UNIVERSIDAD SANTO TOMAS
PRIMER CLAUSTRO UNIVERSITARIO DE COLOMBIA
T U N J A

Desafíos éticos y normativos de la Autenticación biométrica con Inteligencia Artificial

PROPONENTE(S)

Juan Felipe Villanueva Arias

DIRECTOR

Martha Susana Contreras Ortiz

Tunja

Fecha de presentación (02 / 06 / 2026)

CONTENIDO

1. FICHA TÉCNICA DEL PROYECTO

Título	**Desafíos éticos y normativos de la Autenticación biométrica con Inteligencia Artificial**
Nombre Estudiante Correo electrónico estudiante Director Lugar de ejecución del proyecto Duración	Juan Felipe Villanueva Arias Juan.villanueva@usantoto.edu.co Martha Susana Contreras Ortiz Tunja 5 meses
Palabras claves	Autenticación biométrica, Inteligencia Artificial, Ciberseguridad, Normatividad, Desafíos éticos
Los abajo firmantes confirman que todos los datos incluidos en la presente propuesta son correctos y verídicos, que no incumplen ninguna ley o norma vigente (incluir nombres y firmas de estudiantes y director).	
Firma del autor Nombre autor: Juan Felipe Villanueva Arias Firma del director Nombre director del proyecto	

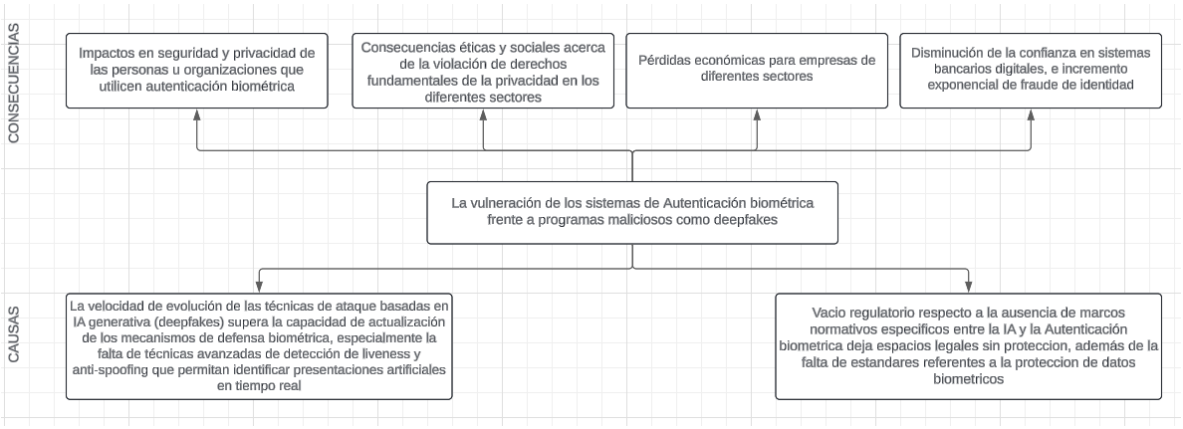
2. PLANTEAMIENTO DEL PROBLEMA

La principal cuestión que se aborda son las crecientes vulnerabilidades de los sistemas de autenticación biométrica frente a las capacidades emergentes de la Inteligencia Artificial, esto generando a su vez desafíos éticos y normativos sin precedentes que comprometen la integridad, privacidad y confianza en estos sistemas de seguridad.

En esencia esta problemática radica en que mientras que la autenticación biométrica se ha posicionado como una solución por así decirlo “infalible”, existen sistemas de vulneración especialmente las tecnologías de deepfakes y o síntesis biométrica que han demostrado a su vez que estos sistemas pueden ser comprometidos de manera sofisticada creando una gran problemática. Se puede resaltar que la autenticación biométrica se basa en características únicas e inmutables del ser humano como reconocimiento fácil, reconocimiento ocular, huella dactilar, entre otras.

Aunque existe la creencia que los sistemas de autenticación biométrica son los más seguros, se ha demostrado que pueden ser vulnerados con la implementación de nuevas tecnologías. Sin embargo, en sectores como: el de salud, el judicial, el financiero y el educativo son ampliamente utilizados, para guardar grandes volúmenes de información confidencial. Si llegara a vulnerarse esta información se podrían generar consecuencias de seguridad y privacidad.

Figura 1. Árbol de problemas



Fuente: Autor

3. JUSTIFICACIÓN

Esta investigación es necesaria ya que los sistemas de autenticación biométrica representan la última línea de defensa en la protección de datos sensibles y la identidad digital de millones de personas, si se llegara a vulnerar; esta sería una crisis de confianza que amenazaría los cimientos de la seguridad digital moderna y podría tener terribles consecuencias.

La relevancia de esta investigación radica en que los sistemas biométricos han alcanzado un nivel de implementación masiva sin que exista realmente una comprensión completa de todas o la gran mayoría de sus vulnerabilidades emergentes. Mientras que sectores críticos como el banco, los hospitales, las instituciones educativas y la justicia han depositado su confianza en estas tecnologías como soluciones "infalibles", la realidad demuestra que pueden ser comprometidas por diversos programas sofisticados utilizando deepfakes y síntesis biométrica.

Este proyecto busca desarrollar un marco integral que permita:

- Identificar y categorizar las vulnerabilidades específicas de los sistemas biométricos frente a ataques basados en IA
- Proponer mecanismos de detección y mitigación de amenazas emergentes
- Establecer protocolos éticos y normativos para el desarrollo responsable de tecnologías biométricas
- Crear herramientas de evaluación de riesgo que permitan a las organizaciones tomar decisiones informadas

Cabe resaltar que los resultados de este trabajo tendrán impacto directo en múltiples niveles: técnico, al proporcionar herramientas para mejorar la robustez de los sistemas biométricos; normativo, al informar el desarrollo de regulaciones más efectivas entre otras

4. OBJETIVOS

4.1 Objetivo General

Evaluar los desafíos técnicos, éticos y normativos asociados a la implementación de sistemas de autenticación biométrica basados en inteligencia artificial, mediante el análisis de vulnerabilidades, arquitecturas de seguridad y marcos regulatorios, con el propósito de establecer lineamientos técnicos para su adopción segura y responsable en el sector educativo.

4.2 Objetivos específicos

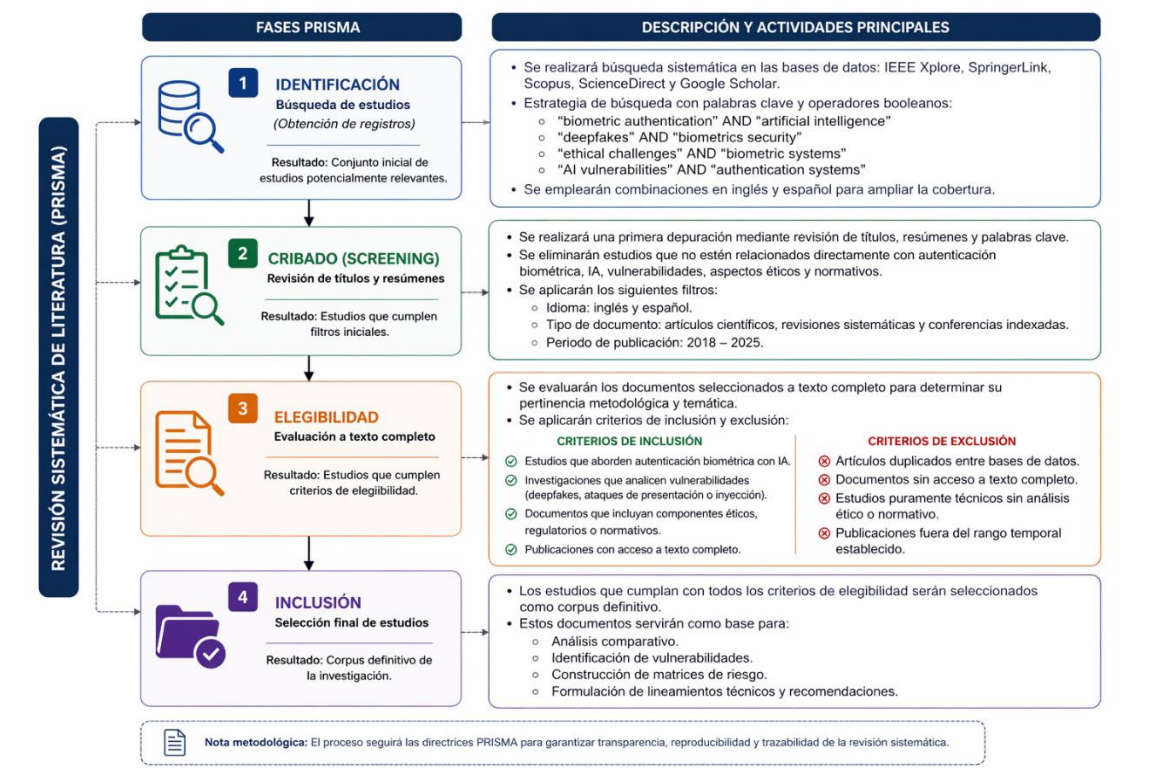
Nro.	Objetivos específicos
1	Analizar las vulnerabilidades técnicas y los riesgos asociados a los sistemas de autenticación biométrica con inteligencia artificial, a través de la revisión de arquitecturas de implementación, mecanismos de protección de datos y marcos regulatorios vigentes, para determinar sus implicaciones en la seguridad de la información y la protección de datos biométricos.
2	Comparar los riesgos y desafíos técnicos que enfrentan los sectores educativo, judicial, financiero y de salud, en la implementación de sistemas de autenticación biométrica con inteligencia artificial en algunos de sus procesos, mediante un análisis estructurado de amenazas, superficies de ataque y requerimientos de seguridad, para identificar diferencias en niveles de exposición y criticidad.
3	Proponer una guía de lineamientos técnicos y buenas prácticas para la implementación segura de sistemas de autenticación biométrica basados en inteligencia artificial, fundamentada en el análisis de vulnerabilidades, arquitecturas y requisitos normativos estudiados, con el fin de orientar al sector educativo en la mitigación de riesgos y el cumplimiento de estándares de seguridad y protección de datos.

5. METODOLOGÍA

PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) es una metodología estándar internacional que te guía paso a paso para hacer búsquedas bibliográficas de manera sistemática, transparente y reproducible. Es fácil de usar porque tiene una estructura clara y es la más utilizada mundialmente en investigación académica. (Page et al., 2021; *PRISMA Statement*, 2025) y sus principales características son:

- **Estructura simple**: Solo 4 fases principales
- **Perfecta para Scopus**: Diseñada específicamente para bases de datos académicas
- **Ampliamente aceptada**: Reconocida internacionalmente
- **Fácil documentación**: Lista de verificación clara
- **Ideal para tu tema**: Excelente para temas multidisciplinarios como biometría + IA + ética

Figura 2. Metodología Prisma



Fuente: Elaboración propia. Contenido metodológico del autor; diagramación generada con asistencia de ChatGPT (OpenAI).

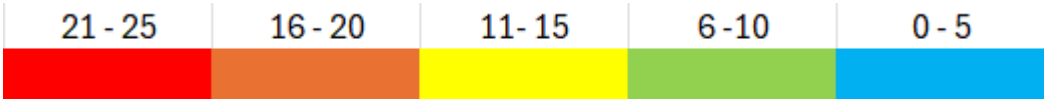
La metodología se desarrolló de la siguiente manera, como dice el diagrama primero se buscó todos los estudios relacionados en bases de datos de la universidad que a su vez fueron proporcionadas por el CRAI, siendo estas : IEEE, Spring, Scopus, Science Direct y Google Academic filtrándolos por palabras clave referentes a la monografía eliminando así los que no tienen relevancia con esta, posteriormente los resultados se filtraron nuevamente como lo dice el segundo paso “cribado”, donde se aplicaron diversos filtros como artículos en español y/o Ingles y siendo estos artículos no menores de 2018 hasta el 2025 excluyendo los artículos sin acceso a el texto completo, duplicados o documentos puramente técnicos sin componentes éticos o normativos, finalmente los mejores candidatos fueron incluidos en la monografía.

En la siguiente tabla se mostrarán los resultados esperados para cada objetivo específico de la monografía.

Tabla 1. Entregables asociados a cada objetivo especifico

Objetivo 1	Se realizará una matriz identificando las vulnerabilidades de los sistemas de autenticación biométrica con IA y las problemáticas que generan, como ataques de presentación e inyección digital, además de la identificación de las fallas de las arquitecturas de los diferentes procesos biométricos y una tabla de la relación entre la vulnerabilidad y el riesgo, a partir de la revisión bibliográfica de literatura.
Objetivo 2	Se realizará un cuadro comparativo técnico para los sectores: educativo: judicial, médico y financiero; además de la identificación de las amenazas diferenciadas y la realización de una tabla de riesgos clasificando su criticidad.
Objetivo 3	Se realizará un documento guía sobre el sector educativo que incluye: una matriz de autenticación remota además de un modelo de control de acceso físico al campus con múltiples niveles de seguridad biométrica, y recomendaciones de arquitectura para el almacenamiento seguro de datos en la nube, todo adaptado a distintos niveles de presupuesto institucional y de cumplimiento del marco normativo GDPR.

Para las tablas de las matrices se utilizará una guía de colores con el fin de identificar su nivel de criticidad desde el 5 hasta el 25 de la siguiente manera:



- **Rojo** significa que es Crítico y requiere una atención Inmediata o especial cuidado
- **Naranja** significa que es un problema mayor y igualmente requiere atención
- **Amarillo** significa que es una problemática moderada y esta debe ser revisada
- **Verde** significa que es una problemática menor y no requiere especial cuidado
- **Azul** significa que es una problemática insignificante y sin mayor cuidado

6. Desarrollo de la Investigación

En este capítulo se presentan las evidencias y el proceso seguido durante la investigación, organizando la información según el cumplimiento de cada objetivo

6.1 Objetivo 1 (Clasificación desafíos Éticos y normativos)

En este primer objetivo se desarrollará la clasificación de desafíos éticos y normativos con el fin de dar cumplimiento al primer objetivo propuesto en: Tabla 1. Entregables asociados a cada objetivo especifico.

6.1.1 Revisión sistemática de literatura sobre Ética biométrica

La revisión sistemática de literatura sobre ética biométrica ofrece un análisis fundamental para poder entender y comprender los desafíos que enfrenta la implementación de sistemas de autenticación biométrica en esta era de Inteligencia Artificial, esto a través de un exhaustivo análisis identificando así problemáticas críticas en cuestiones éticas sociales y legales.

La privacidad de los datos biométricos representa un gran desafío ético y uno de los más complejos y controvertidos en el campo de la autenticación digital, ya que, a diferencia de otros tipos de información personal, los datos biométricos poseen características únicas del ser humano que los hacen la mejor opción a la hora de guardar o proteger los datos más sensibles.

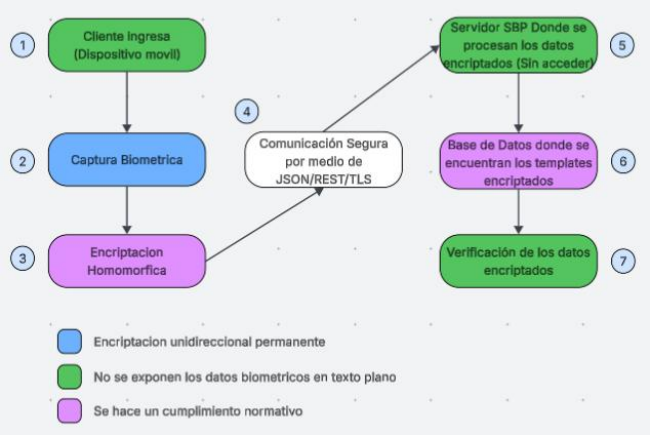
El Reglamento General de Protección de Datos (GDPR) de la Unión Europea, implementado en mayo de 2018 (Tanwar et al., 2019), clasifico los datos biométricos como “categoría especial de datos personales”. Esta clasificación se refiere precisamente a la naturaleza intrínseca de la información biométrica que como ya se mencionó a diferencia de las otras formas de protección de datos como contraseñas o números de identificación esta está vinculada directamente con las características físicas y únicas de cada individuo lo que la hace tan especial; además el GDPR establece que el procesamiento de datos biométricos está, en principio, prohibido, salvo que se cumplan condiciones excepcionales específicas, siendo la más relevante el consentimiento explícito y libre del titular de los datos que

como veremos más adelante parece indispensable el hecho de romper con esta regla a menos que se cuenten con las medidas y recursos necesarios.

El concepto de “Consentimiento informado” en el contexto biométrico presenta desafíos únicos. Según la literatura académica muchos de los usuarios no comprenden completamente las implicaciones de proporcionar sus datos biométricos ya que estos a diferencia de compartir un número telefónico o dirección de correo electrónico cuando una persona registra su huella dactilar por ejemplo está cediendo información que no puede ser modificada o reemplazada posteriormente por las empresas u organizaciones que recopilan y procesan estos datos biométricos

El estándar IEEE 2410 para la privacidad biométrica, desarrollado por la IEEE Standars Association (*IEEE SA - IEEE 2410-2021*, 2021a), proporciona un marco técnico y ético que nos puede a ayudar a afrontar estas problemáticas ya que el estándar nos especifica requisitos detallados para la implementación de técnicas para preservar la información, esto incluyendo técnicas de encriptado homomórfica, que nos permite realizar operaciones computacionales sobre datos encriptados sin necesidad de descifrarlos. Esta innovación tecnológica representa un gran avance porque aborda una de las vulnerabilidades a lo hora de almacenar los datos biométricos ya que usualmente se debe procesar datos biométricos en texto plano o con encriptación reversible convirtiéndolo en datos de fácil vulneración, pero ¿por qué? Pues porque las organizaciones ya no necesitan el acceso directo a los datos biométricos originales del usuario, lo que significa que incluso si una base de datos de una organización es comprometida por actores maliciosos, los datos biométricos seguirán estando encriptados ya que solo el usuario posee las claves criptográficas necesarias. A continuación, se presentará la arquitectura de la encriptación homomórfica simplificada

Figura 3. Encriptación Homomórfica



Fuente: Autor con referencias de:(IEEE SA - IEEE 2410-2021)

Sin embargo (*A Review of Privacy-Preserving Biometric Identification and Authentication Protocols - ScienceDirect*, 2025) publicada en Computers & Security (2025), nos dice que, aunque existen soluciones como la encriptación homomórfica mencionada anteriormente, su adopción en sistemas biométricos comerciales sigue siendo muy limitada esto debido a su elevado costo, la complejidad de su implementación y la falta de estándares.

