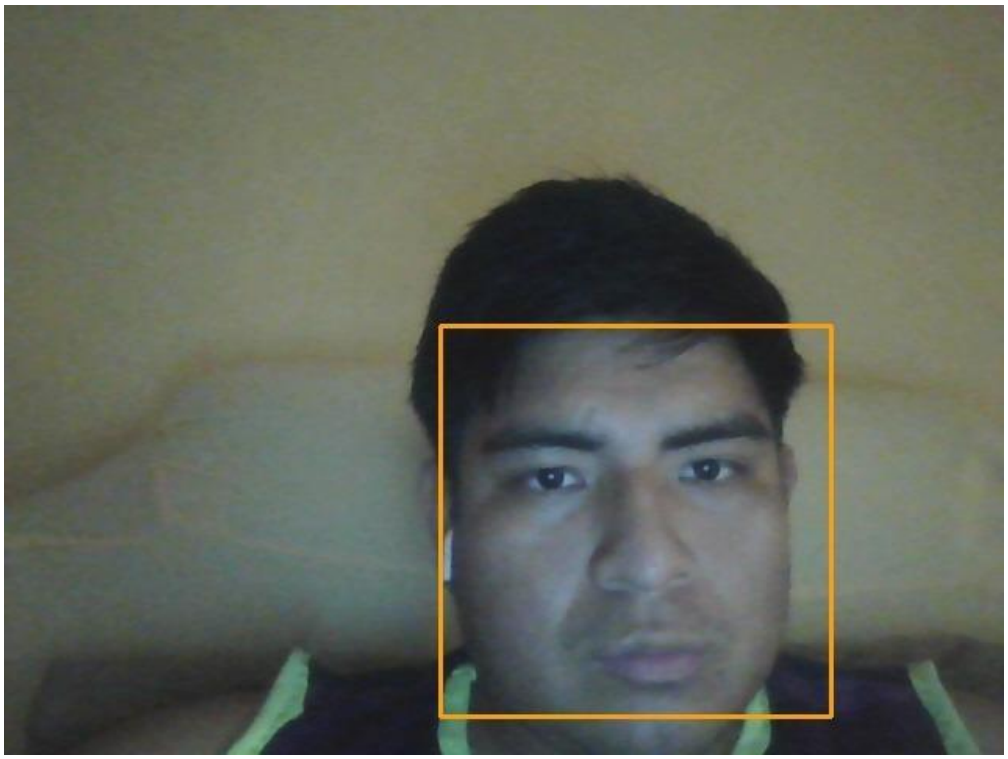
Con el fin de comprobar la aplicabilidad de la metodología propuesta, se realizó una práctica experimental utilizando programación en Python. A través de un sistema prototipo, se implementaron funciones para la captura de imágenes faciales, la generación de consentimientos informados automáticos y la creación de reportes técnico-normativos. Dichos reportes incluyeron indicadores de iluminación, nitidez y encuadre, los cuales fueron evaluados mediante métricas predefinidas y contrastados con los rangos recomendados en la literatura técnica y normativa.

El desarrollo de esta práctica permitió verificar que los componentes metodológicos, en particular la integración del enfoque CLASP y las directrices de la norma ISO/IEC 23894:2023, pueden ser aplicados de manera efectiva a nivel técnico.

Asimismo, se demostró que es posible automatizar la detección de condiciones mínimas de calidad en los procesos de captura y almacenamiento de datos biométricos, lo que contribuye a una validación más objetiva y transparente.

De esta manera, la validación práctica respalda la pertinencia de la propuesta metodológica, mostrando que no solo es teóricamente coherente, sino que también puede materializarse en herramientas aplicables a contextos académicos e institucionales, favoreciendo la reproducibilidad y la evaluación responsable de sistemas de reconocimiento facial.

Gráfico 10 Captura experimental en Python durante la práctica de validación



Nota. Elaboración propia como evidencia de la práctica experimental realizada en el marco de la propuesta metodológica.

Tabla 23 Resultados de riesgos técnico-normativos de la práctica experimental

Riesgo	Severidad	Probabilidad	Nivel	Explicación
Iluminación adecuada	0.2	0.3	0.06	Brillo promedio 122.4. Dentro del rango recomendado (90–180).
Nitidez adecuada	0.2	0.3	0.06	Varianza del Laplaciano 142.8. En el rango esperado (120–250).
Encuadre adecuado	0.2	0.3	0.06	Cobertura facial promedio 23.8%. En el rango recomendado (15–35%).

Nota. Elaborada por los autores a partir de la práctica realizada en Python, esta tabla muestra los valores técnicos obtenidos en la validación práctica, comparados con rangos normativos recomendados.

