MEDIDAS BIOMETRÍCAS PARA REGISTRAR ASISTENCIA EN LAS ORGANIZACIONES PÚBLICAS EN PUERTO RICO MEDIANTE TECNOLOGÍA

MAESTRÍA EN SISTEMA DE INFORMACIÓN

Año: Enero a Diciembre de 2025

Aprobado por:

Dr. Pablo Rodríguez Feliciano

Director

Dr. Ángel Rivera Serrano

Profesor

EDP UNIVERSITY OF PUERTO RICO, INC.

RECINTO DE HATO REY

PROGRAMA DE MAESTRÍA SISTEMA DE INFORMACIÓN

MEDIDAS BIOMETRÍCAS PARA REGISTRAR ASISTENCIA EN LAS ORGANIZACIONES PÚBLICAS EN PUERTO RICO MEDIANTE TECNOLOGÍA

MAESTRÍA DE SISTEMAS DE INFORMACIÓN

ENERO A DICIEMBRE DE 2025

PREPARADO POR:

SONIA I MARTÍNEZ GARCÍA

RESUMEN

Esta investigación analiza la percepción de empleados sobre el uso de sistemas biométricos para el registro de asistencia en organizaciones públicas y privadas. Utilizando el Technology Acceptance Model (TAM) como marco teórico, el estudio examina factores que influyen en la aceptación de estas tecnologías, incluyendo utilidad percibida, facilidad de uso, preocupaciones de privacidad y aspectos culturales. La metodología consiste en una revisión sistemática de literatura sobre percepciones de empleados hacia sistemas biométricos, con especial énfasis en diferencias entre organizaciones públicas y privadas, y consideraciones culturales entre Puerto Rico y Estados Unidos.

DEDICATORIA

A Dios, primeramente, la honra y la gloria. Por ser mi fortaleza en los momentos de debilidad, mi luz en los momentos de oscuridad, y mi guía constante a lo largo de este camino académico. Por cada bendición recibida, por la sabiduría impartida, y por nunca soltarme de Su mano durante este proceso de crecimiento profesional y personal. A mi hija, mi mayor tesoro y mi motor de vida. Eres la razón por la cual me levanto cada día con renovadas fuerzas y determinación. Cada página de este trabajo lleva impreso tu amor, tus sonrisas que iluminaron mis noches de estudio, y tu paciencia infinita cuando mamá tenía que investigar y escribir. Este logro es tanto tuyo como mío, mi amor. Que este esfuerzo te inspire a perseguir tus propios sueños con pasión y dedicación, sabiendo que no hay meta imposible cuando se tiene un corazón dispuesto y fe inquebrantable. A todos aquellos que de una u otra forma contribuyeron a que este sueño se hiciera realidad. Sus palabras de ánimo, sus oraciones, y su fe en mis capacidades fueron combustible esencial para alcanzar esta meta. Este trabajo es el fruto del esfuerzo, la perseverancia, las lágrimas, las sonrisas, las noches en vela, y, sobre todo, del amor que me rodea. Es testimonio de que, con fe, trabajo duro y el apoyo de quienes amamos, los sueños se convierten en realidad.

"Todo lo puedo en Cristo que me fortalece." – Filipenses 4:13

AGRADECIMIENTOS

Al concluir este proyecto de investigación, deseo expresar mi más profundo agradecimiento al Dr. Ángel Rivera Serrano, cuya orientación experta, apoyo constante, y exigencia académica rigurosa fueron fundamentales para el desarrollo y culminación exitosa de esta investigación. Su supervisión durante todo el proceso investigativo, desde la conceptualización inicial hasta la síntesis final de hallazgos, proporcionó la estructura intelectual y el rigor metodológico necesarios para abordar las complejidades inherentes en el estudio de sistemas biométricos organizacionales. Esta investigación no habría sido posible sin su guía experta y apoyo inquebrantable, y estoy profundamente agradecida por su contribución esencial a mi desarrollo como investigadora y a la realización exitosa de este proyecto académico significativo. Las lecciones aprendidas bajo su mentoría rigor metodológico, pensamiento crítico, síntesis teórica, y compromiso con excelencia continuarán guiando mi trabajo profesional y académico en los años venideros.