La investigación (*Ethical Considerations in the Use of Facial Recognition for Public Safety – IEEE Public Safety Technology*, 2026) también nos revela una dimensión ética frecuentemente ignorada por muchos, hablo del concepto de “privacidad como derecho humano fundamental” versus “privacidad como commodity negociable”, ¿pero ¿qué es esto? Pues se trata de que muchas implementaciones comerciales de sistemas biométricos, especialmente en aplicaciones móviles y servicios en línea aparece la opción de “aceptar términos y condiciones de servicio” una opción que muchas veces nosotros pasamos por alto sin detenerse a leer de que trata, haciendo énfasis a la problemática es que estos servicios nos dan la opción de aceptar términos de servicio extensos que otorgan amplios permisos para recopilar y procesar nuestros datos biométricos, o renunciar completamente al servicio. Esta dinámica de "tómalo o déjalo" es éticamente problemática porque nos obliga en cierta forma de aceptar dichos términos para acceder a sus servicios, servicios que de no tener las correctas implementaciones mencionadas anteriormente podrían terminar por afectarnos, sin embargo cabe resaltar que no siempre se pide esta confirmación puesto que existen casos donde el reconocimiento facial puede ser capturado sin el conocimiento ni consentimiento de la persona esto desde grandes distancias convirtiendo así cada fotografía publica de una persona en un posible vulnerabilidad biométrica.

Además, no está de más y resulta evidente que algunas personas de poblaciones vulnerables deben de seguir una serie de pasos para cualquier sistema de recopilación de datos biométricos según (Kavanagh et al., 2019)

Esta revisión sistemática de literatura sobre ética biométrica nos evidencia que se atraviesa un momento crítico donde la tecnología ha avanzado más rápido de lo que los marcos éticos y regulatorios han sido para controlarla. Cabe destacar que estos datos biométricos son otra forma de información personal nuestra, son en esencia la expresión digital de la identidad física más íntima e inmutable.

6.1.2 Análisis de Marcos Normativos Internacionales

El Reglamento General de Protección de Datos (GDPR) de la Unión Europea (Kyriakou et al., 2024; Tanwar et al., 2019), que entró en vigor el 25 de mayo de 2018, nos da sin duda alguna el marco más completo y estricto sobre la protección de datos biométricos a nivel mundial, esto gracias a su gran influencia donde la mayoría de las organizaciones globales adoptan sus estándares

¿Pero cómo el GDPR funciona?, pues este establece seis principios fundamentales que abarcan todo el procesamiento de datos personales como:

Tabla 2 Principios Fundamentales GDPR

PRINCIPIOS FUNDAMENTALES DEL GDPR

Licitud, lealtad y Transparencia	**Nos habla del procesamiento y que este debe realizarse de manera licita, leal y trasparente, lo que significa que las organizaciones deben comunicar claramente que datos biométricos se están recopilando con que propósito, como se almacenan y con quien se comparten.**
Limitación de la finalidad	**básicamente nos dice que los datos deben recopilarse con fines determinados explícitos y legítimos, este principio es particularmente relevante para los sistemas biométricos porque prohíbe la "expansión de misión" ósea que los datos recopilados no pueden ser reutilizados para usarse en propósitos diferentes al mencionado al inicio.**
Minimización de datos	**Estos datos deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados, en esencia para la biometría esto significa que las organizaciones deben justificar por qué necesitan los datos y por qué no pueden lograr su "objetivo" de otra forma.**
Exactitud	**Básicamente nos dice que los datos deben de ser exactos y de ser necesario actualizados.**
Limitación del plazo de conservación	**nos habla de cuánto tiempo deben de mantenerse estos datos por así decirlo "cautivos" ya que en algún momento estos deben ser liberados como por ejemplo ¿Qué pasa con un exempleado o un estudiante graduado? Ya no sería necesario tener estos datos.**
Integridad y confidencialidad	**Los datos deben tratarse de manera que se garantice su seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito.**

Fuente: Autor basado en (Kyriakou et al., 2024)

El Artículo 9 del GDPR establece que se debe distinguir a la hora de clasificar y guardar datos personales ya que no es lo mismo guardar datos como información sobre su origen, opiniones políticas, filosóficas, orientación sexual, datos de salud etc. A guardar los datos digitales de nuestra identidad física más íntima e inmutable. El artículo establece que estos deben clasificarse como “categorías especiales de datos personales”.

Cabe recalcar que el GDPR define los datos biométricos como "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos". Lo que significa que esta definición no solo abarca aspectos físicos, sino que también el reconocimiento de marcha, análisis de patrón de teclado y características vocales

Asimismo, también hay algunos derechos que nosotros como usuarios tenemos y a veces ni nos damos cuenta, estos incluidos en el GDPR estableciendo así un conjunto de estos los cuales son:

- **Derecho de acceso (Artículo15):** Establece que tenemos el derecho a obtener confirmación de si nuestros datos personales están siendo procesados y de ser verdad, el acceso a estos datos. Puesto que los datos biométricos son de carácter sensible el hecho de poder saber si están o no siendo procesados puede ser muy importante.

- **Derecho de rectificación (Artículo 16):** Establece que podemos solicitar la corrección de datos inexactos. Que, aunque no haya errores como tal de los datos biométricos de los usuarios, puede que las plantillas internas donde se almacenen si los tengan, en este caso tener el derecho a que por así decirse “guarden bien mi información” no está de más.

- **Derecho de supresión o al olvido (Artículo 17):** Establece que podemos solicitar la eliminación de nuestros datos personales bajo ciertas circunstancias. Dada la naturaleza de los datos biométricos y lo sensibles que son este articulo puede llegar a ser muy práctico.

- **Derecho a limitación del tratamiento (Artículo 18):** Establece que podemos solicitar que se restrinja el procesamiento de datos bajo ciertas circunstancias. Como se mencionó con anterioridad al ser datos muy sensibles puede llegar a ser muy importante.

- **Derecho a la portabilidad de Datos (Artículo 20):** Establece que tenemos el derecho a recibir nuestros datos en un formato estructurado. Que refiriéndose a datos biométricos puede suponer cuestiones interesantes sobre portabilidad de plantillas biométricas.

- **Derecho de oposición (Artículo 21):** Establece que tenemos el derecho de oponernos al procesamiento de nuestros datos personales bajo ciertas circunstancias sobre todo cuando el interés es del controlador. Lo que lo convierte en muy práctico.

Una de las características más importantes del GDPR es su régimen de sanciones administrativas las cuales pueden alcanzar cifras enormes de hasta 20 millones de euros o el equivalente al 4% de la facturación global anual del ejercicio financiero anterior. Gracias a estas potenciales y elevadas multas el cumplimiento de la protección de los datos paso de ser secundaria a una dé prioridad de nivel ejecutivo en organizaciones de todo el mundo. Esto debido a infracciones del procesamiento de los artículos del 5 al 9 y o violaciones de los derechos y esto sumado a que el procesamiento de datos biométricos sin alguna base legal constituye una violación del artículo 9, las organizaciones que implementan sistemas biométricos lo deben de hacer con mucha precaución. (Sun & Liu, 2025)

6.1.3 Identificación de vulnerabilidades por IA en biometría

Lo que se consideraba hace unos pocos años como un sistema de seguridad impenetrable como lo son los rasgos faciales, de voz o de huella hoy en día están bajo amenaza continua, esto debido a que la mayoría de los sistemas biométricos se construyeron sobre la idea de que los rasgos del ser humano eran difíciles o incluso imposibles de replicar o falsificar, pero fue precisamente esto lo que los llevo a no desconfiar.

La llegada de redes generativas (GANs, difusores, modelos TTS avanzados, etc.) evidencia que en realidad ahora no solo es barato sino también accesible el producir tanto videos como audios o imágenes que imitan a una persona con un alto grado de realismo.

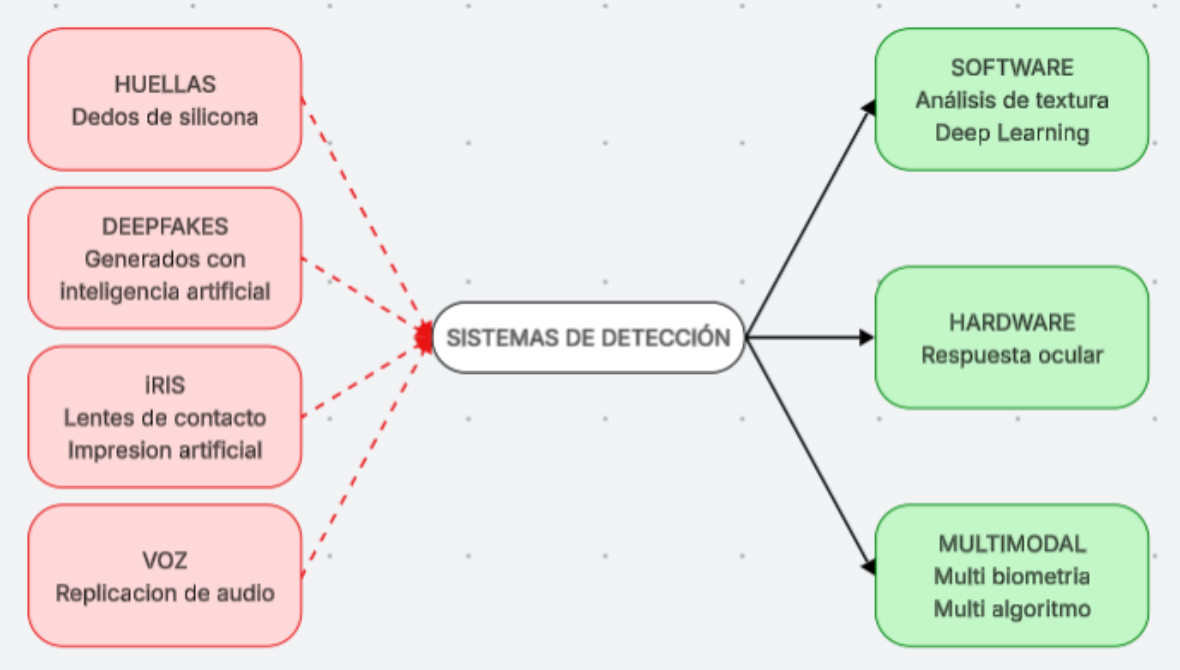
Varios estudios como (Bendiab et al., 2025) demuestran que el uso de deepfakes y técnicas generativas ha aumentado considerablemente, esta investigación documenta un incremento significativo en ataques de presentación y de inyección digital que comprometen sistemas de autenticación biométrica mediante contenido sintético generado por IA o “selfies deepfakes”.

La gravedad de esta amenaza es tal que la investigación advierte sobre una creciente pérdida de confianza en sistemas de autenticación facial biométrica esto

debido a la proliferación de deepfakes (Bendiab et al., 2025). ¿Pero cómo y cuáles son estos ataques que han logrado números tan altos y que a su vez según el GDPR tienen sanciones que preocupan incluso a las empresas? Gracias a esta situación se evidencia la urgencia de desarrollar contramedidas avanzadas como:

- **Ataques de presentación (Presentation Attacks):** Consiste en presentar ante el sensor como cámara, micrófono o lector una representación física o audiovisual del usuario objetivo replicándolo mostrando en pantallas, mascaras 2D/3D, fotos impresas o dispositivos reproduciendo alguna grabación, cabe recalcar que estas técnicas o ataques eran fácilmente detectaos con técnicas en el pasado como liveness esto gracias a que en si el material expuesto no era “humano” por así decirlo, en esencia tenía escasez de parpadeos, respuestas a estímulos, análisis de textura, entre otros. La problemática radica en que gracias a programas como deepfakes o “videos realizados con IA que utiliza procesos de machine learning” que imitan micro expresiones y reflejos esto sumado a reproducciones de alta resolución que son capaces de engañar sensores convencionales. A continuación, se mostrará una ilustración sobre los ataques dirigidos a los múltiples sistemas de detección.

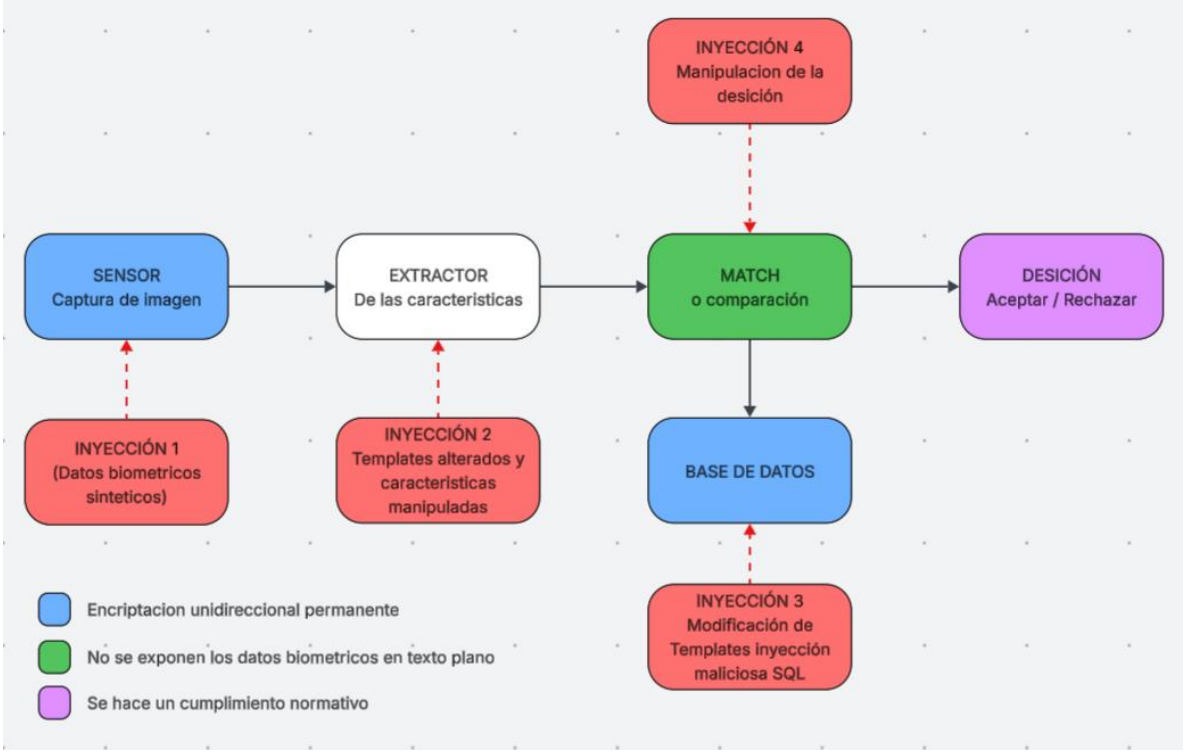
Figura 4. Vectores de Ataque y Contramedidas del Sistema de Detección Biométrica



Fuente: Autor con referencias de:*(Marcel et al., 2023)*

- **Ataques de inyección (Injection Attacks):** este tipo de ataques son un poco más complejos. Este consiste en la emulación de cámaras virtuales que envían video pregrabado o generado con IA o la misma inyección de código que se salta el paso de lo que "ve" la pantalla y solo muestra un flujo de datos que no tiene como tal seguridad. Pudiendo así generar múltiples ataques de este tipo mostradas en la siguiente ilustración

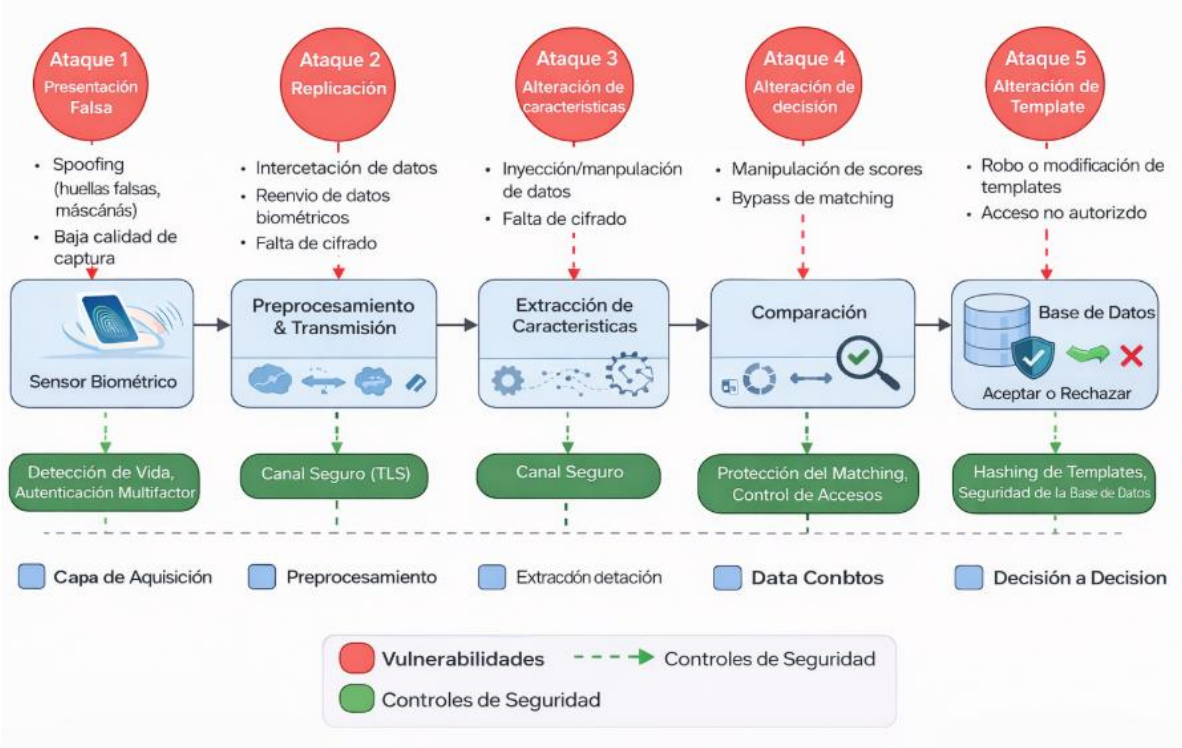
Figura 5. Arquitectura ataques de inyección



Fuente: Autor con referencias de:*(Marcel et al., 2023)*

Cabe destacar que la IA asimismo puede crear identidades completas como: rostro, voz, historial, foto de perfil, documentos falsos, entre otros, lo que facilita fraudes de "identidades sintéticas" que no pertenecen a nadie real y más bien fueron creados artificialmente. Pero ¿con que fin? Principalmente si nos enfocamos en las fuentes de entretenimiento como redes sociales, repositorios públicos y datos filtrados, pues estas identidades sintéticas se usan para cubrir cuentas, obtener créditos o facilitar el lavado de dinero. La siguiente ilustración recopilara los ataques mencionados anteriormente e ilustrara un gráfico de la arquitectura convencional o típica de un sistema de autenticación biométrica y donde se genera la instrucción de algunos.