Conexión entre propuesta y validación

La práctica experimental confirma que los lineamientos teóricos planteados en la propuesta en particular la integración del enfoque CLASP y de la norma ISO/IEC 23894:2023 pueden trasladarse a un prototipo funcional. Esto demuestra que la propuesta no se limita a un planteamiento conceptual, sino que ofrece una ruta viable para la implementación de sistemas de reconocimiento facial responsables y auditables en contextos académicos e institucionales.

Conclusiones de la propuesta

- La metodología integra seguridad y cumplimiento regulatorio desde el diseño, reduciendo riesgos éticos y técnicos.
- La validación práctica mostró que es posible automatizar indicadores de calidad alineados con estándares internacionales.
- El modelo es replicable en entornos académicos y constituye una base sólida para futuros estudios en inteligencia artificial y protección de datos biométricos.

Recomendaciones a partir de la validación práctica

- **Metodológicas:** aplicar CLASP + ISO/IEC 23894:2023 en otras tecnologías biométricas (huella, iris).
- **Académicas:** incluir prácticas de programación en Python y reportes técnico-normativos en cursos de ciberseguridad e IA.

- **Prácticas:** implementar prototipos similares en instituciones públicas y educativas para auditar calidad y seguridad antes de un despliegue real.

Cierre del capítulo

La propuesta metodológica presentada articula teoría y práctica para demostrar que es posible diseñar, evaluar e implementar sistemas de reconocimiento facial responsables y seguros. La validación documental con estudios previos y la validación práctica mediante un prototipo en Python confirman la pertinencia y aplicabilidad del modelo, ofreciendo un marco replicable y sostenible que garantiza la protección de los derechos de los usuarios y la transparencia en el uso de datos biométricos.

CONCLUSIONES

- La implementación de redes neuronales en sistemas de reconocimiento facial en espacios públicos tiene un impacto directo en la privacidad, debido al procesamiento de datos biométricos sensibles que requieren un alto nivel de protección.
- Existe una estrecha relación entre la privacidad y la regulación, lo que pone de relieve la necesidad de una regulación eficaz. Sin embargo, se observa una relación débil entre la privacidad y la precisión, lo que refleja una tensión entre el progreso tecnológico y la protección de los derechos.
- La precisión de los sistemas es mayor en entornos controlados (90-100%) y disminuye en espacios públicos (75-90%), lo que aumenta el riesgo de errores y violaciones.
- Las redes neuronales convolucionales (CNN) son las más utilizadas (60%). Sin embargo, el cifrado (36%) y la anonimización (24%) no se utilizan ampliamente, y el consentimiento informado solo se menciona en el 20% de los estudios.
- Si bien el enfoque CLASP y la norma ISO/IEC 23894:2023 ofrecen herramientas útiles para la gestión de riesgos y la protección de datos, su adopción sigue siendo limitada, especialmente en Ecuador.
- En el ámbito nacional, pese a contar con un marco legal basado en el RGPD y la LOPDP, persisten obstáculos como la ausencia de comités de protección de datos y la escasa capacitación institucional.
- La validación práctica realizada en Python demostró que las directrices metodológicas propuestas pueden traducirse en un sistema funcional, demostrando la viabilidad de automatizar las mediciones de calidad (iluminación, nitidez y encuadre) y generar informes técnicos y regulatorios útiles para la trazabilidad.
- En general, la propuesta metodológica integra teoría y práctica, demostrando un modelo reproducible que garantiza una mayor seguridad, ética y cumplimiento normativo en el desarrollo de sistemas de reconocimiento facial.

RECOMENDACIONES

Desde una perspectiva metodológica:

- Aplicar la metodología combinada CLASP + ISO/IEC 23894:2023 en otras tecnologías biométricas (como huella digital o iris) para evaluar su aplicabilidad en distintos contextos.
- Explorar el uso de inteligencia artificial explicable (XAI/IAA) como mecanismo de transparencia y confianza en algoritmos biométricos.
- Replicar prácticas experimentales en Python u otros entornos de programación para validar la metodología en diferentes escenarios de prueba.

Desde una perspectiva académica:

- Incorporar asignaturas y proyectos prácticos que integren captura de datos biométricos, programación en Python y reportes técnico-normativos, fortaleciendo competencias en ciberseguridad e inteligencia artificial.
- Promover investigaciones interdisciplinarias que articulen aspectos técnicos, legales y éticos, utilizando la propuesta metodológica como guía replicable en tesis o proyectos institucionales.

Desde una perspectiva práctica:

- Establecer en Ecuador comités de protección de datos, con base en la LOPDP, para garantizar la vigilancia y cumplimiento en proyectos biométricos.
- Implementar prototipos de auditoría similares al desarrollado en la práctica experimental, de modo que instituciones públicas y educativas puedan verificar la calidad y seguridad de los sistemas antes de su despliegue real.
- Fortalecer protocolos de incidentes de seguridad, formularios claros de consentimiento informado y la generación automática de reportes técnico-normativos como parte de la rendición de cuentas institucional.