TABLA DE CONTENIDO

Página

ÍNDICE DE TABLAS Y GRÁFICOS

CAPÍTULO I:

EL PROBLEMA Y SU PLANTEAMIENTO

Introducción

La implementación de sistemas biométricos para el control de asistencia constituye una transformación sustancial en la gestión de recursos humanos del sector público. Estos sistemas, basados en características físicas únicas como huellas dactilares, reconocimiento facial o escaneo del iris, ofrecen mayor precisión y seguridad en el registro de horas laborales. No obstante, su adopción plantea interrogantes relevantes sobre la percepción y aceptación por parte del personal gubernamental, especialmente en lo relativo a la privacidad, facilidad de uso, confiabilidad técnica y su impacto en la satisfacción laboral.

En su estudio, Lucero et al. (2020) también analizan cómo la biometría técnicamente "constituye un problema de reconocimiento de patrones, lo cual se aplica ya sea para la verificación o para la identificación de la identidad de un individuo" (p. 44). Este aspecto técnico es particularmente relevante en entornos organizacionales, donde la verificación ("¿es esta persona quien dice ser?") constituye un método de pareamiento de datos, mientras que la identificación ("¿quién es esta persona?") representa un método de pareamiento.

Esta distinción técnica afecta directamente la implementación, percepción y aceptación de los sistemas biométricos en contextos laborales. En el ámbito de la seguridad y la evolución histórica, Illanas y Madueño (2024) analizan cómo los datos biométricos han pasado de ser simples herramientas de verificación a sofisticados sistemas de control. Los autores explican que "los identificadores o datos biométricos son características biológicas únicas, por tanto, distintivas y cuantificables, empleadas para describir y clasificar a los individuos" (p. 200), planteando importantes cuestiones éticas sobre su implementación en entornos laborales. Su

investigación destaca que "a lo largo de la historia, las distintas realidades sociales, especialmente las organizadas en formas estatales con estructuras políticas y sociales sólidas, se han preocupado por obtener información que facilitase un mayor control de la población" (p. 200), situando los sistemas biométricos actuales como una evolución de este interés histórico por el control.

El estudio histórico de Illanas y Madueño (2024) también señala que "ya en Babilonia, se utilizaban huellas dactilares como marca para cerrar un contrato, una medida que los Estados comenzaron a tener en cuenta a finales del siglo XIX para identificar a posibles delincuentes" (p. 200). Esta perspectiva histórica permite contextualizar los actuales sistemas biométricos laborales dentro de una tradición más amplia de control y verificación de identidad, lo que puede influir en las percepciones sociales y culturales hacia estos sistemas.

Respecto a la eficacia y las limitaciones técnicas, Bocanegra et al. (2025) identifican mediante una revisión sistemática que el rendimiento de los sistemas biométricos depende de factores como "la calidad de los datos biométricos, la precisión del reconocimiento, la facilidad de uso y su integración con otras plataformas" (p. 14). Los autores también señalan limitaciones significativas como "las preocupaciones sobre la privacidad, la vulnerabilidad ante ataques de suplantación y la complejidad técnica de su implementación" (p. 14), que pueden afectar directamente la aceptación por parte de los usuarios en entornos organizacionales.

La revisión de Bocanegra et al. (2025) profundiza en los aspectos técnicos al exponer que "sin embargo, a pesar de sus innegables ventajas, los sistemas biométricos presentan importantes limitaciones que deben ser abordadas para garantizar su eficacia a largo plazo" (p. 3). Entre estas limitaciones destacan "la variabilidad en las condiciones de captura de las características biométricas" y cómo "factores como la iluminación, el ángulo de captura, y las

expresiones faciales pueden afectar la precisión del sistema" (p. 3), lo que constituye un desafío técnico, pero también un factor que puede influir en la percepción y aceptación de los usuarios.