Figura 6. Ataques a la Arquitectura biométrica convencional



Fuente: Autor con referencias de:*(Vandana & Kaur, 2021)*

En la tabla 3 se presentan dos ataques hacia empresas usando ingeniera social para el caso de Hong Kong e inyección biométrica para el sector bancario con el fin de vulnerar sus sistemas.

Tabla 3. Casos de Vulnerabilidades

CASOS DE VULNERABILIDADES

Hong Kong (2023)	**Nos habla de que se reportó una transferencia de 25M facilitada por deepfakes en una videollamada que suplantó al CFO y a otros ejecutivos.**
Sector Bancario	**ataques dirigidos a verificar identidades de ejecutivos o clientes mediante material audiovisual falso para autorizar pagos.**

Fuente: Autor con referencias de (Bendiab et al., 2025)

¿Acaso existen algunas vulnerabilidades biométricas? Pues resulta que sí, algunas de estas con el paso del tiempo se han visto cada vez más fuertes ya que se

alimentan de la información que los mismos usuarios a veces comparten como imágenes públicas de redes sociales tales como:

Tabla 4. Vulnerabilidades Biométricas y sus efectos

Vulnerabilidad	Amenaza que Genera
Reconocimiento Facial: Esta expuesto gracias a la masiva disponibilidad de imágenes que son públicas existentes en las múltiples redes sociales y de la facilidad para adquirirlas, esto con el fin de generar caras y animarlas.	**Deepfakes-as-a-Service:** Estos modelos comerciales son encontrados en internet y estos permiten a personas con pocos recursos crear un contenido sintético muy profesional o similar, esto generalmente con intenciones poco éticas.
Reconocimiento de Voz: algunos programas modernos replican timbre, tono y pausas a la hora de hablar o emular la voz de alguna persona.	**Impersonificación de voz impulsada por Deepfakes Vocales:** Básicamente como en el ejemplo anterior de la suplantación del CEO en Hong Kong que al utilizar únicamente la autenticación de voz implico en la perdida de millones.
Detección de Vivacidad Tradicional: Como se mencionó anteriormente algunas técnicas de respuesta como (parpadeo, movimientos) son insuficientes frente a deepfakes en tiempo real que incorporan esos micro gestos.	**Identidades sintéticas hibridas:** En esencia combina datos reales y los fabricados para superar controles que son basados en coincidencias simples, haciendo que estos deepfakes con estos micro gestos vulneren sistemas poco sofisticados.
Almacenamiento en Nube: Si bien esta alternativa facilita la escalabilidad, amplía el efecto de ataque.	**Ataques coordinados 24/7:** Básicamente las personas con intenciones de ataque se coordinan en ciertas horas poco monitoreadas aprovechando su gran escalabilidad y amplio ataque

Fuente: Autor con referencias de (Unmasking deepfakes, Springer, 2025)

6.1.4 Matriz de Riesgos

Con base en las vulnerabilidades identificadas en las actividades del primer objetivo, se desarrolló una matriz de riesgos técnicos, donde esta evalúa 16 riesgos categorizados en su probabilidad desde Muy Bajo hasta Muy Alto y el riesgo que genera desde Insignificante Hasta catastrófico.

Tabla 5. Matriz de Riesgos

		Probabilidad				
		Muy Baja (1)	Baja (2)	Media (3)	Alta (4)	Muy Alta (5)
Riesgo	Insignificante (1)				**Captura sin consentimiento** Violación de privacidad, redes sociales, etc	**Privacity como Comodity** Tomalo o dejalo en terminos de servicio
	Menor (2)			**Vulnerabilidades Cloud** Se amplia el arango de ataque	**Detección de Vivacidad Insuficiente** tecnicas tradicionales	**Consentimiento No Informado** Los usuarios no comprenden las implicaciones
	Moderado (3)		**Incumplimineto del GDPR Articulo 9** Procesamiento ilegal de Datos Biometricos	**Ataques Cordinados 24/7** Se aprovecha el no horario laboral para estos ataques	**Deepfakes de Voz** Clonacion de voz con IA	**Deepakes Faciales** Videos Sinteticos Realistas
	Mayor (4)			**Ataques de Inyección** Camaras virtuales inyeccion de codigo	**Scraping de Imágenes en Redes Sociales** Recoleccion masiva de fotos para entrenar la IA	**Presentation Attacks** Máscaras 2D/3D, fotos, videos deepfake
	Catastrofico (5)		**Identidades Sinteticas Hibridas** Combinación de datos reales + Fabricados	**Robos de Bases de Datos Biometricas** Estan sin encriptación adecuada	**Falta de encriptacion Homomorfica** No adopcion por costo y complejidad	**Complejidad & Costos de Implementación**

Fuente: Autor Con referencias de todo el Primer Objetivo

Como los resultados revelan, podemos observar una situación alarmante ya que el 72% de los riesgos son muy graves, con 4 riesgos categorizados como catastróficos, presentándose así uno de estos en cada nivel de probabilidad excepto la “Muy Baja”, por lo tanto esta tabla confirma la premisa fundamental de la investigación: la inteligencia artificial ha transformado radicalmente el panorama de amenazas en autenticación biométrica, convirtiendo sistemas que se consideraban "infalibles" en objetivos vulnerables ante adversarios con acceso a herramientas comerciales de generación de contenido sintético.

6.2 Objetivo 2 (Análisis Comparativo Sectorial)

En este segundo objetivo se desarrollará el análisis comparativo sectorial con el fin de dar cumplimiento al segundo objetivo propuesto en: Tabla 1. Entregables asociados a cada objetivo especifico; Para ello, se examinan en primer lugar los sectores salud y financiero, identificando sus particularidades en cuanto a implementación biométrica, amenazas y marcos regulatorios. Posteriormente se analiza la implementación en los sectores educativo y judicial, explorando sus contextos operativos y desafíos específicos. Finalmente, se realiza una comparación interseccional de los impactos y desafíos comunes entre todos los sectores, sintetizada en una matriz de riesgos por sector que permite visualizar de manera estructurada los niveles de criticidad y exposición de cada uno.

6.2.1 Estudio de casos en sectores salud y financiero

Como se pudo observar hay un gran campo en el que trabajar, pero ¿cómo sabemos por dónde empezar y cuales sectores son los más afectados? Bueno el análisis parte de un comparativo de los sectores salud y financiero en la implementación de sistemas de autenticación biométrica con inteligencia artificial, este revela dos industrias que, aunque comparten algunos desafíos como seguridad y privacidad, estas operan bajo contextos regulatorios, operacionales y éticos muy diferentes. Pues, aunque ambos sectores manejan información altamente sensible como los son datos médicos personales y o financieros respectivamente, la cual de filtrarse puede tener consecuencias devastadoras para varios individuos y organizaciones, la verdad es que la naturaleza de los patrones de uso, las amenazas específicas y las prioridades son diferentes.

Empecemos por el sector salud el cual enfrenta una crisis a la hora de mejorar la precisión con la que se identifican los pacientes, un problema que según la organización Mundial de la Salud (WHO) contribuye a 2.6 millones de muertes anuales. Esta estadística nos habla literalmente de la vida o la muerte de la autenticación biométrica en contextos clínicos(Dhingra-Kumar et al., 2021).

Por su parte el sector financiero reporta que ha experimentado un aumento exponencial en amenazas de ciberseguridad, este ha experimentado un aumento en amenazas de ciberseguridad con un incremento del 125% en Trojans bancarios móviles entre 2019 y 2020(Qamar et al., 2019).

Pero bueno empecemos por el sector salud y por qué hay tanta falta de precisión y errores humanos a la hora de identificar pacientes, varios documentos de estudios de IEEE y ScienceDirect como (Montgomery & Wei, 2023) revelan que los métodos tradicionales de identificación, pulseras con códigos de barras, números de historia clínica, verificación verbal de nombre y fecha de nacimiento son alarmantemente propensos a errores humanos, especialmente en entornos de alta presión como departamentos de emergencia, unidades de cuidados intensivos y salas de cirugía. Los 2.6 millones de muertes anuales se atribuyen a errores de identificación según la WHO las cuales representan tragedias individuales, es decir, a los pacientes se les suministra medicamentos incorrectos, se someten a procedimientos quirúrgicos equivocados o experimentan retrasos críticos en tratamiento debido a confusión sobre su identidad, esto generalmente ocurre en pacientes con demencia o deterioro cognitivo y aquellos con barreras lingüísticas. Pero ¿cómo poder combinar una tecnología de identificación biométrica que acate las normas éticas y regulatorias existentes y dichas anteriormente?

El estudio (Alshehri, 2025) publicado en IEEE (2025) propone un sistema comprehensivo que aborda estas vulnerabilidades mediante la integración de múltiples algoritmos especializados, este sistema comprende cinco componentes principales, los cuales son:

Multi-Factor Authentication Algorithm (MFAA): Este algoritmo combina la autenticación biométrica (huella dactilar, reconocimiento facial, escaneo de iris) con factores adicionales como tokens de dispositivo, geolocalización y comportamiento del usuario. Esta arquitectura es crítica en entornos healthcare porque mitiga el riesgo de que una sola modalidad biométrica comprometida resulte en acceso no autorizado a sistemas médicos críticos.

Biometric template Protection Algorithm (BTPA): Debido a que las plantillas biométricas healthcare no pueden ser “cambiadas” como una contraseña si son comprometidas, BTA implementa técnicas de cancelabilidad biométrica y transformaciones irreversibles, ósea que las plantillas se almacenan en formatos transformados matemáticamente de manera que incluso si la base de datos es violada de laguna forma, estos datos originales biométricos no pueden ser reconstruidos o utilizados para acceso no autorizado.

Dynamic Risk-Based Authentication Algorithm (DRBAA): Este componente evalúa continuamente el contexto y nivel de riesgo de cada intento de acceso. Por ejemplo, si un médico accede a estos registros médicos desde su trabajo a su horario habitual durante horas de trabajo normales presenta un perfil de riesgo bajo, mientras que el mismo medico intentando acceder a múltiples registros de pacientes a las 3 Am o fuera de su horario habitual y fuera de su ubicación de trabajo representa un riesgo alto y por lo tanto activa protocolos de autenticación adicionales

Adaptive Biometric Fusion Algorithm (BFA): Como su nombre indica, es un algoritmo adaptativo lo que significa que, si un médico en su entorno de trabajo donde requiere máscaras, guantes y gorros el reconocimiento facial puede ser inefectivo, pero el escaneo de iris permanece siendo una opción viable por lo que este algoritmo se adapta automáticamente a que modalidad utilizar basándose en condiciones ambientales y de disponibilidad.

Context-Aware Access Control Algorithm (CAACA): Este componente implementa controles de acceso basados en roles, ubicación, hora del día y necesidad clínica. Por ejemplo, un enfermero de piso puede acceder a registros de medicación de pacientes bajo su cuidado directo, pero no a registros psiquiátricos completos o resultados de pruebas genéticas sin justificación. El CAACA implementa el principio de privilegio donde este mantiene una flexibilidad mínima para emergencias médicas donde necesite acceso amplio necesario para salvar vidas.

Con los componentes mencionados se concluye que siempre va a haber un conflicto entre la seguridad y la accesibilidad. EHR o Registros médicos electrónicos, estos representan uno de los avances más significativos y simultáneamente más vulnerables en la digitalización de la atención médica, esto debido a que estos sistemas centralizan toda la información médica competa de los pacientes esto incluyendo a su vez la historia clínica, resultados de laboratorio, imágenes diagnosticas, prescripciones, notas de proveedores, información genética en bases de datos, entre otras. Esta centralización ofrece beneficios innegables como: la eliminación de registros en papel perdidos ilegibles, disponibilidad inmediata de historial médico completo en emergencias, reducción de pruebas diagnósticas duplicadas, sin embargo, esto crea un objetivo de alto valor de ser vulneradora. Estos registros médicos de los pacientes pueden incluso valer 10 o 50 veces más

que la información de las tarjetas de crédito porque contienen información que no puede ser “cancelada” o reemplazada como: historial médico, números de seguro social, entre otras (Czeschik, 2018; Tertulino et al., 2023).

Sin embargo, existen algunas alternativas como el “PHBio Homomorphic Biometric Encryption Scheme in Healthcare 4.0 Ecosystems” (Saraswat et al., 2022) publicado en IEEE (2022) que aborda este dilema fundamental mediante la implementación de encriptación homomórfica de Paillier para autenticación biométrica, que como se mencionó anteriormente sirve para verificar y realizar acciones con la información biométrica sin tener que acceder a ella particularmente, pero ¿cómo funciona junto con el esquema Phbio?

El criptosistema de Paillier es un esquema de encriptación de clave pública que posee la propiedad homomórfica aditiva es decir que hace operaciones matemáticas sobre datos encriptados, produciendo así resultados encriptaos que cuando se descifran, corresponden a las operaciones realizadas sobre los datos originales no encriptados, pero ¿qué significa en el contexto de autenticación biométrica?, bueno antes de responder eso cabe recalcar que este esquema PHBio representa un avance significativo, pero no resuelve todos los desafíos del sector salud. Esto se debe principalmente a su coste, esto debido a que el valor ronda entre ($500K-$2M) significando así que muchas instituciones de salud de países en desarrollo o hospitales rurales quedan excluidas de estas protecciones avanzadas, creando una brecha de seguridad biométrica global(Saraswat et al., 2022).

Fase de Registro: Cuando un paciente o un doctor se registra por primera vez en el sistema, sus datos biométricos, por ejemplo: su huella dactilar es capturada y transformada en un vector de características matemáticas, posteriormente este pasa a ser encriptado usando el criptosistema de Paillier antes de ser almacenado en la base de datos del servidor, por lo que el servidor nunca tiene acceso a la plantilla biométrica no encriptada.

Fase de Autenticación: Cuando el usuario intenta autenticarse después de haberse registrado, este proporciona una nueva muestra biológica, por ejemplo: coloca su dedo en un escáner. Pues esta nueva muestra también es transformada

en un vector de características y encriptada localmente en el dispositivo del usuario antes de ser de nuevo transmitida al servidor

Comparación Homomórfica: El servidor ahora posee dos vectores encriptados: la plantilla con la que se registró primeramente que esta almenada y la muestra de autenticación recién proporcionada. Utilizando las propiedades homomórfica de la encriptación de Paillier, el servidor calcula la distancia euclidiana (EUDD – Euclidean Distance) entre estos dos vectores mientras ambos permanecen completamente encriptados y posteriormente es devuelta al usuario, que en palabras entendibles significa que los datos biométricos se transforman en vectores de números tanto el de registro como el de autenticación y lo que se hace es medir la distancia (euclidiana) ósea la diferencia de un vector a otro, si son muy similares entonces es muy probable que sea la misma persona, si son diferentes entonces es otra persona y lo innovador o inusual acá es que el servidor es capaz de hacer esto sin necesidad de desencriptarlo.

Decisión de Autenticación: El usuario (o su dispositivo) descifra la distancia calculada. Si esta distancia está por debajo de un umbral predefinido indicando que la nueva muestra está por debajo de un umbral predefinido, indicando que la nueva muestra es suficiente similar a la plantilla registrada, la autenticación es exitosa, en cambio sí excede el umbral, la autenticación falla.

Esto proporciona algunas ventajas de seguridad, en esencia múltiples capas de protección. Primeramente, el servidor central el cual es el objetivo de ataques externos nunca tiene acceso a datos biométricos no encriptados. Incluso si llegara a ser comprometida la base de datos los atacantes obtienen solo plantillas biométricas encriptadas que son computacionalmente inaccesibles de descifrar sin las claves apropiadas. Sin embargo, aún hay varios desafíos de implementación como la complejidad ya que las operaciones son entre 100 a 1000 veces mas lentas que las mismas sobre los datos no encriptados, el problema radicaría en contextos médicos de emergencia donde cada segunda cuenta.