BIBLIOGRAFIA

ASAMBLEA LEGISLATIVA DEL DISTRITO FEDERAL. (2021). DECRETO POR EL QUE SE EXPIDE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DE LA CIUDAD DE MÉXICO. *A G.O.C.D.M.X.*, 61.

Asamblea Nacional. (2021). *LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES*. https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Biometric Security: How Secure Is It Really? (2019, junio 8). https://www.covesmart.com/es/resources/home-safety/biometrics-a-guide-to-biometric-security/?srsltid=AfmBOoojWaoOXCyhixo0ehnCkLgg1rdluheyaGvve31uo14o0Xaq8074

BPONE. (2023, noviembre 15). Ecuador: Reglamento de la Ley Orgánica de Protección de Datos Personales (Decreto No. 904). *BPONE The Best Professional Outsourcing*. https://bp-one.com/ecuador-reglamento-de-la-ley-organica-de-proteccion-de-datos-personales-decreto-no-904/

Conoce la Ley Estadounidense de Privacidad y Protección de Datos. (s. f.). *Kiteworks | Your Private Data Network*. Recuperado 7 de agosto de 2025, de https://www.kiteworks.com/es/glosario-riesgo-cumplimiento/american-data-privacy-protection-act/

Diario Oficial de la Unión Europea (Ed.). (2016). *REGLAMENTO (UE) 2016/ 679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO*. 88.

El equipo de Veesion. (2023, diciembre 28). ¿Qué es la vigilancia biométrica? *Veesion*. https://veesion.io/es/que-es-la-vigilancia-biometrica/

Facial Liveness Detection Whitepaper Spanish. (s. f.). *ID R&D*. Recuperado 5 de agosto de 2025, de https://www.idrnd.ai/facial-liveness-detection-whitepaper-spanish/

Gallo, J., & Egas, A. (2024, diciembre 2). *Nuevo reglamento de la ley de Protección de Datos Personales*. https://www.dentons.com/es/insights/articles/2024/december/2/nuevo-reglamento-de-la-ley-de-proteccion-de-datos-personales

Gárate Briones, E. A. (2020). MAGÍSTER EN SISTEMAS DE INFORMACIÓN GERENCIAL. *Escuela Superior Politecnica del Litoral*, 58.

Gestor Normativo. (2012). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Gómez Cruz, F., & Jiménez Valero, J. S. (2020). ARQUITECTURA DE SOFTWARE PARA LA APLICACIÓN DE TÉCNICAS DE RECONOCIMIENTO FACIAL A TRAVÉS DE DISPOSITIVOS IOT. *Universidad Catolica de Colombia*, 66.

Gutiérrez, B. V. (2021). *Desarrollo seguro de software bajo la metodología DevSecOps*. 99.

Hernández Sampieri, R., & Fernández Collado, C. F. (2014). *Metodología de la investigación* (P. Baptista Lucio, Ed.; Sexta edición). McGraw-Hill Education. https://apiperiodico.jalisco.gob.mx/api/sites/periodicooficial.jalisco.gob.mx/files/metodologia_de_la_investigacion_-_roberto_hernandez_sampieri.pdf

Ley de comercio electrónico, firmas electrónicas y mensajes de datos. (s. f.). https://www.firmadigital.gob.ec/wp-content/uploads/2018/01/reglamento_ley_de_comercio_electronico.pdf

Ley de Protección de Datos de Francia: Una Visión General de la Privacidad de Datos en Francia. (s. f.). *Kiteworks | Your Private Data Network*. Recuperado 7 de agosto de 2025, de https://www.kiteworks.com/es/glosario-riesgo-cumplimiento/french-data-protection-act/

Leyes de protección de datos en Alemania—Leyes de protección de datos del mundo. (2018). https://www.dlapiperdataprotection.com/index.html?t=law&c=DE

Leyes de protección de datos en Brasil—Leyes de protección de datos del mundo. (2020). https://www.dlapiperdataprotection.com/index.html?t=law&c=BR

Leyes de protección de datos en Italia—Leyes de protección de datos del mundo. (2018). https://www.dlapiperdataprotection.com/index.html?t=law&c=IT

Martínez Guerrero, M. (2018). Reconocimiento facial para la autentificación de usuarios. *Ingeniería del agua*, *18*, 34. https://doi.org/10.4995/ia.2014.3293

Molina, F. S. (2022). *La Inteligencia Artificial y su incidencia en las comunicaciones*. 12.

Monforte, E. (2022, junio 27). Datos biométricos: Qué son y para qué se utilizan. *Camerfirma*. https://www.camerfirma.com/datos-biometricos-que-son-para-que-se-utilizan/

O que é deep learning? | SAP. (2024, junio 10). https://www.sap.com/brazil/resources/what-is-deep-learning

Peñaherrera Plúa, J. P., & Triviño Quiñonez, J. E. (2024). Diseño de un sistema de reconocimiento facial para acceso a áreas restringidas utilizando visión artificial y redes neuronales. *Universidad Politécnica Salesiana del Ecuador*, 44.