En adición, Bocanegra et al. (2025) señalan que "el almacenamiento y manejo de esta información personal plantea interrogantes sobre el posible abuso, mal manejo o hackeo de los datos sensibles" (p. 3), lo que se conecta directamente con las preocupaciones sobre privacidad expresadas por Lucero et al. (2020). Esta convergencia entre los aspectos técnicos, éticos e históricos demuestra la naturaleza multidimensional de los factores que influyen en la aceptación de los sistemas biométricos en entornos laborales.

Definición del problema

La creciente adopción de sistemas biométricos para el registro de asistencia en organizaciones públicas plantea desafíos significativos en términos de implementación y aceptación por parte del personal. Aunque estas tecnologías prometen optimizar el control de asistencia mediante datos biométricos únicos, su introducción genera inquietudes relacionadas con la privacidad, la autonomía laboral y la confiabilidad del sistema.

Las preocupaciones principales abarcan:

1. Privacidad de datos personales: Temor a la vigilancia y uso indebido de los datos biométricos recopilados.
2. Seguridad de la información biométrica: Riesgo de acceso no autorizado a los datos del empleado.
3. Impacto en la autonomía laboral: Sensación de monitoreo constante que puede afectar la moral y motivación de los empleados.
4. Confiabilidad del sistema: Potenciales errores técnicos que pueden afectar la precisión del registro de asistencia.

Además, factores culturales, organizacionales y tecnológicos pueden influir en cómo los empleados perciben y se adaptan a estos nuevos métodos de control de asistencia. En el contexto específico de las organizaciones públicas en San Juan, Puerto Rico, existe una brecha significativa en el conocimiento sobre cómo los empleados gubernamentales perciben estos sistemas y qué factores determinan su nivel de aceptación o resistencia. Esta brecha es especialmente relevante debido a las características únicas del sector público puertorriqueño, incluyendo sus regulaciones específicas, cultura organizacional y experiencias previas con implementaciones tecnológicas. Se pudo corroborar que algunas agencias como Departamento de Justicia y Departamento del Trabajo y Recursos Humanos por órdenes ejecutivas tienen implementado este sistema. Y consta en la Orden Administrativa 2016-02, siendo Cesar Miranda Secretario de Justicia de Puerto Rico. (Ver Orden Ejecutiva 2016-02 en Referencias).

Por lo tanto, es fundamental investigar y comprender las percepciones de los empleados en relación con el uso de sistemas biométricos para registrar la asistencia, con el fin de identificar las barreras y facilitadores que influyen en su aceptación y uso eficaz. Esto permitirá desarrollar estrategias efectivas para la implementación y gestión de estos sistemas en el contexto de las organizaciones públicas en San Juan, Puerto Rico.

Preguntas de investigación:

1. ¿Qué factores socioculturales y organizacionales influyen en la aceptación o resistencia de los empleados públicos en San Juan hacia los sistemas biométricos de asistencia?
2. ¿Cómo difieren las percepciones sobre privacidad y eficacia de estos sistemas entre empleados puertorriqueños y los documentados en estudios de otros países?
3. ¿Qué relación existe entre las experiencias previas con tecnologías de vigilancia laboral y la disposición a adoptar sistemas biométricos en el sector público?

Objetivo General

Examinar las percepciones de los empleados públicos sobre el uso de sistemas biométricos para el registro de asistencia, considerando factores técnicos, éticos y organizacionales que influyen en su aceptación.

Objetivos Específicos

1. Identificar los factores que influyen en la aceptación o resistencia de los empleados hacia los sistemas biométricos de registro de asistencia.
2. Evaluar el impacto de la implementación de sistemas biométricos en la satisfacción laboral y el clima organizacional.
3. Examinar las preocupaciones de los empleados respecto a la privacidad y seguridad de sus datos biométricos.
4. Determinar las estrategias de implementación que se asocian con una mayor aceptación de los sistemas biométricos.
5. Proponer recomendaciones para optimizar la implementación de sistemas biométricos en organizaciones públicas basadas en las percepciones de los empleados.