En cuanto al sector financiero, en este opera lo que puede describirse solo como un estado de guerra cibernética perpetua ya que las instituciones financieras son objetivos continuos de ataques.

El aumento del 125% en Trojans bancarios móviles entre 2019 y 2020 documentado en estudios recientes (Qamar et al., 2019) representa solo la punta del iceberg, ¿Cómo lo hacen? Estos malware o programas malignos se disfrazan como aplicaciones legitimas, se instalan en teléfonos inteligentes de víctimas y luego interceptan credenciales bancarias, códigos de autenticación de dos factores y ora información sensible.

Los estudios (Blanco Gonzalo et al., 2018; Goicoechea-Telleria et al., 2016) documentan un experimento revelador realizado en la conferencia GeekPwn 2019, se les propuso desafiar y derrotar sistemas de autenticación biométrica en smartphones comerciales. Los resultados fueron alarmantes. Ya que múltiples equipos lograron desbloquear dispositivos protegidos por huella dactilar o reconocimiento facial en menos de 30 minutos usando diversas técnicas

Los Deepfakes de video de los cuales ya hablé son bastante preocupantes sin embargo el deepfakes de voz es importante de tener en cuenta, porque un estudio documentado a cerca de un fraude donde unos criminales utilizaron tecnología de clonación de voz habilitada por IA para imitar la voz donde criminales utilizaron tecnología de clonación de voz habilitada por IA para imitar la voz de un CEO. Los atacantes habían recopilado muestras de voz del ejecutivo de entrevistas públicas, presentaciones y otras fuentes disponibles públicamente. El software de síntesis de voz entrenado genero un audio que recopilaba convincentemente no solo la voz del CEO sino de sus patrones de habla, acento y cadencia. Con este audio en su poder procedieron a llamar al departamento financiero de la compañía, afirmando ser el Ceo y solicitando una transferencia urgente de 25 millones a un proveedor. El empleado que recibió la llamada, reconociendo la voz de su CEO y sin sospecha alguna de que estaba hablando con una IA en vez de su jefe real, hizo la transferencia. Para cuando fue descubierto, los fondos habían sido movidos a través de múltiples jurisdicciones y lavados.

Este incidente nos deja ver una vulnerabilidad fundamental de autenticación biométrica mientras que las características físicas como huellas dactilares o iris requieren acceso físico para duplicar, las características de voz son trasmitidas a través del aire cada vez que alguien habla. Cualquier grabación de voz de una

conferencia puede ser potencialmente utilizadas como material de entrenamiento para sistemas de síntesis de voz.

El estudio (Liébana-Cabanillas et al., 2025) proporciona análisis empírico detallado de Biometric Payment cards (BPCs), una tecnología emergente que busca combinar la conveniencia de los pagos sin contacto con la seguridad de autenticación biométrica.

Las BPCs son tarjetas de crédito o débito físicas con sensores de huella dactilar integrados. Durante una transacción, el titular de la tarjeta coloca su dedo en el sensor integrado en la tarjeta, posteriormente el sensor captura la huella dactilar, la compara con una plantilla almacenada de forma segura en el chip de la tarjeta y solo si hay coincidencia, autoriza la transacción. Cabe recalcar que toda la plantilla biométrica sucede en la tarjeta, esta nunca sale, toda la comparación ocurre en esta, eliminando preocupaciones sobre transmisión y almacenamiento de datos biométricos en servidores centrales, pero ¿cómo funciona esto?, simple esta tecnología sofisticada combina tres marcos teóricos y tres técnicas analíticas los cuales son, en marco teórico los siguientes:

Unified Theory of Acceptance and Use of Technology 2 (UTAUT2): Este modelo, se creó originalmente para poder entender la adopción de tecnología del consumidor, identificando factores que influencian si las personas adoptan una nueva tecnología, ósea las personas se harán preguntas como ¿la tecnología me ayudara a lograr mis objetivos?, ¿Qué tan fácil es de usar? ¿Otras personas importantes para mi piensas que debería usarla?, ¿tengo el conocimiento y recursos para usarla?

Privacy Regulation Theory (PRT): Esta teoría reconoce que las personas lo que hacen es buscar un equilibrio de entre su necesidad de privacidad versus su necesidad de interacción social y convivencia, ósea las personas buscan balancear sus preocupaciones sobre proporcionar datos biométricos contra el deseo de transacciones que pueden ser convenientes y seguras.

Trust Theory (TT): La confianza de las personas en el sistema de pagos con tarjetas es fundamental para la adopción de nuevas tecnologías financieras pues los usuarios deben confiar que sus datos biométricos serán protegidos, que el

sistema funcionara correctamente cuando se necesite. Ahora acerca de las técnicas analíticas son tres, entre ellas están:

Partial Least Squares Structural Equation Modeling (PLS-SEM): Esta técnica estadística permite a los investigadores examinar relaciones complejas entre múltiples variables simultáneamente identificando así que factores tienen más intención de usar BPCs.

Fuzzy Set Qualitative Comparative Analysis (fsQCA): Mientras PLS SEM examina efectos lineales y aditivos, fsQCA reconoce que la casualidad en comportamiento humano es frecuente y diferentes combinaciones pueden llevarlo al mismo resultado. FsQCA identifica múltiples “paths” o configuraciones que resultan en adopción o rechazo de BPCs

Necessary Condition Analysis (NCA): Esta técnica identifica si algunos factores son o no necesarios para un resultado, por ejemplo: ¿la confianza mínima es realmente necesaria para cualquier adopción de BPC, independientemente de otros factores?

Pero ¿es esto la única alternativa?, ¿acaso es suficiente?, pues resulta que no. El estudio “Calls for behavioural biometrics as bank frauds soars” publicado en Biometric Tecnology Today (2021) documenta el surgimiento de biometría comportamental como una tecnología disruptiva, es decir. A diferencia del proceso “normal” el cual es: usar al menos dos de tres factores de algo que se sabe cómo la contraseña o el PIN, algo que tiene cómo un dispositivo o Token y algo de la persona cómo la biometría entre las que se encuentra la huella dactilar, registro facial o el iris; esta funcionaria midiendo características anatómicamente estadísticas, es decir la biometría comportamental analiza patrones de como las personas interactúan con sus dispositivos, patrones como: escritura(velocidad, ritmo presión de las teclas, tiempo entre teclas, etc) dinámica del mouse (su velocidad, aceleración, patrones de click), patrones de navegación táctil en dispositivos móviles como (la presión, área de contacto, gestos de deslizamiento), incluso patrones de marcha detectados por acelerómetros de teléfonos inteligentes. Esto dándonos así varias ventajas frente al Payment Services Directive 2 (PSD2) de la unión europea, entrado en aplicación en 2021 las cuales son:

Autenticación Continua: A diferencia de la biometría física que típicamente autentica en un único punto de inicio de sesión, la biometría comportamental puede operar continuamente durante toda una sesión, por ejemplo: el sistema monitorea constantemente si los patrones de comportamiento coinciden o no con el perfil esperado del usuario legítimo, donde si lo patrones son diferentes ósea divergen entre sí, se sugiere que el dispositivo fua hackeado o robado, etc. Por lo que el sistema puede solicitar una re-autenticación o terminar la sesión.

Sin fricción: La biometría comportamental opera pasivamente en segundo plano sin requerir acción explicita del usuario. Los usuarios solamente interactúan con su aplicación bancaria como de costumbre ósea como normalmente lo harían, mientras que su comportamiento está siendo autenticado invisiblemente. Esto proporcionando seguridad sin sacrificar la experiencia del usuario.

Difícil de Falsificar: Mientras que un atacante podría robar una contraseña o incluso obtener una imagen de la huella dactilar, poder replicar los patrones comportamentales sutiles y subconscientes de un individuo como lo puede ser la simple escritura, la manera de mover el ratón, resulta mucho más complejo y desafiante.

Cumplimiento Regulatorio: La biometría comportamental puede satisfacer el componente de algo que tú eres, (requisitos SCA bajo PSD2) permitiendo a los bancos la posibilidad de cumplir regulaciones mientras mantienen interfaces de usuario fluidas.

También existen situaciones donde por ejemplo una persona dejo su sesión abierta en un dispositivo y otra persona asume el control de la sesión, estas ocasiones son particulares ya que los sistemas tradicionales de autenticación no son capaces de autentificar estas situaciones porque precisamente la autenticación ya se hizo, en cambio la biometría comportamental al monitorear toda la sesión puede detectar desviaciones o patrones que no coinciden con los de la persona legitima.

Pero existen limitaciones y desafíos antes de que se pueda regular o comercializar estas alternativas como que la biometría comportamental típicamente tiene tasas de errores más altas que la biometría física, algunos comportamientos no son tan consistentes como lo pueden ser las características anatómicas de una persona, además una persona por ejemplo puede escribir de manera diferente si esta se encuentra cansada, estresada o distraída. Estos sistemas deben de ser calibrados cuidadosamente para evitar falsas alarmas que pueden llegar a ser frustrantes ya que pueden llegar a bloquear a un usuario legítimo que solo estaba cansado.

Además, a algunos usuarios puede que no les guste mucho la idea de estar vigilados constantemente, saber que el software vigila hasta como el usuario mueve el mouse, presiona cada tecla puede que lo haga sentir incómodo, por eso las regulaciones del GDPR requiere que los usuarios sean informados sobre este monitoreo.

6.2.2 Análisis de implementación en sectores educativo y judicial

Después de hablar del sector salud y el sector de las finanzas seguiremos con el sector judicial y el educativo donde estos representan formas de implementación biométrica que, aunque pudiera considerarse que son superficialmente disparejas la verdad es que comparten desafíos fundamentalmente relacionados con legitimidad institucional, verificación de identidad y equilibrio entre eficiencia y lo operacional además claro de los derechos individuales.

El sector educativo ha experimentado transformación sin precedentes en la última década la cual fue acelerada dramáticamente por la pandemia que hubo por allá en 2020 del COVID-19, la cual forzó una migración masiva de modalidades nuevas de aprendizaje remoto y la cual creo necesidades urgentes de autenticación de estudiantes y protocolos de exámenes en línea.

En el caso del sector judicial que ya contaba con tecnologías biométricas como autenticación por huella, ahora enfrenta otro tipo de problemática, ahora referente a lo ético y legal de manera compleja sobre la expansión de bases biométricas gubernamentales, uso de reconocimiento facial en vigilancia y aplicación de ley y estándares apropiados de evidencia biométrica en procedimientos legales.

Ambos sectores operan bajo un público intenso y extenso con expectativas de integridad institucional, ya que en educación la credibilidad en cuanto a credenciales académicas, diplomas, grados, certificaciones y demás, dependen de la confianza que las personas tengan en estos certificados porque representan logros genuinos, no fraudes académicos; en el sistema judicial, la legitimidad de veredictos criminales, decisiones civiles y toda la justicia depende de identificación precisa de acusados, testigos y evidencia. Cualquier error de identificación en cualquier sector puede tener consecuencias devastadoras como: estudiantes injustamente acusados de hacer trampa lo que podría desmotivarlos a dejar la carrera o personas inocentes identificados erróneamente pueden enfrentar cargos injustos algunos siendo condenados.

Teniendo en cuenta lo anterior, se aborda el sector educativo, remontándonos pues así en la pandemia del COVID-19 en 2020 que actuó como un experimento masivo en transformación educativa digital. Algunas de las instituciones que habían resistido o habían adoptado gradualmente esta tecnología de e-learning durante décadas fueron forzadas repentinamente a migrar completamente a otras alternativas como la modalidad en línea en cuestión de semanas. Dicha transición expuso varios errores de sistemas de autenticación tradicionales en entornos de aprendizaje remoto.

El estudio (Labayen et al., 2021) documenta estos desafíos. En entornos presenciales tradicionales, la autenticación de los estudiantes es necesaria e indispensable por diversas razones, así pues, los profesores pueden reconocer visualmente a los estudiantes que asisten a las clases, así mismo para los exámenes donde el maestro podría detectar fácilmente si alguien intenta suplantar a otra persona.

En contraparte el e-learning imposibilita la detección de un posible fraudo o implantación de una persona. Cuando un estudiante se conecta a un examen en línea desde su hogar, ¿Cómo podría la institución verificar y asegurarse de que el estudiante no está consultando en internet las respuestas de un examen, o utilizando la inteligencia artificial, o tal vez que otra persona este presentándose en su lugar?

La anterior investigación (Labayen et al., 2021) documentan un aumento significativo en el fraude del sector educativo gracias a la transición al aprendizaje en línea durante la pandemia que azoto al mundo en el 2020. Investigaciones muestran que varios estudiantes admitieron haber echo trampa en al menos una ocasión durante exámenes o tareas online diciendo que hacer trampa era “más fácil” estando en línea comparado a hacer un examen presencial supervisado; y los maestros reportaron sospechas de fraude académico en sus cursos en línea.

Básicamente, después de la pandemia y de que las instituciones comenzaran a usar medios virtuales para que los estudiantes pudieran proseguir con sus exámenes y clases, la credibilidad de estos sistemas, así como de los certificados proporcionados por estas instituciones, han perdido y pierden cada vez más credibilidad. Entonces, ¿qué solución tenemos?, pues el sistema de estudio de IEEE mencionado anteriormente también implementa un enfoque de autenticación de tres capas de verificación, las cuales son:

Autenticación preexamen: Antes de que un estudiante pueda acceder a un examen en línea, este debe completar un proceso de autenticación biométrica robusto el cual comprende:

- **Reconocimiento facial:** El estudiante debe colocar su rostro frente a la cámara web. El sistema captura múltiples imágenes desde diferentes ángulos y procede a extraer características faciales discriminativas usando redes neuronales convolucionales (CNNs) donde posteriormente compara estas características con la plantilla de registro el estudiante que está almacenada en la base de datos de la institución. Cabe recalcar que el uso de CNNs entrenados en granes bases de datos permite el reconocimiento incluso cuando las variaciones de iluminación, expresión y características fáciles menores son diferentes.

- **Reconocimiento de Iris:** Para exámenes de alta importancia como (exámenes finales, certificaciones profesionales), el sistema puede requerir autenticación de iris adicional. Donde el estudiante deberá mirar a la cámara a una distancia especifica mientras el sistema captura imágenes de alta resolución del iris. ¿Por qué el iris?, pues este contiene patrones

extremadamente complejos y únicos, haciendo que el reconocimiento de iris sea uno de los métodos biométricos más precisos disponibles.

Una vez que el estudiante ha sido identificado y autenticado correctamente, este se dispondrá a realizar la prueba, donde el sistema mantendrá una vigilancia continua para detectar comportamientos sospechosos, esto según la arquitectura de referencia propuesta por Labayen et al. (2021), el sistema funcionaría de la siguiente manera:

- **Biometría comportamental:** Como ya mencioné anteriormente esta biometría analiza el patrón de comportamiento de una persona, en este caso la analizaría durante toda la sesión.

- **Reconocimiento Facial (continuo):** La cámara web permanece activa durante toda la sesión del examen, capturando periódicamente frames de video. El sistema utiliza algoritmos de detección de rostro para verificar continuamente que: el rostro sea el del estudiante que está presentando la prueba, que solo haya un rostro visible indicando que solo esta esa persona realizando la prueba y por último que el estudiante este mirando únicamente a la pantalla.

- **Detección de Movimiento Ocular:** implementaciones avanzadas utilizan algoritmos de eye tracking para monitorear la dirección de la mirada del estudiante donde podrán detectar si el estudiante mira a otro lado donde posiblemente tenga notas o si está leyendo un párrafo de una posible doble pantalla.

- **Análisis de Audio Ambiental:** El sistema captura el audio del entorno del estudiante. Algunos algoritmos de procesamiento de lenguaje natural (NLP) pueden detectar voces múltiples (sugiriendo así que puede haber otra persona presente ayudándolo) o la voz del mismo estudiante, pero comunicando alguna pregunta.

Después de que el estudiante termina de hacer su prueba completa, algoritmos de inteligencia artificial analizan todos los datos capturados durante la sesión para generar una puntuación de la siguiente manera:

Análisis de Anomalías Temporales: El sistema examina la línea de tiempo del examen para algún posible evento sospechoso tales como: periodos donde el rostro del estudiante desaparece de la vista de la cámara, momentos donde múltiples rostros son detectados, cambios repentinos en patrones comportamentales. Estas anomalías se marcan y se mandan a revisar por personas que finalmente dan su veredicto.

Aprendizaje Automático Supervisado: El sistema utiliza modelos de ML entrenados en bases de datos de sesiones de exámenes pasadas (tanto de sesiones sin trampa como sesiones en las que se hizo trampa) para identificar algunos patrones que las personas a simple vista no notarían y pasarían desapercibidos.

Pero ¿Es realmente eficaz este sistema? Pues sí, resulta que el mismo estudio de (Labayen et al., 2021) ha demostrado mejoras significativas en la detección de fraude académico y reducción de carga de trabajo para instructores en comparación con sistemas de supervisión tradicionales basados únicamente en cámara, sino que la carga de trabajo de los instructores para revisar sesiones marcadas disminuyo considerablemente comparado con la revisión manual de todas las grabaciones del examen y por supuesto la satisfacción estudiantil fue moderadamente más positiva.

Tras el análisis del sector educativo, se procede a examinar al sector judicial donde la biometría ha sido una herramienta fundamental en la investigación criminal y adjudicación judicial por más de un siglo.

En el sector judicial, la biometría ha sido una herramienta fundamental tanto en la investigación criminal como en la adjudicación judicial durante más de un siglo. Un ejemplo paradigmático es el uso sistemático de las huellas dactilares para la identificación criminal, práctica que se consolidó a finales del siglo XIX gracias a la adopción de sistemas basados en el reconocimiento de los patrones de crestas presentes en las yemas de los dedos, los cuales son únicos en cada individuo y se mantienen invariables a lo largo de toda su vida.