Peralta-Díaz, F. (2025). *SUPERINTENDENTE DE PROTECCIÓN DE DATOS PERSONALES*. 4.

Pérez Lorenzo, I. (2023). RECONOCIMIENTO FACIAL A TRAVÉS DE DEEP LEARNING. *Universidad Rey Juan Carlos*, *56*. https://burjcdigital.urjc.es/server/api/core/bitstreams/b9c72452-fdc9-4cdc-b9ff-f4df663e461b/content

PIPEDA: Canada's Privacy And Data Protection Law. (s. f.). *Consent Management Platform (CMP) Usercentrics*. Recuperado 7 de agosto de 2025, de https://usercentrics.com/knowledge-hub/canada-personal-information-protection-and-electronic-documents-act-pipeda/

¿Qué es el reconocimiento facial? - Explicación del software de reconocimiento facial y análisis facial - AWS. (s. f.). [Aws]. Amazon Web Services, Inc. Recuperado 4 de agosto de 2025, de https://aws.amazon.com/es/what-is/facial-recognition/

¿Qué es la autenticación biométrica? Casos de uso, ventajas y desventajas | OneSpan. (s. f.). Recuperado 5 de agosto de 2025, de https://www.onespan.com/topics/biometric-authentication

¿Qué es la Equidad Algorítmica? - Términos y Definiciones de Ciberseguridad. (s. f.). Recuperado 5 de agosto de 2025, de https://www.vpnunlimited.com/es/help/cybersecurity/algorithmic-fairness

¿Qué son las redes neuronales convolucionales? | IBM. (2021, octubre 6). https://www.ibm.com/es-es/think/topics/convolutional-neural-networks

Reglamento codigo organico economia docial de los conocimiento. (2017). 17.

Rodriguez Ponce, K. J., Gutierrez Sanchez, F. J., & Mendoza De los Santos, A. C. (2024). Sistema de control de acceso biométrico mediante reconocimiento facial con técnicas de vivacidad. *Innovation and Software*, *5*(2), Article 2. https://doi.org/10.48168/innosoft.s16.a179

Rouhiainen, L. (2018). *Inteligencia artificial: 101 cosas que debes saber hoy sobre nuestro futuro* (Sexta edición). Alienta Editorial. https://planetadelibrosar0.cdnstatics.com/libros_contenido_extra/40/39307_Inteligencia_artificial.pdf

Santos Chavez, J. J. (2024, febrero 9). *4 Buenas Prácticas de Desarrollo Seguro de Software*. https://www.deltaprotect.com/blog/desarrollo-seguro-de-software

Simón Chico, J. (2021). *Sistemas de Reconocimiento Facial basados en Redes Neuronales Convolucionales usando Información de Género y Raza* [bachelorThesis]. https://repositorio.uam.es/handle/10486/701293

Stryker, C., & Kavlakoglu, E. (2024, agosto 9). *¿Qué es la Inteligencia Artificial (IA)? | IBM*. https://www.ibm.com/es-es/think/topics/artificial-intelligence

Travieso, C. M., Solé-Casals, J., Zaiats, V., Alonso, J. B., & Ferrer, M. A. (2008). *REDUCCIÓN DEL VECTOR DE CARACTERÍSTICAS EN RECONOCIMIENTO FACIAL*. 4.

Verma, U. (2024, enero 5). *Algorithmic Bias: What It Is and Why It Matters*. Built In. https://builtin.com/data-science/auditing-algorithms-data-science-bias

Vilches, C. (2024, enero 5). *Biblioguias: Gestión de datos de investigación: Protección de los datos*. https://biblioguias.cepal.org/c.php?g=495473&p=4398118

What Is a Spoofing Attack? Detect and Prevent. (s. f.). *Arkose Labs*. Recuperado 5 de agosto de 2025, de https://www.arkoselabs.com/explained/what-is-a-spoofing-attack/

ISO. (2023). *Information technology — Artificia intelligence — Guidance on risk management.* Informe, Switzerland . Recuperado el 07 de Agosto de 2025, de https://cdn.standards.iteh.ai/samples/77304/cb803ee4e9624430a5db177459158b24/ISO-IEC-23894-2023.pdf

(2023). *REGLAMENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE.* Asamblea Nacional, Quito. Recuperado el 07 de Agosto de 2025, de https://www.cosede.gob.ec/wp-content/uploads/2023/12/REGLAMENTO-GENERAL-A-LA-LEY-ORG%C3%81NICA-DE-PROTECCION-DE-DATOS-PERSONALES_compressed-1.pdf

ANEXOS

CERTIFICADO DE ANÁLISIS DE COINCIDENCIA NO ACCIDENTAL

LIC. EDGAR RIVADENEIRA EN CALIDAD DE DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR,

CERTIFICA

Que el trabajo de integración curricular denominado "**IMPACTO DE REDES NEURONALES PARA RECONOCIMIENTO FACIAL EN LA SEGURIDAD DE LA INFORMACIÓN**", presentado por **Edwin Leonel Belduma Belduma** estudiantes de la **carrera de Software** pasó el análisis de coincidencia no accidental en la herramienta TURNITIN, reflejando un **porcentaje de similitud del 2%**, como se puede evidenciar en el documento adjunto.