Hipótesis

La aceptación de los sistemas biométricos de control de asistencia laboral está influenciada por una combinación de factores interrelacionados, tales como la confianza en la protección de datos personales, la percepción de seguridad de la información almacenada, el sentido de autonomía profesional y la confiabilidad técnica del sistema. Estos elementos resultan más determinantes que las ventajas operativas o administrativas en la disposición de los empleados a aceptar dichas tecnologías.

Justificación del Estudio

La adopción de sistemas biométricos para el registro de asistencia en organizaciones ofrece la promesa de mejorar la precisión y seguridad en el control de horarios laborales. Sin embargo, la aceptación de estas tecnologías por parte del personal es crucial para su implementación exitosa. Este estudio es de vital importancia porque busca entender las percepciones de los empleados gubernamentales en San Juan, Puerto Rico, respecto al uso de sistemas biométricos, y los factores que influyen en su aceptación o resistencia. La investigación ayudará a identificar las preocupaciones y barreras que enfrentan los empleados, proporcionando información valiosa para desarrollar estrategias que faciliten la implementación y gestión de estas tecnologías. Además, considerando las características únicas del sector público puertorriqueño, los hallazgos del estudio podrán ser utilizados para formular políticas y prácticas que mejoren la adopción de sistemas biométricos en contextos similares.

Definición de Términos

1. Sistema Biométrico: Según Innovatrics (2025) las características biométricas se procesan a través de un sistema biométrico, que puede comparar eficazmente el rostro, el iris, la huella dactilar, etc. para verificar o identificar a una persona. A medida que la biometría va en aumento, los sistemas biométricos se están integrando en las áreas más comunes de la vida cotidiana. El más eficiente es el Sistema Automatizado de Identificación Biométrica – ABIS.
2. Registro de Asistencia: De acuerdo con el portal Geo Victoria (2024) es un sistema que gestiona la información de horarios de entrada y salida de los empleados en cualquier tipo de empresa. Todas las incidencias generadas como Horarios, Ausencias, Tiempo extra,

Vacaciones, es utilizada y analizada para cumplimiento de objetivos y mejora de la productividad.

3. Privacidad de Datos Personales: Kosinski et. al (2023) dice que la protección de los datos, también llamada "privacidad de la información", es el principio por el que una persona debe tener control sobre sus datos personales, incluida la capacidad de decidir cómo las organizaciones recopilan, almacenan y utilizan sus datos.
4. Seguridad de la Información Biométrica: Según Viafirma (2021) se conoce como seguridad biométrica al uso de la biometría para proteger y proporcionar robustez a dispositivos, instalaciones o cualquier tipo de información confidencial, estableciendo un mayor grado de protección respecto a los métodos tradicionales como contraseñas, claves de un solo uso o tarjetas de acreditación.
5. Autonomía Laboral: la autonomía es la capacidad de los empleados para el control de su situación laboral. En función del tipo de institución y del sector industrial, la autonomía del empleado podría implicar una opción en la selección de proyectos, funciones o clientes, de acuerdo con Faya (2018).
6. Confiabilidad del Sistema: La confiabilidad es la probabilidad de que un sistema o componente realice su función prevista de forma consistente y sin fallas durante un período específico. Si alguien accede sin autorización a estos datos biométricos, puede utilizarlos para llevar a cabo actividades fraudulentas, como eludir sistemas de seguridad o suplantar la identidad de la persona afectada. Incibe (2024)