(Maiti et al., 2025) señalan que esta afirmación se sustenta en dos principios fundamentales. El primero es el de la persistencia: los patrones de las crestas se

forman durante el desarrollo embrionario, entre las semanas 10 y 24 de gestación, y permanecen estables durante toda la vida del individuo; incluso ante lesiones menores como cortes o quemaduras, estas crestas se regeneran conservando su configuración original. El segundo principio es el de la unicidad: la probabilidad de que dos personas compartan patrones dactilares idénticos es extraordinariamente baja, al punto de considerarse prácticamente imposible, incluso en el caso de gemelos idénticos.

Uno de los avances tecnológicos más significativos en biometría forense ha sido pasar del típico método tradicional de tinta y papel a una captura de huellas dactilares en sistemas “live-Scan” electrónicos controlados, esto quitando limitaciones de algunos métodos tradicionales como una simple técnica inadecuada del rodado del dedo estas posteriormente deben ser escaneadas y enviadas por correo lo que creaba además del trabajo extra la posibilidad de error humano y claro el almacenamiento.

Pero ¿Cómo funciona esto? Pues este sistema de huella dactilar, tanto a la hora de declarar a alguien culpable coincidiendo sus huellas dactilares en una posible escena del crimen, como a lo cotidiano de una persona desbloqueando su celular inteligente, funciona de la misma manera, un sistema de conteo de puntos coincidentes donde cada país maneja su propio sistema, en este caso la mayoría usa un sistema de 12 puntos a excepción de Estados Unidos y Reino unido, sin embargo esta no es la única característica ya que dicho estudio nos habla de que el número de puntos no es el único factor determinante, esto debido a que la calidad de algunas impresiones sumado a la rareza de las características particulares observadas y la ausencia de diferencias inexplicables da muchos factores a tener en cuenta.

6.2.3 Comparación de impactos y desafíos interseccionales

Tras identificar los diferentes impactos y consecuencias que tienen los múltiples sectores, se desarrolla un análisis comparativo interseccional de la implementación de sistemas de autenticación biométrica con inteligencia artificial, revelando que, aunque diferentes sectores enfrentan desafíos únicos contextuales a sus operaciones específicas, si existen ciertos patrones ya sean éticos, algorítmicos, de escalabilidad o seguridad entre otros.

Tabla 6. Cuadro comparativo técnico por sector

Análisis	Salud	Financiero	Educativo	Judicial	Similitudes	Diferencias
Tasa de Adopción	50 – 60%	60 – 75%	30 – 40%	70 – 85%	Todas están en crecimiento	El gobierno Lidera
Principal Motivador	2.6 M Muertes/año Por errores de Identificación	Fraude 125%	Covid-19 y la migración a el aprendizaje a distancia	Seguridad Nacional	Seguridad / Precisión	Salud = Vidas, Finanzas = Dinero, Educación = Integridad
Desafío Ético Primario	Consentimiento pacientes vulnerables	Privacidad vs conveniencia	Vigilancia Estudiantes menores	Vigilancia masiva sin orden judicial	Tension, Privacidad / Seguridad Universal	Gravedad: Salud>Judicial> Financiero>Educativo
Vulnerabilidad I.A Principal	Robo EHR deepfakes personal medico	Deepfakes / Voz / Facial	Impersonación de exámenes y fraude Académico	Line-Ups virtuales sesgados	Deepfakes Amenaza Transversal	Impacto: Financiero = Perdidas ($) Salud = Perdidas (Vidas)
Sesgo Algorítmico	Menor precisión / Diagnosticar errores	Menor precisión / Exclusión algorítmica	Menor precisión (Acusaciones injustas / Trampa)	Menor precisión / Condenas Erróneas	Todos Afectados	Judicial: Consecuencias de libertad personal
Costo implementación	Alto (500K – 2M) Año	Moderado Alto (100k – 500k)	Bajo Moderado (20k – 100k)	Muy Alto (1M - 10M)	Biometría 3 – 5x veces más cara que las típicas contraseñas	Gobierno Absorbe costo; educación sensible de presupuesto
Modalidad Preferida	Facial + Iris	Facial + Huella + Comportamental	Facial + Tecleo + Mouse	Huella Dactilar + Facial	Multimodal Preferido	Contexto determina: salud = sin contacto
Consecuencia de Fallo	Muerte / Lesión del paciente	Perdida Financiera / Fraude	Injusticia Académica y Desconfianza de Credenciales	Encarcelamiento Injusto, Libertad comprometida	Impacto severo en todos	Judicial > Salud > Educativo > Financiero
Innovación Emergente	Encriptación Homomórfica PHBio	Biometryc payment Cards (BPC)	Proctoreo Multimodal I. A	Live Scan búsquedas faciales masivas	I.A Mejora Precisión en todos	Salud / Finanzas: Inversión I + D Educación: Adopción Reactiva
Posible Adopción (Tiempo)	75% + para 2030	85% + para 2030	55% + para 2030	90% + para 2030	Todos en crecimiento Sostenido	Velocidad Gobierno > Finanzas > Salud > Educación

Referencias de (Alanazi et al., 2025; Dhingra-Kumar et al., 2021; Qamar et al., 2019)

¿Qué podemos sacar de todo esto?, pues vamos a desglosar un poco lo que hay en ese cuadro comparativo empezando por la convergencia de deepfakes, donde el análisis revela que estos son una amenaza que afecta a todos los sectores, pero con algunas diferencias específicas las cuales son:

- Financiero: El caso documentado del CEO mencionado anteriormente que causo transferencias fraudulentas de 25M.

- Salud: La suplantación de personal médico mediante deepfakes podría comprometer gravemente la seguridad de los pacientes y de sus datos clínicos confidenciales y privados. Exponiéndolos no solo a ellos sino a cualquier medico en el sistema y todos sus pacientes.

- Educación: El 62% de los estudiantes admitió hacer trampa en exámenes online durante 2020 – 2021 con deepfakes permitiendo así la Impersonación de algunos haciéndose pasar por otros.

- Judicial: Los line-ups virtuales pueden ser comprometidos por imágenes sintéticas generadas por I.A.

También tenemos otros problemas provenientes de los costos para cada sector, puesto que es más sencillo para el gobierno pagar 1M – 10M mientras que el sector educación lucha contra 20k – 100k, siendo así debemos tener claro que en caso de fallar cual es más preocupante, siendo: Judicial > Salud > Educativo > Financiero. ¿Pero porque es así?

- Judicial: Bueno empecemos en orden, primeramente, el sector judicial tiene daños irreversibles y permanentes ya que una condena errónea basada en identificación biométrica falsa positiva podría resultar en años de encarcelamiento injusto. Existen varios casos donde varias personas fueron exoneradas mediante evidencia de ADN después de estar encarcelados por una huella dactilar mal interpretada, ósea un error humano.

- Salud: Aunque es fatal, los errores son típicamente resultados de sistemas inadecuados más que de malas intenciones provenientes de las personas o

de errores humanos, los 2.6M de muertes anuales atribuibles a errores de identificación de pacientes representan a identificaciones de pacientes.

- Educativo: Este representa a los falsos conocimientos que una persona con un título y que ejerce puede representar y de su peligro para la sociedad dado que si estas personas con título se gradúan de la modalidad virtual o estos tuvieron que pasar numerosos exámenes hechos con suplantación de identidad o ayudas de inteligencia artificial o de otra persona, podría decirse que esta no posee los conocimientos necesarios para poder ejercer su carrera por lo que las universidades pierden cada vez más prestigio y los títulos pierden su credibilidad y confianza. Por ejemplo, creo que todo preferiríamos ser atendidos en una operación medica por un médico de renombre a ser atendidos por alguien que se graduó usando ayudas externas como chat gpt.
- Financiero: Por último, este se encuentra acá debido a que, aunque de ser vulnerado puede representar pérdidas millonarias, al final de cuentas este no es tan importante como los otros dos ya que el dinero es menos imprescindible a comparación de una formación que afecta a su vez a los jóvenes futuros del país, a las vidas de las personas y de su libertad.

En cuanto a la trayectoria de adaptación de los diferentes sectores podemos decir que son dramáticamente diferentes, Gobierno entre 70 a 85%, Financiero entre 60 a 75%, Salud de entre 50 a 60, Educativo de entre 30 a 40%. Esto debido a la importancia que la sociedad le da a las mismas y del poder adquisitivo que estas tienen, siendo que el gobierno es el más adquisitivo e importante para la sociedad, seguido por el dinero del sector financiero, donde a este lo sigue el sector salud y por último el sector educativo.

Otro patrón critico es el sesgo algorítmico, me refiero a que los sistemas de reconocimiento facial exhiben tasas de error significativamente más altas para personas de piel oscura, mujeres y personas ya de edad lo que deriva en: para el sector judicial puede implicar alguna condena errónea, en el sector salud puede derivar diagnósticos incorrectos, en educación los estudiantes de ciertos grupos demográficos pueden ser falsamente acusados de hacer trampa, en el sector financiero puede resultar en exclusión financiera de algunas poblaciones. (Yang, 2025).

6.2.4 Matriz de Riesgos por Sector

Con base en el análisis comparativo de los cuatro sectores críticos, se desarrolló una matriz de riesgos técnicos para cada uno donde evalúan riesgos categorizados en su probabilidad desde Muy Bajo hasta Muy Alto y el riesgo que genera desde Insignificante Hasta catastrófico.

Tabla 7. Matriz de Riesgos Sector Salud

		Probabilidad				
	SECTOR SALUD	Muy Baja (1)	Baja (2)	Media (3)	Alta (4)	Muy Alta (5)
Riesgo	Insignificante (1)					
	Menor (2)					
	Moderado (3)					**Sesgo Algoritmico en Diagnostico** Menor presicion para minorias o diagnosticos incorrectos
	Mayor (4)				**Conflicto Seguridad vs Accesibilidad (CAACA)** Atuentiacion rapida y sin restricciones	**Falta de Encriptacion Homomorfica (PHBIO)** Principalmente por su costo
	Catastrofico (5)		**Robos de EHR** (Electronic Healt Records) valen entre 10 a 50 veces mas quer una tarjeta de credito	**Deepfakes de Personal Medico** Suplantacion de doctores / enfermeros con deepfakes	**Errores de Identificación de Pacientes** Metodos tradicionales como pulseras	**Complejidad Implementacion PHBIO**

Fuente 1. Autor

Tabla 8. Matriz de Riesgos Sector Financiero

		Probabilidad				
	SECTOR FINANCIERO	Muy Baja (1)	Baja (2)	Media (3)	Alta (4)	Muy Alta (5)
Riesgo	Insignificante (1)					
	Menor (2)					
	Moderado (3)			**Limitaciones (BPC)** Tecnologia emergente solo en la tarjeta		
	Mayor (4)				**Conflicto Seguridad vs Accesibilidad (CAACA)** Atuentiacion rapida y sin restricciones	**Trojans Bancarios Moviles** Incremento por año
	Catastrofico (5)		**Deepfakes de Voz** Clonacion de voz para suplantacion (Caso Hong Kong)	**Vulnerabilidad Smartphones** Vulneracion de biometria		**Sesgo Algoritmico o Exclusion financiera**

Fuente 2. Autor

Tabla 9. Matriz de Riesgos Sector Judicial

		Probabilidad				
	SECTOR JUDICIAL	Muy Baja (1)	Baja (2)	Media (3)	Alta (4)	Muy Alta (5)
Riesgo	Insignificante (1)					
	Menor (2)		**Fallos en Persistencia** las lesiones severas alteran las huellas			
	Moderado (3)			**Limitaciones (BPC)** Tecnologia emergente solo en la tarjeta		
	Mayor (4)				**Vigilancia Masiva sin Orden Judicial** Reconocimiento Facial en Publico	
	Catastrofico (5)			**Lines-ups Virtuales comprometidos por IA** Imágenes Sinteticas		**Condenas Erroneas por Huellas**

Fuente 3. Autor

Tabla 10. Matriz de Riesgos Sector Educativo

	Probabilidad					
	SECTOR EDUCATIVO	Muy Baja (1)	Baja (2)	Media (3)	Alta (4)	Muy Alta (5)
Riesgo	y					
	Menor (2)				**Deteccion Eye Tracking con fallas** El sistemas puede tener fallos	
	Moderado (3)		**Sesgo Algoritmico** Estudiantes falsamente acusados			
	Mayor (4)		**Fallas en Autenticacion Pre-examen** El sistema no identifica bien al estudiante (suplantacion de identidad)	**Deepfakes Suplantacion** Deepfakes faciales para acceder		**Uso de IA en examenes** Estudiantes Consultan a la IA para hacer el Examen
	Catastrofico (5)			**Menor credibilidad de las instituciones** Titulos concedidos a estudiantes sin conocimientos	**Impersonacion en Examenes Online** otra persona realiza el examen	**PRESUPUESTO LIMITADO**

Fuente 4. Autor

6.3 Objetivo 3 (Implementación Guia Sector Educativo)

La presente guía se orienta específicamente a instituciones de educación superior, dado que los escenarios analizados como: control de acceso a campus, exámenes virtuales con protocolo biométrico y gestión de datos en la nube, corresponden a la dinámica operativa y presupuestal de universidades e instituciones técnicas de nivel superior.

6.3.1 Diseño de Matriz para Autenticación Remota

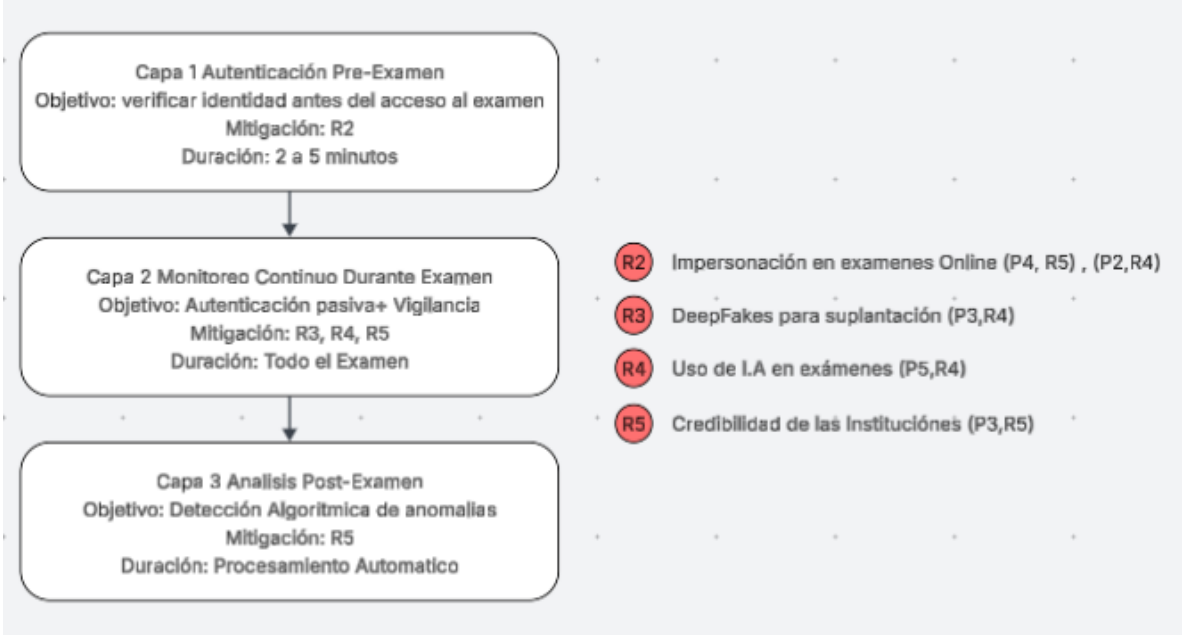
La presente guía constituye una propuesta de diseño arquitectónico y lineamientos técnicos fundamentada en revisión bibliográfica sistematizada, análisis de riesgos y buenas prácticas documentadas. No representa el desarrollo ni despliegue de una plataforma biométrica funcional. Los componentes descritos tales como: detección de deepfakes, evaluación algorítmica y monitoreo conductual, se presentan como tecnologías de referencia con soporte en literatura científica, cuya implementación efectiva requeriría etapas adicionales de experimentación y validación técnica.

Como se mencionó anteriormente, la pandemia aceleró de manera significativa la metodología virtual en el sector educativo tanto por los exámenes virtuales como las clases y calificaciones por lo que las instituciones se tuvieron que adaptar de manera muy drástica lo que las llevo a tener varias vulnerabilidades sobre todo en los exámenes realizados virtualmente esto gracias a que los estudiantes podían tener a la mano varias herramientas a su disposición para hacer trampa e incluso algunos de estos ni siquiera eran los que presentaban el examen, donde el estudio (Labayen et al., 2021) documento un aumento significativo de fraude académico.

Para dar cumplimiento a este objetivo se creará una matriz de implementación escalonada para sistemas de autenticación, basándose tanto en el primer como segundo objetivo, con la idea de mitigar los riesgos presentados en la Tabla 10. Matriz de Riesgos Sector Educativo adaptándose a una limitación de presupuesto.

El sistema propuesto se basa en la arquitectura de (Labayen et al., 2021) implementando 3 capas temporales de autenticación que abordan las vulnerabilidades identificadas en el primer objetivo (ataques de presentación, ataques de inyección y deepfakes) además de los riesgos específicos del sector educativo del objetivo 2.

Figura 7. Diagrama Adaptado de Autenticación



Fuente: Autor con referencias de (Labayen et al., 2021)

Capa 1 Autenticación preexamen: su propósito es el de verificar con certeza la identidad del estudiante antes de otorgarle acceso al examen mitigando el riesgo R2 mostrado en la tabla.

Primero se realiza un registro biométrico del estudiante, esta se almacena en la base de datos de la institución posteriormente esta se compara de la persona que está tomando el examen verificando que sea la misma persona registrada en la base de datos que la que está haciendo el examen donde de ser el mismo estudiante se procedería a la realización del examen activando la detección de vivacidad que monitorea los gestos de la persona que está realizando el examen.