Guaranda, 12 de Agosto del 2025

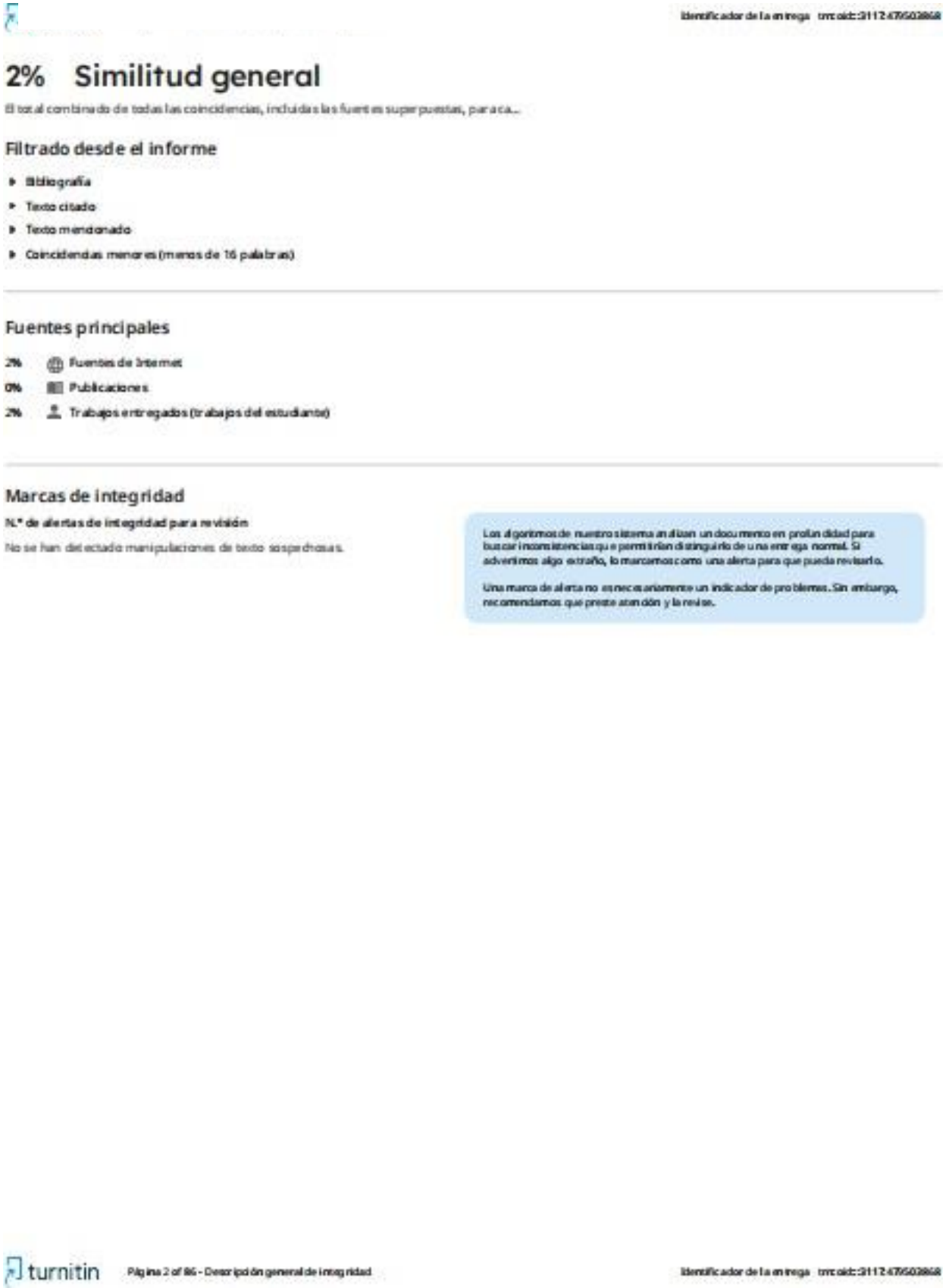
Atentamente,

Firmado electrónicamente por:
EDGAR PATRICIO
RIVADENEIRA RAMOS
Validar únicamente con FirmaEC

Lic. Edgar Rivadeneira
Director

DOCUMENTO EMITIDO AUTOMÁTICAMENTE POR EL SISTEMA TURNITIN

Gráfico 11 Reporte de similitud de Turnitin



Identificador de la entrega trn:oid:3112:479502868

2% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Texto mencionado
- Coincidencias menores (menos de 16 palabras)