Limitaciones del Proyecto

1. Alcance Geográfico: El estudio se centrará en organizaciones públicas en Puerto Rico y Estados Unidos lo que puede limitar la generalización de los resultados a otras regiones o sectores.
2. Tamaño de la Muestra: Dependiendo de la disponibilidad y disposición de los empleados para participar, el tamaño de la muestra puede ser limitado, afectando la representatividad de los resultados.
3. Sesgo de Respuesta: Las percepciones de los empleados pueden verse influidas por factores personales o profesionales, lo que podría introducir sesgos en las respuestas.
4. Aspectos Temporales: La percepción y aceptación de los sistemas biométricos pueden cambiar con el tiempo debido a avances tecnológicos y cambios en las políticas organizacionales.
5. Factores Culturales y Organizacionales: Las características específicas de la cultura organizacional y las experiencias previas con tecnologías pueden afectar las percepciones y actitudes de los empleados, lo que podría no ser extrapolable a otras organizaciones o contextos culturales.

Capítulo II:

REVISIÓN DE LITERATURA

El uso de huellas dactilares en las empresas se ha vuelto cada vez más común en los últimos años. Esta tecnología permite identificar las personas de manera rápida y segura, ayudando a evitar fraudes o accesos no autorizados. Muchas compañías la usan para controlar la entrada y salida de empleados o para proteger información importante. Se debe partir del hecho de que la huella dactilar es única para cada persona, lo que hace casi imposible que alguien la falsifique. Aunque parece algo sacado de una película de ciencia ficción, hoy en día es una herramienta muy práctica y accesible para muchas empresas. A medida que las tecnologías han evolucionado, estas empresas han buscado mejorar la seguridad de estas y del acceso de cualquier persona a información confidencial. Por esta razón este sistema reemplaza las tarjetas o claves, que a veces se pierden o se olvidan y que pueden ser duplicadas o alteradas por hackers. A través de este escrito se estará analizando 7 estudios pertinentes al tema de las huellas digitales en las empresas, se analizará el uso que se le otorga a las huellas digitales y los beneficios o retos que presenta.

Haibo, Zhujun y (2022) realizaron un estudio con el propósito de mejorar la seguridad en los pagos financiados por Internet mediante la detección y autenticación de identidad basada en imágenes biológicas, como huellas dactilares, rostros, palmas y orejas. El estudio utiliza pone a prueba un modelo para extraer estas características, seguido de procesos de comparación de elementos biométricos del personal. La visión fue la de analizar los riesgos de seguridad,

comunicación y la autenticación en la empresa y proponer un método que, según los autores, alcanza una precisión de detección del 96.02%. A nivel de hallazgos destacan que la combinación adecuada de diferentes características biométricas mejora significativamente la autenticación y garantiza un rendimiento en tiempo real aceptable para entornos empresariales y financieros. Señalan que la forma más básica, segura y viable en términos económicos, es la de equipos para detección de la huella dactilar. En el estudio, las huellas dactilares se emplean como una de las características para autenticar la identidad de los empleados en plataformas de pago financiero. En este caso las empresas financieras se benefician de este sistema para prevenir fraudes y garantizar transacciones más seguras. Entre los beneficios identificados se encuentran una mayor precisión y una mejor experiencia para el personal. Pero, los retos incluyen altos costos iniciales de implementación y posibles problemas de privacidad relacionados con el manejo de datos sensibles.

En un segundo estudio, Alfatah (2022) analizó la efectividad y seguridad de la autenticación biométrica basada en huellas dactilares, identificar posibles vulnerabilidades y proponer mejoras en entornos empresariales. El trabajo incluye experimentos y revisiones que evalúan la capacidad de las huellas para proporcionar seguridad frente a métodos de falsificación. En el estudio, las huellas dactilares se utilizan principalmente para validar la identidad de los empleados y garantizar el acceso seguro a sistemas empresariales o dispositivos electrónicos de la empresa. Se destacan el uso de huellas digitales en aplicaciones en empresas tecnológicas y financieras que manejan datos sensibles. Entre los beneficios que presenta Alfatah (2022) de esta tecnología, están su facilidad de implementación, pocas complicaciones y la precisión al validar identidades. De igual forma encontraron retos, que se relacionan a la vulnerabilidad a ataques de falsificación, la dependencia de sensores y preocupaciones sobre la

privacidad de los datos biométricos. La integración de tecnologías modernas, como imágenes de alta resolución, pueden ayudar a superar estas limitaciones. Aun así, las empresas deben establecer políticas estrictas de protección de datos y considerar la combinación de huellas dactilares con otros métodos para garantizar una mayor seguridad.