Capa 2 Autenticación pasiva: Esta continua durante toda la sesión del examen y detecta los comportamientos anómalos que se indican en la tabla para mitigar los R3 o R4.

Primero se realiza un reconocimiento facial continuo donde se evalúa que en efecto siga siendo la misma persona, la que está haciendo el examen a la que se está registrada evitando que la persona sea cambiada durante la realización del examen o que hayan 2 en vez de una sola persona realizándolo, además de que esto permite

que el sistema pueda identificar que el estudiante este mirando hacia la pantalla y no hacia el celular o algunas notas escondidas mitigando los riesgos R2, R3.

Esto nos asegura que se implementen medidas contra Deepfakes faciales identificados en las vulnerabilidades del objetivo 1 específicamente la Tabla 4. Vulnerabilidades Biométricas y sus efectos, donde aparecen numerosas vulnerabilidades y los efectos que generan, pero cuales contramedidas se pueden usar para mitigar estas vulnerabilidades?, bueno para cada vulnerabilidad existe una contramedida aplicable que se puede implementar en este sistema las cuales son las siguientes.

Tabla 11. Vulnerabilidades y sus Contramedidas

Vulnerabilidad	Amenaza que Genera	Contramedida
Reconocimiento Facial	**Deepfakes-as-a-Service**	**Análisis forense de profundidad 3D y señales cruzadas:** Estos usan sensores que capturan la profundidad además de múltiples modalidades que nos ayudan a poder detectar las múltiples inconsistencias en videos y o fotos.
Reconocimiento de Voz	**Impersonificación de voz impulsada por Deepfakes Vocales**	**Autenticación multifactor y adaptativa:** Esta es particular ya que no depende exclusivamente de la biometría sino de combinar con factores comportamentales lo que puede ser crucial a la hora de detectarlos gracias a su "doble factor". Esto haciendo que no se dependa únicamente de un solo factor de autenticación como la voz sino de múltiples combinados entre si añadiendo a su vez los factores comportamentales que fueron mencionados anteriormente.

Vulnerabilidad	Amenaza que Genera	Contramedida
Detección de Vivacidad Tradicional	**Identidades sintéticas hibridas**	**Detección de la vivacidad avanzada:** Básicamente se trata acerca de pruebas estáticas como el parpadeo, patrones espectrales, análisis de micro textura, entre otros que nos pueden ayudar a detectar algunos deepfakes enfocados en esta modalidad.
Almacenamiento en Nube	**Ataques coordinados 24/7**	**Encriptación y protección de plantillas (incluyendo técnicas avanzadas):** Como las ya mencionadas anteriormente, la encriptación homomórfica que no requiere de desencriptar los datos biométricos, lo cual hace inútiles los datos que se logren extraer.

Fuente: Autor con referencias de (Unmasking deepfakes, Springer, 2025)

Capa 3 Evaluación algorítmica automatizada: Finalmente se realiza una evaluación algorítmica automatizada de todos los datos capturados para identificar anomalías y generar una puntuación la cual determinará si el estudiante realizo o no realizo trampa donde dependiendo de donde el sistema haya detectado la infracción tendrá más o menos peso, de la siguiente manera.

Tabla 12. Peso de eventos marcados

Evento	Indicador de Fraude	Peso
Rostro desaparece por 10 segundos o mas	Posible reemplazo de la persona	Alto
Multiples rostros detectados	Ayuda de un terero	Critico
Cambio abrupto del patron de tecleo	Posible cambio de persona	Alto
Mirada prolongada fuera de la pantalla	Consulta externa como notas u otra pantalla	Medio
Multiples voces	Colaboración	Alto
Patron del mouse incosistente	Posible cambio de persona	Medio

Fuente: Autor

A continuación, se presentará una tabla comparativa de lo que podría incluir las instituciones del sector educativo dependiendo de su presupuesto referente al sistema. Cabe recalcar que Los valores corresponden a referencias de mercado consultadas en 2024-2025 (ver referencias de cada tabla) y deben considerarse como estimaciones orientativas sujetas a variación según contexto institucional, ubicación geográfica y volumen de usuarios.

Tabla 13. Reconocimiento Facial Pre-Examen

Caracteristicas Presupuesto en Dolares $ Nivel	Básico 20k a 40k Tecnologia	Intermedio 40k a 80k Justificación Tecnica	Avanzado 80k a 150k Enlaces de Referencia	Enlace
Basico	Facial basico	Usa algoritmos open-source de reconocimiento facial 2D. Precisión: ~95-97% bajo condiciones ideales. Suficiente para verificación 1:1 (comparar rostro con foto ID), pero vulnerable a ataques de presentación sofisticados (deepfakes). ¿Por qué NO avanzado? No incluye CNN profundas (FaceNet, ArcFace) que alcanzan 99%+ de precisión.	[1] SIA: Facial Recognition 99%+ accuracy[2] Keyless: Basic vs Advanced FR	(Parker & Ray, 2022; Keyless, 2023)
Intermedio	Facial Avanzado (CNN: FaceNet/ArcFace)	Implementa redes neuronales convolucionales (CNN) profundas entrenadas en millones de rostros. Precisión: 99-99.5%. Mejor manejo de variaciones (iluminación, ángulo, expresión). ¿Por qué NO multimodal? Solo usa facial, no integra iris/huella.	[3] Envista: CNN 99%+ accuracy[4] ROC.ai: Face Recognition SOTA	(Envista Forensics, 2024; ROC.ai, 2023)
Avanzado	Multimodal OBLIGATORIO (Facial + Iris + Huella)	Combina tres modalidades biométricas. Facial (99%+) + Iris (99.9%+) + Huella (99%+) = Precisión combinada 99.99%+. Previene bypass de una sola modalidad. ¿Por qué caro? Requiere hardware especializado (cámara IR para iris $500-2K, lector huella $200-400).	[5] Incode: Fingerprint vs Facial[6] NEC: Multimodal Biometrics	(Incode Technologies, 2024; NEC Corporation, 2024)

Fuente: Autor con referencias de (Parker & Ray, 2022; Keyless, 2023; Envista Forensics, 2024; ROC.ai, 2023; Incode Technologies, 2024; NEC Corporation, 2024)

Tabla 14. Reconocimiento Iris Pre-Examen

Caracteristicas Presupuesto en Dolares $ Nivel	Básico 20k a 40k Inclusion	Intermedio 40k a 80k Justificación Tecnica	Avanzado 80k a 150k Enlaces de Referencia	Enlace
Básico	NO	Razón: Iris requiere hardware especializado (cámara NIR $300-2K por unidad). No es costo-efectivo para presupuesto <$40K. Alternativa: Solo facial básico es suficiente para verificación 1:1 pre-examen.	[7] CGDev: Iris scanners $300-500[8] Verazial: Iris high cost	(Gelb & Krishnan, 2018; Verázial, 2025)
Intermedio	OPCIONAL	Razón: Presupuesto permite comprar 1-2 cámaras iris para casos críticos (exámenes de medicina, ingeniería). Precisión iris: 99.9% (mejor que facial 99%). ¿Por qué opcional? No todos los estudiantes tienen acceso a cámara NIR en casa para exámenes remotos. Requiere envío de hardware.	[9] TipsOI: Iris 99.9% accuracy[10] Security101: Iris cost considerations	(TipsOI, 2024; Security101, 2022)
Avanzado	OBLIGATORIO	Razón: Para exámenes críticos, iris es MANDATORIO como segunda modalidad. Previene fraude con gemelos idénticos (facial no puede diferenciarlos, iris sí). Implementación: Envío de cámaras USB NIR (~$300) a estudiantes o instalación en centros de examen supervisados.	[11] Bayometric: Iris for identical twins[12] Wikipedia: Iris recognition Kenya education	(Bayometric, 2024; Wikipedia, 2025)

Fuente: Autor con referencias de (Gelb & Krishnan, 2018; Verázial, 2025; TipsOI, 2024; Security101, 2022; Bayometric, 2024; Wikipedia, 2025)

Tabla 15. Detección de Vivacidad Liveness Detección

Caracteristicas Presupuesto en Dolares $ Nivel	Básico 20k a 40k Tipo	Intermedio 40k a 80k Justificación Tecnica	Avanzado 80k a 150k Enlaces de Referencia	Enlace
Básico	Solo ACTIVA	Qué incluye: Solicita gestos aleatorios (parpadeo, sonrisa, girar cabeza). ¿Por qué NO pasiva? Liveness pasiva requiere análisis ML de textura de piel, reflejos, profundidad 3D → Costo computacional alto, requiere servidores GPU (~$3K-5K). Activa usa solo webcam estándar. Vulnerabilidad: Deepfakes avanzados pueden simular parpadeos/gestos.	[13] Regula: Active vs Passive Liveness[14] Keyless: Passive <300ms vs Active 2-3s	((Regula Forensics, 2025; Keyless, 2024)
Intermedio	Activa + Pasiva (sin rPPG)	Qué incluye: Activa (gestos) + Pasiva (análisis textura, reflejo ocular, detección 2D/3D). ¿Por qué NO rPPG? rPPG (Remote Photoplethysmography - detección flujo sanguíneo) requiere cámaras alta velocidad (60+ FPS) + algoritmos avanzados → Agrega $10K-20K al costo. Pasiva básica detecta fotos/videos pero no deepfakes en tiempo real.	[15] Sumsub: Liveness ISO/IEC 30107-3[16] HyperVerge: Passive single-image	(Sumsub, 2025; HyperVerge, 2024)
Avanzado	Multi-espectral + rPPG + Integración espectral	Qué incluye: (1) Multi-espectral: Cámara RGB + IR + UV detecta materiales sintéticos vs piel real. (2) rPPG: Analiza variaciones de color en rostro causadas por flujo sanguíneo (imposible en video pregrabado). (3) Análisis temporal: Micro-expresiones, patrones de respiración. Costo: Cámaras multi-espectrales $1K-3K + Procesamiento GPU $5K + Software especializado $10K-20K.	[17] Facia: Active vs Passive advanced[18] Daon: rPPG liveness detection	(Facia, 2024; Daon, 2025)

Fuente: Autor con referencias de (Regula Forensics, 2025; Keyless, 2024; Sumsub, 2025; HyperVerge, 2024; Facia, 2024; Daon, 2025)

Tabla 16. Biometría Comportamental

Caracteristicas Presupuesto en Dolares $ Nivel	Básico 20k a 40k Que Captura?	Intermedio 40k a 80k Justificación Tecnica	Avanzado 80k a 150k Enlaces de Referencia	Enlace
Básico	Solo Tecleo (Keystroke Dynamics)	Qué mide: Tiempo entre pulsaciones de teclas, velocidad de tipeo, errores de tecleo. ¿Por qué NO mouse? Análisis de mouse (velocidad, aceleración, patrones de clics) requiere SDK especializado (TypingDNA Pro: $2K-5K/año vs Free tier solo tecleo). Tecleo es suficiente para detectar cambios de persona (velocidad tecleo cambia 30-50%	[19] TypingDNA: Keystroke dynamics[Monografía]: Objetivo 1 - Tabla 3	(TypingDNA, 2024; BehavioSec, 2024)
Intermedio	Tecleo + Mouse	Qué agrega: Patrones de movimiento de mouse (velocidad angular, trayectorias curvas vs rectas, tiempos de inactividad). Utilidad: Si estudiante A toma examen pero otra persona responde preguntas, mouse patterns revelan cambio de usuario. Costo: TypingDNA Pro + MouseDynamics library: $5K-10K/año.	[20] BehavioSec: Mouse dynamics[Monografía]: Actividad 6.3.1 - Capa 2	(BioCatch, 2025)
Avanzado	Completo (Tecleo + Mouse + Navegación + Presión + Gait)	Qué agrega: (1) Navegación: Orden de respuesta de preguntas, tiempo por pregunta. (2) Presión de tecla (requiere teclado capacitivo). (3) Gait analysis (análisis de marcha si estudiante se levanta - requiere sensor de movimiento). Utilidad: Perfil comportamental 360° → Detecta hasta estrés anómalo (cambio de presión teclas).	[21] BioCatch: Behavioral biometrics[22] NuData: Behavioral analytics	(NuData Security, 2024)

Fuente: Autor con referencias de (TypingDNA, 2024; BehavioSec, 2024; BioCatch, 2025; NuData Security, 2024)

Tabla 17. Audio Ambiental Detección de múltiples voces

Caracteristicas Presupuesto en Dolares $ Nivel	Básico 20k a 40k Tecnologia	Intermedio 40k a 80k Justificación Tecnica	Avanzado 80k a 150k Enlaces de Referencia	Enlace
Básico	NO	Razón: Análisis de audio requiere micrófono abierto durante examen (2-3 horas) → Grabación 500MB-1GB por estudiante → Storage $0.023/GB en S3 × 1,000 estudiantes = $23-50/examen. Procesamiento NLP: $0.01-0.05/minuto → $1.2-6/estudiante. Presupuesto <$40K no puede costear procesamiento de 1,000+ estudiantes.	[29] AWS Transcribe pricing[30] Google Speech-to-Text pricing	(AWS, 2025; Google Cloud, 2025)
Intermedio	Básico (Detección voces sin NLP)	Qué hace: Detecta presencia de múltiples voces usando análisis de frecuencia (no transcribe contenido). Algoritmo simple: (1) Detecta picos de energía en audio. (2) Clasifica frecuencia (voz masculina ~100Hz, femenina ~200Hz). (3) Alerta si detecta >1 voz simultánea. Costo: Procesamiento local (no cloud) → $0 en storage, solo CPU.	[31] Pyannote: Speaker diarization[32] Simple voice detection algorithms	(Bredin et al., 2020; Real Python, 2024)
Avanzado	Completo (NLP con GPT-4 - Transcripción + Análisis semántico)	Qué hace: (1) Transcribe audio completo (AWS Transcribe/Google STT). (2) Analiza contenido con GPT-4 API: Detecta si estudiante hace preguntas ("¿Cuál es la respuesta a...?") o recibe instrucciones ("La respuesta correcta es..."). (3) Clasifica como "colaboración" si detecta intercambio pregunta-respuesta. Costo: GPT-4 API: $0.03/1K tokens × 10K tokens/examen (2 horas) = $0.30/estudiante × 1,000 = $300/examen. Anual (10 exámenes): $3K.	[33] OpenAI GPT-4 API pricing[34] Azure Cognitive Services	(OpenAI, 2025; Microsoft Azure, 2025)

Fuente: Autor con referencias de (AWS, 2025; Google Cloud, 2025; Bredin et al., 2020; Real Python, 2024; OpenAI, 2025; Microsoft Azure, 2025)

Estas a su vez cumplen con el marco normativo del GDPR mencionado en el Objetivo 1, donde se nos menciona que el estudiante debe de dar su consentimiento explicito para su captura biométrica, además de la privacidad como comodidad mencionada anteriormente, adicionalmente el estudiante puede solicitar una copia de sus datos biométricos que la institución deberá de proveer en un lapso de 30 días, también cuando el estudiante se gradué estos datos biométricos deberán de ser borrados si el estudiante lo solicita y finalmente si el estudiante fue marcado como que realizo fraude en la prueba este debe de recibir una explicación detallada por una persona encargada.

6.3.2 Diseño de Sistemas de Control Acceso Físico al Campus

El control de acceso físico en entornos educativos sobre todo en instituciones educativas representa un desafíos significativo debido a la alta circulación de los estudiantes, docentes, administrativos y algunos visitantes, desafío que la universidad santo tomás a afrontado exitosamente gracias a su implementación de mecanismos como el uso de QR para su ingreso y acceso a la universidad; sin embargo, este puede presentar algunas vulnerabilidades que la biometría facial o de huella puede cubrir de una mejor manera.

En este contexto la incorporación de tecnologías biométricas, como el reconocimiento facial y de huella dactilar, no solo nos permite fortalecer los mecanismos de autenticación ofreciendo así mayores garantías de seguridad donde con base en los riesgos identificados a lo largo de esta monografía especialmente aquellos asociados al uso de inteligencia artificial para la generación de deepfakes y ataques de inyección biométrica, se propone un modelo de control de acceso físico que integra múltiples capas de seguridad combinando las diferentes tecnologías orientadas a mitigar dichas vulnerabilidades.(*AI Deepfakes: A Threat to Facial Biometric Authentication*, 2025; Bendiab et al., 2025)

Este modelo no solo mitiga las vulnerabilidades, sino que además garantiza la detección de intentos de fraude y el cumplimiento de los principios normativos relacionados con la protección de datos biométricos, además de la autenticidad del usuario, a continuación, se mostrara una tabla con los debidos pasos que describe la implementación de dichas tecnologías y su contribución a la mitigación de los riesgos y el riesgo mitigado.