Fuentes principales

2%	Fuentes de Internet
0%	Publicaciones
2%	Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

turnitin Página 2 of 86 - Descripción general de integridad

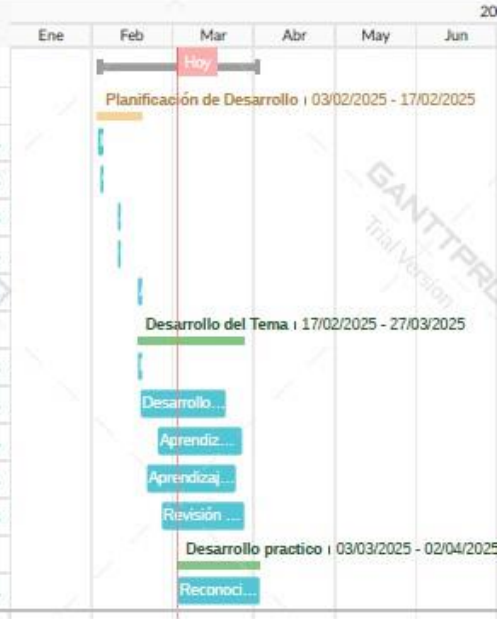
Identificador de la entrega trn:oid:3112:479502868

CRONOGRAMA (GANNT)

Gráfico 12 Cronogramas de Actividades para la elaboración del Proyecto

Ueb | Anteproyecto

	Nombre de tarea	Asignado	Fecha de in	Fecha final	Estado
			03/02/202	02/04/202	
1	**Planificación de Desarrollo**		03/02/202	17/02/202	
1.1	Investigación del Tema	sin asignar	03/02/202	04/02/202	Abierto
1.2	Consulta de documentos pertinentes	sin asignar	04/02/202	04/02/202	Abierto
1.3	Análisis del tema con el director	sin asignar	10/02/202	10/02/202	Abierto
1.4	Cambios en la descripción del tema	sin asignar	10/02/202	10/02/202	Abierto
1.5	Aprobación del Tema	sin asignar	17/02/202	17/02/202	Abierto
2	**Desarrollo del Tema**		17/02/202	27/03/202	
2.1	Lectura Bibliografica sobre el tema	sin asignar	17/02/202	17/02/202	Abierto
2.2	Desarrollo del anteproyecto	sin asignar	18/02/202	20/03/202	Abierto
2.3	Aprendizaje de redes neuronales par...	sin asignar	24/02/202	26/03/202	Abierto
2.4	Aprendizaje de python y framework	sin asignar	20/02/202	24/03/202	Abierto
2.5	Revisión del anteproyecto	sin asignar	25/02/202	27/03/202	Abierto
3	**Desarrollo practico**		03/03/202	02/04/202	
3.1	Reconocimiento Facial desarrollado ...	sin asignar	03/03/202	02/04/202	Abierto



Nota. Elaborado por el autor con base en la planificación estructurada del proyecto de investigación, el cronograma presenta las tareas principales y subtareas, divididas en tres fases: planificación del desarrollo, desarrollo temático y desarrollo práctico, especificando las fechas de inicio y finalización, así como el progreso. La herramienta utilizada permite visualizar la duración estimada y la secuencia lógica de las actividades, facilitando así la gestión del tiempo y el seguimiento del logro de los objetivos.

PRESUPUESTO EJECUTADO

Tabla 24 Propuesta para la elaboración del proyecto de titulación

Descripción	Cantidad	Valor Unitario ($)	Total ($)
Computadora portátil	1	890	890
Impresora	1	280	280
Acceso a bases de datos académicas	1	50	50
Insumos de trabajo (cuadernos, lápices, impresiones)	8	5.00	40
Movilización	5	20	100
Servicios de suscripción a herramientas de IA o análisis de datos	1	20	20
Cursos en línea	1	50	50
Gastos adicionales e imprevistos	1	100	100
Total General	-	-	**1530**

Nota. Elaborado por el autor con base en una estimación básica de los recursos necesarios para desarrollar el proyecto final. Los detalles incluyen costos relacionados con equipo tecnológico, acceso a información académica, materiales de trabajo, viajes, suscripciones especializadas y posibles imprevistos. El presupuesto total es de $1,530, lo que permite una planificación financiera adecuada para asegurar la finalización de las actividades planificadas.

ANÁLISIS CUANTITATIVO Y ESTADÍSTICO EN EL RECONOCIMIENTO FACIAL

Gráfico 13 Análisis de enfoques y medidas de protección en estudios de reconocimiento facial

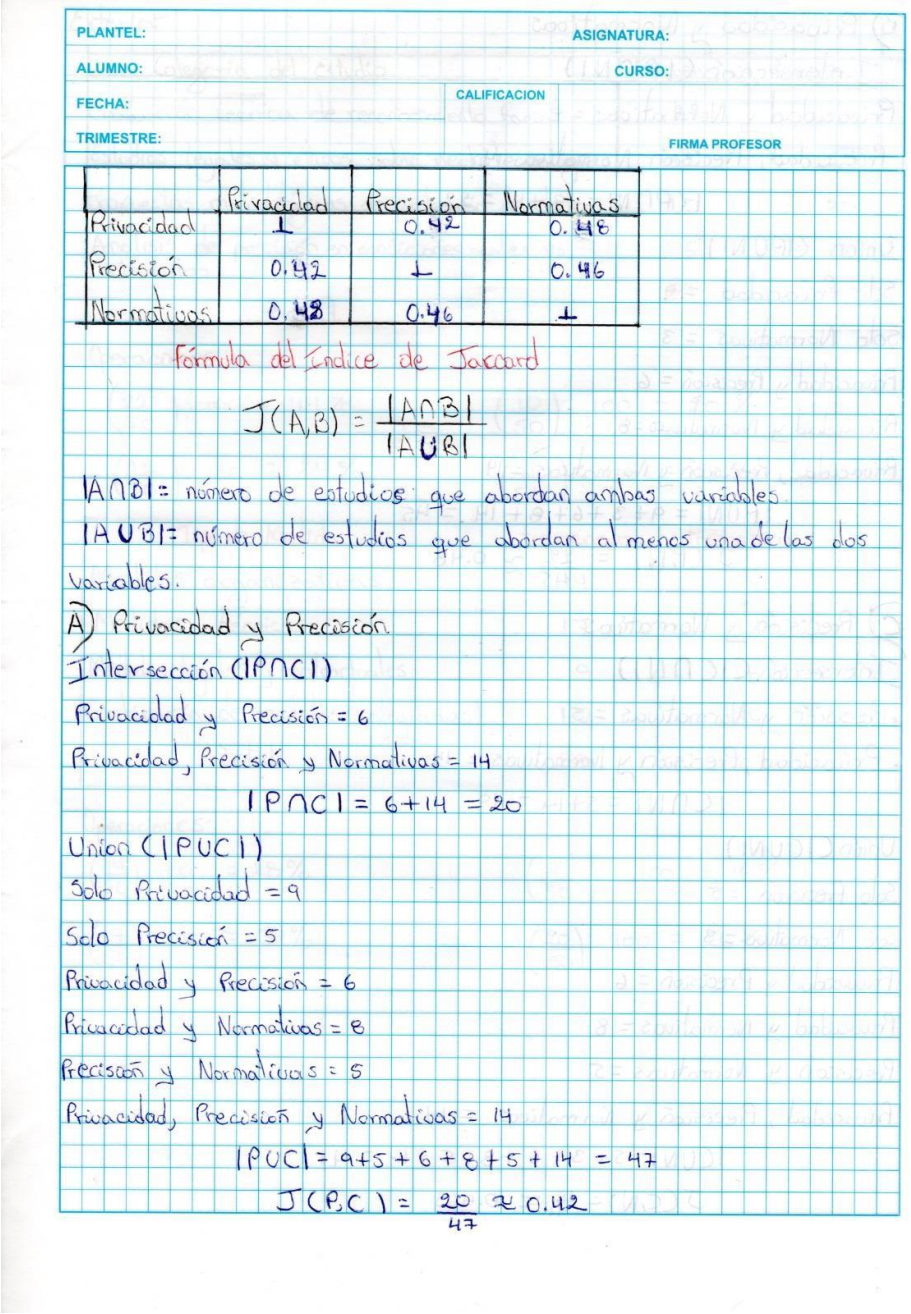


Área de Enfoque	Porcentaje (%)	Número de estudios (de 50)
Privacidad y protección de datos personales	50	25
Retos técnicos y precisión de sistemas	30	15
Aspectos normativos y éticos	20	10
Total	**100**	**50**

Medida de Protección	Porcentaje (%)	Número de estudios (de 50)
Cifrado de datos	36	18
Anonimización de datos	24	12
Consentimiento informado	20	10