Tabla 18. Implementación de las tecnologías

Pasos	Tecnologia	¿Que hace?	Solucion	Ataque Mitigado
1	Identificacion Biometrica	usa tecnologías de reconocimiento facial y de huella	Al tener que mostrar el rostro o la huella, la persona debe de estar previamente en la base de datos de la universidad donde solo la persona reguistrada tiene acceso y no un impostor	Suplantación de identidad
2	Liveness Detection	hace un análisis de profundidad facial 3D y respuesta a estímulos aleatorios.	Ayuda a mitigar el ataque de algún posible deepfakes o uso de imágenes y videos	Deepfakes / Replay Atacks
3	Capa de Deteccion Multifactor (MFAA)	usa mas de una tecnología de reconocimiento como ya usa la universidad siendo este un aplicativo movil con codigo dinamico	En caso de una posible vulneración el atacante debera de implementarlo en las demas capas para poder ingresar lo que resuelve en que sera dependiendo de la vulneracion cada vez mas dificil	Credential stuffing / bypass
4	Capa de control contextual	El sistema usa variables como la hora y el rol del usuario para permitir o no el acceso	Evita que un atacante que se hace pasar por ejemplo por estudiante quiera ingresar en un horario que no es el abitual lo que genera que no pueda ingresar	Accesos anómalos
5	Seguridad Fisica	Una entidad es la encargada de que no exista alguna actividad sospechosa aumentado la seguridad	Evita que el atacante pueda realizar sus ataques de forma evidente o que trate de ingresar a la fuerza maximizanod la seguridad	Intrusión directa

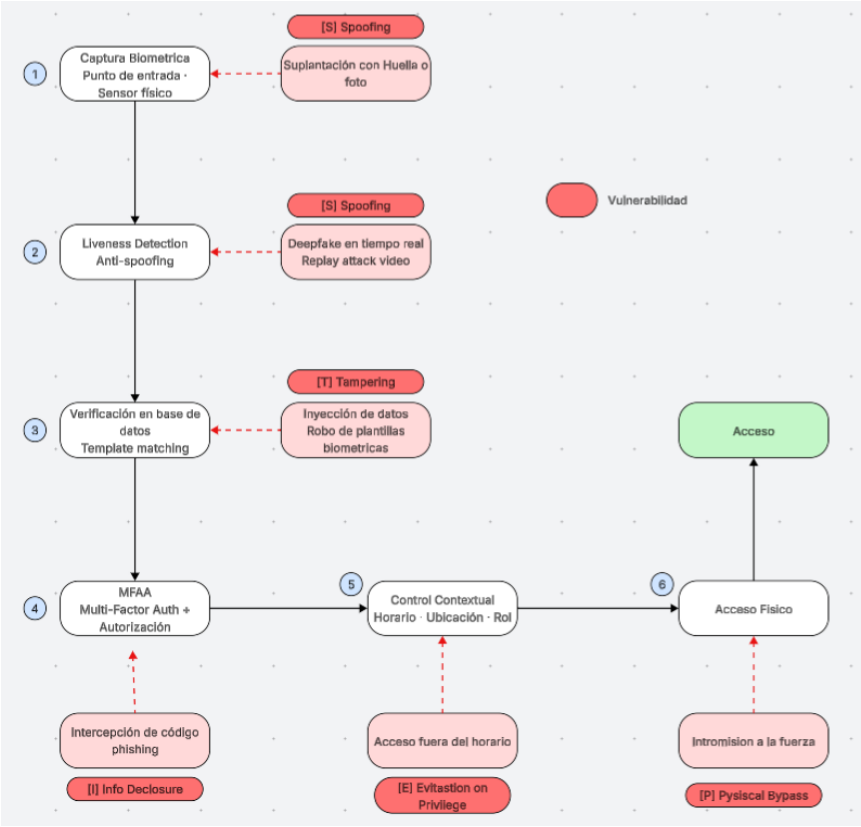
Fuente: Autor con referencias en el primer y segundo objetivo

La arquitectura del sistema de control para el acceso al campus sería el siguiente, donde se ilustra de manera secuencial cada una de las etapas del proceso de autenticación, así como las posibles vulnerabilidades, previamente identificadas en la Tabla 14. Reconocimiento Iris Pre-Examen, permitiendo evidenciar los puntos más críticos del sistema.

El modelo nos muestra un enfoque de seguridad en múltiples capas en el cual nos muestra cada uno de los pasos y de las posibles vulnerabilidades que pueden atacar el sistema, las cuales fueron mencionadas en la tabla anterior.

Es importante tener en cuenta que aunque la arquitectura sigue un paso a paso el o los atacantes no, por lo que se puede presentar un ataque de manera combinada que incrementa la complejidad de su detección y acción, por ejemplo un ataque de deepfake podría complementarse con técnicas de ingeniería social para evadir mecanismos multifactor, en ese caso el diseño propuesto por capas permite mitigar estos escenarios al requerir que el atacante supere no uno sino los múltiples desafíos que tiene este sistema.

Figura 8. Diagrama De Flujo Modelo de Amenazas STRIDE del Acceso Físico al Campus



Fuente: Autor

6.3.3 Desarrollo de Recomendaciones de arquitectura del almacenamiento de datos de Cloud

Habiendo ya desarrollado unos fundamentos técnicos y operacionales para sistemas de autenticación biométrica en el sector educativo, desarrollando que datos biométricos se recopilan y como se procesan, esta actividad final aborda la pregunta que se ha podido generar en las últimas 2 actividades, donde y como se almacenan estos datos biométricos de los estudiantes de forma segura, cumpliendo con obligaciones normativas y mitigando riesgos de brechas de seguridad.

La importancia de esta actividad radica en cómo se mencionó antes en la actividad 6.1.1 Revisión sistemática de literatura sobre Ética biométrica, los datos biométricos son de “categoría especial de datos personales” según GDPR Articulo 9, y a diferencia de contraseñas o números de identificación, estos no pueden ser cambiados si son comprometidos. En caso de ser comprometidos podrían representar un daño permanente e irreversible para los afectados. Sin mencionar que la matriz de riesgos del primer objetivo específico: Tabla 5. Matriz de Riesgos Identifico el robo de bases de datos biométricas como un riesgo catastrófico. También la matriz de riesgos del sector educativo Tabla 10. Matriz de Riesgos Sector Educativo señalo que el “presupuesto limitado” de un nivel de criticidad de 25, es el más alto y la principal limitante que afecta la capacidad de instituciones educativas para implementar una infraestructura de almacenamiento de alto costo.

A lo largo del documento se hablan de diferentes sistemas propuestos para generar 3 tipos de datos. La siguiente tabla presenta un inventario detallado de estos datos indicando su nivel de sensibilidad, las actividades que producen y sus características distintivas.

Tabla 19. Sistemas propuestos y sus características

Sistema Propuesto	Sensibilidad	Menciones	Caracteristicas
Templates Biométricos	Alta	Actividad 6.3.1 (Autenticación Remota) / Actividad 6.3.2 (Acceso Fisico)	Es inmutable y requiere encriptacion obligatoria
Logs de Transacciones	Media	Actividad 6.3.1 / Actividad 6.3.2	Es inmutable y requiere una retencion de al menos 5 años
Datos Administrativos	Baja	Actividad 6.3.1 / Actividad 6.3.2	Requiere una vinculacion segura con los templates

Fuente: Autor

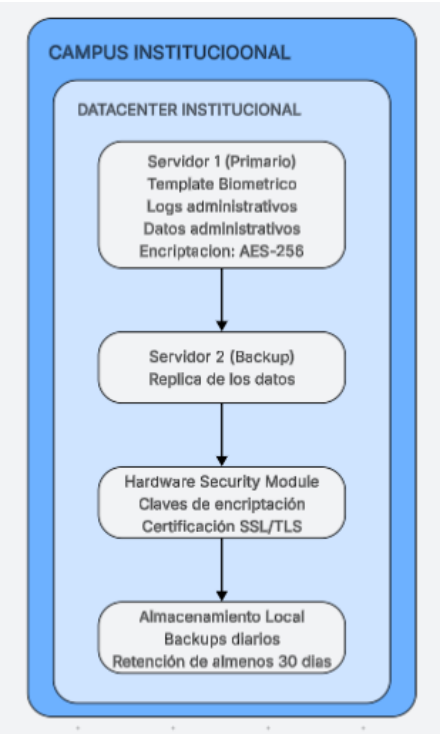
Para visualizar claramente esta jerarquía de sensibilidad y las capas de protección requeridas a continuación la Tabla 16 presenta una pirámide invertida donde la amplitud de cada nivel representa tanto el volumen de datos como el nivel de protección necesario.

Figura 9. Pirámide clasificada por sensibilidad

Fuente: Autor

Estos (Templates, logos, administrativos) se almacenarán en servidores físicos propiedad de la institución, ubicados en datacenters institucionales, basándome en el análisis de sensibilidad presentado a continuación, se mostrará la arquitectura de dichos sistemas.

Figura 10. Datacenters Institucionales



Fuente: Autor

El servidor 1 (Primario): Almacena Templates biométricos, logs y datos administrativos con encriptación. Este servidor maneja todas las operaciones de matching biométrico en tiempo real, procesando solicitudes de autenticación tanto de exámenes online (Actividad 6.3.1) como de torniquetes de acceso físico (Actividad 6.3.2).

El servidor 2 (Backup): Es el que mantiene una réplica síncrona de todos los datos del servidor primario, en caso de falla del servidor principal. Esta redundancia garantiza que el sistema de control de acceso físico continúe operando incluso si el servidor primario experimenta problemas técnicos, evitando situaciones donde estudiantes queden bloqueados fuera de las instalaciones.

El Hardware Security Module (HSM): Es un dispositivo físico especializado que almacena las claves de encriptación utilizadas para proteger Templates biométricos.

El Almacenamiento Local (NAS/SAN): Es un sistema de backup automatizado que ejecuta respaldos incrementales diarios de todos los datos, con retención de 30 días. Estos Backus permiten recuperación ante corrupción de datos, ransomware, o errores de administración.

Esto nos proporciona varias ventajas y desventajas que deben ser cuidadosamente evaluados por cada institución según su perfil de riesgo y capacidad presupuestal, dichas ventajas y desventajas serán mostradas en la tabla a continuación.

Tabla 20. Ventajas y Desventajas

VENTAJAS	DESVENTAJAS
control físico total de los servidores	Costo Inicial elevado
acceso restringido al datacenter	Costo Operacional Continuo
Cumplimiento del GDPR	Escalabilidad Limitada
No dependencia de Terceros	Riesgos Instalacion Fisica

Fuente: Autor

El objetivo final es proporcionar a las instituciones educativas un conjunto de opciones arquitectónicas fundamentadas que permitan tomar decisiones informadas basadas en sus circunstancias específicas, siempre manteniendo como prioridad absoluta la protección de los datos biométricos irreemplazables de su comunidad estudiantil.

Formulario de la guía de implementación (3 Objetivo específico):

CUESTIONARIO GUíA DE IMPLEMENTACIÓN

El presente cuestionario tiene como objetivo evaluar la propuesta de implementación de sistemas de autenticación biométrica con inteligencia artificial presentada en la monografía "Desafíos Éticos y Normativos de la Autenticación Biométrica con Inteligencia Artificial". Su opinión es valiosa para validar la viabilidad, pertinencia y aplicabilidad de las soluciones propuestas para el sector educativo.
Tiempo estimado 10 minutos.

* Indica que la pregunta es obligatoria

DECLARACIÓN DE CONSENTIMIENTO *

- [ ] **Acepto que mis respuestas sean utilizadas con fines académicos en el análisis y conclusiones de la monografía "Desafíos Éticos y Normativos de la Autenticación Biométrica con Inteligencia Artificial".**
- [ ] **Autorizo que mi nombre e institución sean mencionados en los agradecimientos (opcional).**
- [ ] **Prefiero mantener mi participación anónima.**

Evaluación del 3 Objetivo

Seleccione la opción que mejor represente su grado de acuerdo según la siguiente escala:

(1) Totalmente en desacuerdo, (2) En desacuerdo, (3) Neutral / (4) No estoy seguro, (5) De acuerdo, (6) Totalmente de acuerdo

DISEÑO DE MATRIZ PARA AUTENTICACIÓN REMOTA Actividad 6.3.1

Esta actividad propone un sistema de autenticación biométrica para exámenes online con 3 capas (pre-examen, durante examen, post-examen) y 3 niveles de implementación según presupuesto

El fraude académico en exámenes online es un problema real y significativo * que requiere soluciones tecnológicas.

(1) Totalmente en desacuerdo, (2) En desacuerdo, (3) Neutral / (4) No estoy seguro, (5) De acuerdo, (6) Totalmente de acuerdo

1	2	3	4	5	6
☆	☆	☆	☆	☆	☆

El sistema de 3 capas (pre-examen, durante examen, post-examen) aborda de manera integral los riesgos de fraude académico. *

(1) Totalmente en desacuerdo, (2) En desacuerdo, (3) Neutral / (4) No estoy seguro, (5) De acuerdo, (6) Totalmente de acuerdo

1 2 3 4 5 6

☆ ☆ ☆ ☆ ☆ ☆

La propuesta mitiga efectivamente los riesgos identificados (R2: Suplantación, R3: Deepfakes, R4: Uso de IA, R5: Credibilidad). *

(1) Totalmente en desacuerdo, (2) En desacuerdo, (3) Neutral / (4) No estoy seguro, (5) De acuerdo, (6) Totalmente de acuerdo

1 2 3 4 5 6

☆ ☆ ☆ ☆ ☆ ☆

Las tecnologías propuestas (reconocimiento facial, detección de vivacidad, biometría comportamental) son técnicamente viables para implementar. *

(1) Totalmente en desacuerdo, (2) En desacuerdo, (3) Neutral / (4) No estoy seguro, (5) De acuerdo, (6) Totalmente de acuerdo

1 2 3 4 5 6

☆ ☆ ☆ ☆ ☆ ☆

DISEÑO DE SISTEMAS DE CONTROL DE ACCESO FÍSICO AL CAMPUS
Actividad 6.3.2
Esta actividad propone reemplazar el sistema de códigos QR con un sistema biométrico multimodal (facial + huella dactilar) para control de acceso a instalaciones educativas, con 5 capas de seguridad.

El sistema QR actual representa un riesgo de seguridad significativo que justificaría una inversión adicional en un sistema de biometría? *

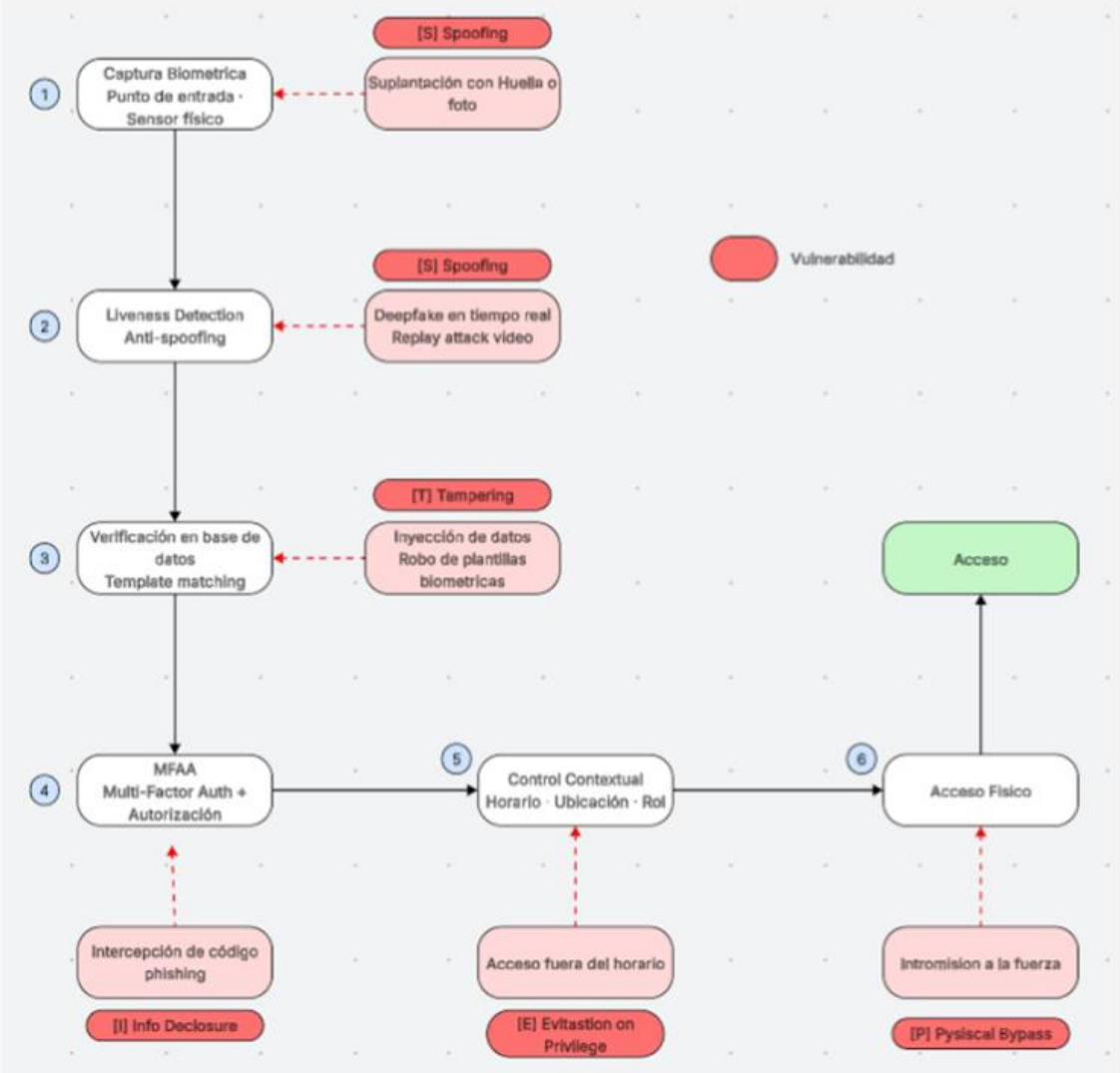
(1) Totalmente en desacuerdo, (2) En desacuerdo, (3) Neutral / (4) No estoy seguro, (5) De acuerdo, (6) Totalmente de acuerdo

1 2 3 4 5 6

☆ ☆ ☆ ☆ ☆ ☆

El Diagrama modelo de Amenazas STRIDE del Acceso Físico al Campus (Diagrama de Flujo 2) ilustra claramente el flujo de autenticación y las vulnerabilidades mitigadas. *

(1) Totalmente en desacuerdo, (2) En desacuerdo, (3) Neutral / (4) No estoy seguro, (5) De acuerdo, (6) Totalmente de acuerdo