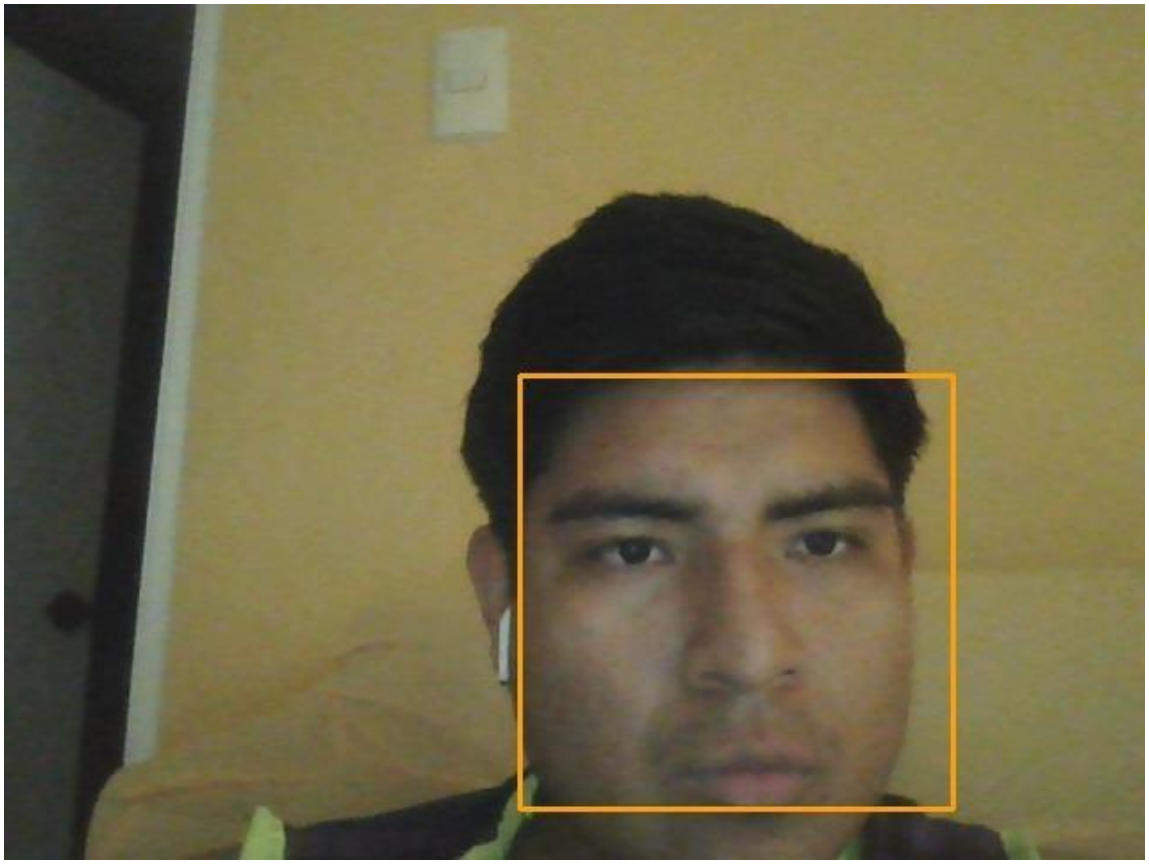
Nota: Elaborado por el autor con Microsoft Excel. El gráfico circular representa la categorización de 50 estudios científicos según su área de interés: confidencialidad de datos personales, precisión técnica y aspectos regulatorios. A continuación, se presentan las salvaguardas identificadas, calculadas con base en frecuencias relativas y porcentajes. Este análisis visualiza las tendencias predominantes en el uso de técnicas como el cifrado, la anonimización y el consentimiento informado, facilitando así la interpretación cuantitativa y cualitativa de la evidencia revisada.

Gráfico 14 Cálculo del índice de Jaccard aplicado a estudios sobre privacidad, precisión y regulación



Nota. Esta imagen elaborada por el autor, cálculo manual del índice de Jaccard, utilizado para medir el grado de similitud entre los estudios revisados que abordan cuestiones de confidencialidad, precisión y aspectos regulatorios. El análisis identifica el número de estudios que comparten dos o más de estas variables y los compara con el número total de estudios que abordan al menos una de ellas. Este procedimiento permite una evaluación más precisa de la superposición temática entre los enfoques abordados en los trabajos analizados, aportando así rigor estadístico y metodológico a la investigación.

Gráfico 15 Evidencia práctica de detección facial mediante programación



Nota: Elaborado por el autor, la figura presenta la detección automática de un rostro mediante el sistema de reconocimiento facial desarrollado en Python y OpenCV, donde se observa el encuadre del rostro resaltado con un rectángulo de color. Esta evidencia forma parte de las pruebas experimentales realizadas para validar el correcto funcionamiento del algoritmo.

Gráfico 16 Evaluación práctica de riesgos técnico-normativos en el procesamiento de imágenes

Riesgos Técnico-Normativos

Riesgo	Severidad	Probabilidad	Nivel	Explicación
Iluminación adecuada	0.2	0.3	0.06	Brillo promedio 122.4. Dentro del rango recomendado (90–180).
Nitidez adecuada	0.2	0.3	0.06	Varianza del Laplaciano 142.8. En el rango esperado (120–250).
Encuadre adecuado	0.2	0.3	0.06	Cobertura facial promedio 23.8%. En el rango recomendado (15–35%).

Nota: Elaborado por el autor, presenta los resultados de la práctica de programación aplicada a la evaluación de imágenes, mostrando que los parámetros de iluminación, nitidez y encuadre se mantienen dentro de los rangos recomendados. Esto evidencia que el proceso cumple con condiciones técnicas aceptables.