[S] Spoofing
1
Captura Biometrica
Punto de entrada · Sensor físico
Suplantación con Huella o foto
Vulnerabilidad
[S] Spoofing
2
Liveness Detection
Anti-spoofing
Deepfake en tiempo real
Replay attack video
[T] Tampering
3
Verificación en base de datos
Template matching
Inyección de datos
Robo de plantillas biometricas
Acceso
4
MFAA
Multi-Factor Auth + Autorización
5
Control Contextual
Horario · Ubicación · Rol
6
Acceso Fisico
Intercepción de código phishing
[I] Info Declosure
Acceso fuera del horario
[E] Evitastion on Privilege
Intromision a la fuerza
[P] Pysiscal Bypass

La combinación de reconocimiento facial + huella dactilar ofrece mayor seguridad que otra que solo utilice una modalidad ? *

(1) Totalmente en desacuerdo, (2) En desacuerdo, (3) Neutral / (4) No estoy seguro, (5) De acuerdo, (6) Totalmente de acuerdo

1 2 3 4 5 6

☆ ☆ ☆ ☆ ☆ ☆

Las contramedidas propuestas mitigan efectivamente los ataques identificados (suplantación, deepfakes, inyección de datos, phishing, intromisión a la fuerza). *

(1) Totalmente en desacuerdo, (2) En desacuerdo, (3) Neutral / (4) No estoy seguro, (5) De acuerdo, (6) Totalmente de acuerdo

1 2 3 4 5 6

☆ ☆ ☆ ☆ ☆ ☆

La tabla de tecnologías y soluciones (Tabla 13) proporciona claridad sobre cómo cada capa mitiga riesgos específicos. *

(1) Totalmente en desacuerdo, (2) En desacuerdo, (3) Neutral / (4) No estoy seguro, (5) De acuerdo, (6) Totalmente de acuerdo

Pasos	Tecnologia	¿Que hace?	Solucion	Ataque Mitigado
1	Identificacion Biometrica	usa tecnologías de reconocimiento facial y de huella	Al tener que mostrar el rostro o la huella, la persona debe de estar previamente en la base de datos de la universidad donde solo la persona reguistrada tiene acceso y no un impostor	Suplantación de identidad
2	Liveness Detection	hace un análisis de profundidad facial 3D y respuesta a estímulos aleatorios.	Ayuda a mitigar el ataque de algún posible deepfakes o uso de imágenes y videos	Deepfakes / Replay Atacks
3	Capa de Deteccion Multifactor (MFAA)	usa mas de una tecnología de reconocimiento como ya usa la universidad siendo este un aplicativo movil con codigo dinamico	En caso de una posible vulneración el atacante debera de implementarlo en las demas capas para poder ingresar lo que resuelve en que sera dependiendo de la vulneracion cada vez mas dificil	Credential stuffing / bypass
4	Capa de control contextual	El sistema usa variables como la hora y el rol del usuario para permitir o no el acceso	Evita que un atacante que se hace pasar por ejemplo por estudiante quiera ingresar en un horario que no es el abitual lo que genera que no pueda ingresar	Accesos anómalos
5	Seguridad Fisica	Una entidad es la encargada de que no exista alguna actividad sospechosa aumentado la seguridad	Evita que el atacante pueda realizar sus ataques de forma evidente o que trate de ingresar a la fuerza maximizanod la seguridad	Intrusión directa

1 2 3 4 5 6

☆ ☆ ☆ ☆ ☆ ☆

El sistema propuesto es aplicable para instituciones con alta circulación de personas (estudiantes, docentes, administrativos, visitantes). *

(1) Totalmente en desacuerdo, (2) En desacuerdo, (3) Neutral / (4) No estoy seguro, (5) De acuerdo, (6) Totalmente de acuerdo

1	2	3	4	5	6
☆	☆	☆	☆	☆	☆

ARQUITECTURA DE ALMACENAMIENTO DE DATOS CLOUD Actividad 6.3.3

Esta actividad propone una arquitectura de almacenamiento 100% on-premise para templates biométricos, logs y datos administrativos, con servidores primario/backup, HSM, y sistemas de backup locales.

En general, considero que la arquitectura de almacenamiento propuesta protege adecuadamente los datos biométricos y es recomendable para la Universidad Santo Tómas Seccional Tunja. *

(1) Totalmente en desacuerdo, (2) En desacuerdo, (3) Neutral / (4) No estoy seguro, (5) De acuerdo, (6) Totalmente de acuerdo

1	2	3	4	5	6
☆	☆	☆	☆	☆	☆

EVALUACIÓN INTEGRAL DEL OBJETIVO 3

La guía aborda de manera completa los aspectos técnicos, económicos, éticos y normativos de la implementación biométrica. *

(1) Totalmente en desacuerdo, (2) En desacuerdo, (3) Neutral / (4) No estoy seguro, (5) De acuerdo, (6) Totalmente de acuerdo

1	2	3	4	5	6
☆	☆	☆	☆	☆	☆

Las tres actividades (Autenticación Remota, Acceso Físico, Almacenamiento Cloud) se complementan y forman una guía integral. *

(1) Totalmente en desacuerdo, (2) En desacuerdo, (3) Neutral / (4) No estoy seguro, (5) De acuerdo, (6) Totalmente de acuerdo

1 2 3 4 5 6

☆ ☆ ☆ ☆ ☆ ☆

Recomendaría a la Universidad considerar seriamente la implementación de las soluciones propuestas en esta guía. *

(1) Totalmente en desacuerdo, (2) En desacuerdo, (3) Neutral / (4) No estoy seguro, (5) De acuerdo, (6) Totalmente de acuerdo

1 2 3 4 5 6

☆ ☆ ☆ ☆ ☆ ☆

Retroalimentación de los evaluadores de la encuesta: Con el propósito de validar la viabilidad técnica e integridad de la guía propuesta, se diseñó una encuesta de evaluación dirigido a un profesional experto en el área. El cual fue respondido por un docente de la Universidad Santo Tomás Seccional Tunja, con especialización en Inteligencia Artificial, Machine Learning y educación virtual, y con bastante experiencia.

Los resultados de la evaluación reflejan una valoración bastante positiva de la propuesta ya que en la mayoría de sus dimensiones. El evaluador otorgó la puntuación máxima (6 - Totalmente de acuerdo) a aspectos clave como: la existencia real del fraude académico en entornos digitales y la necesidad de soluciones tecnológicas; la efectividad del sistema de tres capas para mitigar riesgos como la suplantación, el uso de deepfakes y el empleo de IA en exámenes; la viabilidad técnica de las tecnologías propuestas (reconocimiento

facial, detección de vivacidad y biometría comportamental); la pertinencia de reemplazar el sistema QR actual por un esquema biométrico más robusto; la superioridad de la autenticación multimodal frente a una sola modalidad biométrica; y la escalabilidad del sistema para instituciones con alta circulación de personas.

En conjunto, la retroalimentación obtenida respalda la validez técnica y la relevancia institucional de la propuesta.

Retroalimentación de los evaluadores del 3 Objetivo de la Monografía: En el proceso de validación académica de la presente monografía, un evaluador con experticia en seguridad informática de la universidad santo tomas revisó el desarrollo del tercer objetivo específico y formuló cuatro observaciones orientadas a fortalecer la rigurosidad, claridad y coherencia del trabajo. A continuación, se describen cada una de estas observaciones y los ajustes que fueron aplicados en consecuencia.

Primera observación (Delimitación del contexto educativo): El evaluador señaló que el documento hacía referencia genérica al "sector educativo" sin precisar si la guía estaba dirigida a educación básica, media o superior. En respuesta a esta observación, se incorporó al inicio del desarrollo del Objetivo 3 una delimitación explícita que establece que la guía se orienta específicamente a instituciones de educación superior.

Segunda observación (Naturaleza y alcance de la propuesta): El evaluador recomendó aclarar que la propuesta corresponde a una guía de diseño arquitectónico y lineamientos técnicos, y no al desarrollo de una plataforma biométrica funcional. Este ajuste fue aplicado mediante la incorporación de un párrafo aclaratorio al inicio de la sección 6.3.1, el cual establece de manera explícita que la guía está fundamentada en revisión bibliográfica sistematizada, análisis de riesgos y buenas prácticas documentadas, y que los componentes descritos como detección de deepfakes, evaluación algorítmica y monitoreo conductual se presentan como tecnologías de referencia con soporte en literatura científica.

Tercera observación (Precisión sobre el rol de los componentes de IA): El evaluador indicó la necesidad de aclarar si los elementos de inteligencia artificial, reconocimiento facial, detección de vivacidad, análisis de patrones y machine learning, se presentan como tecnologías de referencia bibliográfica o como mecanismos implementados dentro de la investigación. Esta observación queda resuelta con el mismo ajuste descrito anteriormente, que delimita explícitamente el nivel de desarrollo alcanzado como una propuesta de revisión y diseño, no

como un desarrollo aplicado, fortaleciendo así la rigurosidad académica de este trabajo.

Cuarta observación (Viabilidad económica y contextualización de costos): El evaluador sugirió contextualizar mejor los valores económicos asociados a la infraestructura propuesta, indicando si corresponden a estimaciones teóricas, referencias de mercado o estudios comparativos, y considerando instituciones con diferentes capacidades presupuestales. En respuesta, la guía mantiene y refuerza la estructura escalonada por niveles de presupuesto (básico, intermedio y avanzado) presente en las tablas y matrices del objetivo.

Finalmente, el evaluador destacó positivamente la pertinencia y actualidad de la temática abordada, así como la articulación lograda entre los aspectos técnicos, normativos y éticos de la propuesta.

7. Referencias

AI Deepfakes: A Threat to Facial Biometric Authentication. (2025). BairesDev.

Alshehri, H. (2025). Developing multi-factor authentication and biometric verification protocols for enhancing data security in IoT healthcare devices. En 2025 17th International Conference on Computer and Automation Engineering (ICCAE 2025) (pp. 367-373). https://doi.org/10.1109/ICCAE64891.2025.10980555

AWS. (2025). Amazon Web Services documentation.

Bayometric. (2024). Biometric technology resources.

Bendiab, G., Haiouni, H., Moulas, I., & Shiaeles, S. (2025). Deepfakes in digital media forensics: Generation, AI-based detection and challenges. Journal of Information Security and Applications, 88, 103935. https://doi.org/10.1016/j.jisa.2024.103935

BioCatch. (2025). Behavioral biometrics.

BehavioSec. (2024). Behavioral biometric authentication.

Blanco Gonzalo, R., Corsetti, B., Goicoechea-Telleria, I., Husseis, A., Liu-Jimenez, J., Sanchez-Reillo, R., Eglitis, T., Ellavarason, E., Guest, R., Lunerti, C., Azimi, M., Khiarak, J., Ezennaya-Gomez, S., Whiskerd, N., Kuzu, R., & Okoh, E. (2018). Attacking a smartphone biometric fingerprint system: A novice's approach. En Proceedings - International Carnahan Conference on Security Technology (2018-October). https://doi.org/10.1109/CCST.2018.8585726

Bredin, H., Yin, R., Coria, J. M., Gelly, G., Korshunov, P., Lavechin, M., Fustes, D., Titeux, H., Bourmeau, W., & Gill, M.-P. (2020). Pyannote.audio: Neural building blocks for speaker diarization. En ICASSP 2020.

Czeschik, C. (2018). Black market value of patient data. En D. Linnhoff-Popien, R. Schneider, & M. Zaddach (Eds.), Digital Marketplaces Unleashed (pp. 883-893). Springer. https://doi.org/10.1007/978-3-662-49275-8_78

Daon. (2025). Identity verification and authentication solutions.

Dhingra-Kumar, N., Brusaferro, S., & Arnoldo, L. (2021). Patient safety in the world. En B. Donaldson, S. Sheridan, & P. Tartaglia (Eds.), Textbook of Patient Safety and Clinical Risk Management (pp. 93-98). Springer. https://doi.org/10.1007/978-3-030-59403-9_8

Envista Forensics. (2024). Digital forensics and biometric analysis.

Ethical considerations in the use of facial recognition for public safety. (2026). IEEE Public Safety Technology. https://publicsafety.ieee.org/topics/ethical-considerations-in-the-use-of-facial-recognition-for-public-safety/

Facia. (2024). Face liveness detection and recognition.

Gelb, A., & Krishnan, N. (2018). Biometrics for development: Benefits and risks. Center for Global Development.

Goicoechea-Telleria, I., Liu-Jimenez, J., Sanchez-Reillo, R., & Ponce-Hernandez, W. (2016). Vulnerabilities of biometric systems integrated in mobile devices: An evaluation. En Proceedings - International Carnahan Conference on Security Technology. https://doi.org/10.1109/CCST.2016.7815677

HyperVerge. (2024). AI-powered identity verification.

IEEE SA. (2021). IEEE 2410-2021 - Standard for biometric privacy. IEEE Standards Association. https://standards.ieee.org/ieee/2410/7746/

Incode Technologies. (2024). Identity verification platform.

Kavanagh, M. M., Baral, S. D., Milanga, M., & Sugarman, J. (2019). Biometrics and public health surveillance in criminalised and key populations: Policy, ethics, and human rights considerations. The Lancet HIV, 6(1), e51-e59. https://doi.org/10.1016/S2352-3018(18)30243-1

Keyless. (2023). Biometric authentication without passwords.

Keyless. (2024). Passwordless biometric security.

Kyriakou, K., Apostolaras, A., Velentzas, P., Syrigos, I., Maglavera, S., Evangelatos, S., Veroni, E., & Korakis, T. (2024). Biometrics data space:

Ensuring trustworthy and secure data exchange for suspect identification. En EEITE 2024 - Proceedings of 2024 5th International Conference in Electronic Engineering, Information Technology and Education. https://doi.org/10.1109/EEITE61750.2024.10654448

Labayen, M., Vea, R., Florez, J., Aginako, N., & Sierra, B. (2021). Online student authentication and proctoring system based on multimodal biometrics technology. IEEE Access, 9, 72398-72411. https://doi.org/10.1109/ACCESS.2021.3079375

Liebana-Cabanillas, F., Ghazanfar, A. A., Higueras-Castillo, E., & Wagner, R. (2025). Press to pay: The power of biometrics in financial transactions investigated by PLS-SEM, fsQCA, and NCA. Technological Forecasting and Social Change, 221(31), 124365. https://doi.org/10.1016/j.techfore.2025.124365

Maiti, D., Basak, M., & Das, D. (2025). A review on fingerprint based authentication: Its challenges and applications. Computer Science Review, 57, 100735. https://doi.org/10.1016/j.cosrev.2025.100735

Marcel, S., Fierrez, J., & Evans, N. (Eds.). (2023). Handbook of biometric anti-spoofing. Advances in Computer Vision and Pattern Recognition. Springer. https://doi.org/10.1007/978-981-19-5288-3

Microsoft Azure. (2025). Azure AI and biometric services.

Montgomery, C., & Wei, E. (2023). Patient identification. En Patient Safety: A Case-Based Innovative Playbook for Safer Care (2.a ed., pp. 75-87). Springer. https://doi.org/10.1007/978-3-031-35933-0_6

NEC Corporation. (2024). Biometric identification solutions.

NuData Security. (2024). Behavioral analytics and biometrics.

OpenAI. (2025). OpenAI platform documentation.

Page, M. J., Moher, D., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hrobjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., & McKenzie, J. E. (2021). PRISMA 2020 explanation and elaboration: Updated guidance and

exemplars for reporting systematic reviews. The BMJ, 372, n160. https://doi.org/10.1136/BMJ.N160

Parker, S., & Ray, A. (2022). Biometric systems in modern security frameworks.

PRISMA Statement. (2025). Preferred Reporting Items for Systematic Reviews and Meta-Analyses. https://www.prisma-statement.org/

Qamar, A., Karim, A., & Chang, V. (2019). Mobile malware attacks: Review, taxonomy & future directions. Future Generation Computer Systems, 97, 887-909. https://doi.org/10.1016/j.future.2019.03.007

Real Python. (2024). Python tutorials and resources.

Regula Forensics. (2025). Document and biometric verification.

A review of privacy-preserving biometric identification and authentication protocols. (2025). ScienceDirect. https://www.sciencedirect.com/science/article/abs/pii/S0167404824006151

ROC.ai. (2023). Biometric algorithm solutions.

Saraswat, D., Ladhiya, K., Bhattacharya, P., & Zuhair, M. (2022). PHBio: A Paillier homomorphic biometric encryption scheme in Healthcare 4.0 ecosystems. En Proceedings of 3rd International Conference on Intelligent Engineering and Management (ICIEM 2022) (pp. 306-312). https://doi.org/10.1109/ICIEM54221.2022.9853180

Security101. (2022). Physical security and access control.

Sun, Z., & Liu, Z. (2025). Ensuring privacy in face recognition: A survey on data generation, inference and storage. Discover Applied Sciences, 7(5), 441. https://doi.org/10.1007/s42452-025-06987-2

Sumsub. (2025). Identity verification platform.

Tanwar, S., Tyagi, S., Kumar, N., & Obaidat, M. S. (2019). Ethical, legal, and social implications of biometric technologies. En Biometric-Based Physical and Cybersecurity Systems (pp. 535-569). Springer. https://doi.org/10.1007/978-3-319-98734-7_21

Tertulino, R., Antunes, N., & Morais, H. (2023). Privacy in electronic health records: A systematic mapping study. Journal of Public Health, 32(3), 435-454. https://doi.org/10.1007/s10389-022-01795-z

TipsOI. (2024). Biometric identification resources.

TypingDNA. (2024). Typing biometrics for authentication.

Vandana, & Kaur, N. (2021). A study of biometric identification and verification system. En 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE 2021) (pp. 60-64). https://doi.org/10.1109/ICACITE51222.2021.9404735

Verazial. (2025). Biometric verification solutions.

Yang, Y. (2025). Racial bias in AI-generated images. AI & Society, 40(7), 5425-5437. https://doi.org/10.1007/s00146-025-02282-1