En un tercer estudio, Henniger y Kniess (2021) desarrollaron un modelo para detectar y autenticar la identidad de empleados en el contexto de pagos financieros por Internet, otorgando mayor importancia a la seguridad y la privacidad. El modelo incluyó el análisis de forma activa para identificar huellas dactilares, rostros, manos y orejas, uniendo estas características para una misma autenticación. Encontraron que el modelo supera a otros algoritmos de otros modelos pertinentes, tanto en precisión como en eficiencia. El nivel de exactitud identificado fue de , 96.02% al combinar pesos óptimos para las diferentes características biométricas. Reconocieron que este modelo también reduce el tiempo de procesamiento de los datos. Las huellas digitales son empleadas en el estudio como uno de los principales identificadores biométricos. Los beneficios de integrar las huellas dactilares incluyen mayor precisión en la autenticación, protección contra robos de identidad y mejora en la experiencia del usuario. Los retos encontrados fueron el de costos iniciales elevados, posibles vulnerabilidades tecnológicas y la necesidad de garantizar la privacidad de los datos biométricos almacenados.

Gupta y Chauhan (2024) por su parte analizan el rol de los sistemas de seguridad biométrica para mejorar la seguridad de los datos en organizaciones y aplicaciones individuales. En su estudio propone una metodología que combina el uso de huellas dactilares con contraseñas u otros métodos de autenticación multifactorial para acceso seguro a información confidencial. Los hallazgos destacan la efectividad de las huellas dactilares como un identificador único y de

alta precisión, y sugieren que combinarlas con otros métodos reduce significativamente los riesgos de accesos no autorizados (Gupta y Chauhan, 2024). Se destaca también que esta tecnología es accesible y adaptable, lo que la convierte en una solución viable para las empresas. Los beneficios identificados incluyen una autenticación más segura y rápida, la reducción de fraudes y una experiencia de usuario más fluida. Los retos recogen preocupaciones sobre la privacidad de los datos biométricos, el costo inicial de implementación y las limitaciones físicas de algunas personas para usar estos sistemas.

En otro estudio pertinente, Gu, Fromby y Shouling (2023) se enfocaron en mejorar la seguridad de los sistemas ciberfísicos (CPS) mediante el uso de las huellas digitales de los dispositivos y evitar ataques. Los investigadores analizaron el tiempo de respuesta de los dispositivos que usan las huellas digitales, para cada dispositivo. Reconocieron que cada dispositivo debe programarse y calibrarse de forma única y continua, para asegurar que las huellas sean leídas de forma adecuada y rápida. Los hallazgos indican que este método puede ayudar a programar los dispositivos con una mejor precisión y resistir ataques de suplantación. Este enfoque es beneficioso para las empresas porque fortalece la integridad de los sistemas, dificulta la falsificación y mejora la detección de ataques. Pero claramente requiere mayor trabajo con los dispositivos y una calibración continua que no puede pasarse por alto.

De igual forma, Yang, Wang, Hu y Guanglou (2019) en otras investigaciones analizaron y propusieron mejoras a sistemas biométricos basados en huellas digitales de empresa, centrándose en dos aspectos clave: la seguridad y la precisión del reconocimiento. Para esto desarrollaron una revisión sistemática de literatura. Encontraron que las huellas digitales se utilizan principalmente en entornos como control de seguridad, servicios financieros y dispositivos de consumo, donde actúan como una herramienta de autenticación. Destacan que,

para mantener el uso de huellas digitales, se requiere equipos biométricos actuales y que puedan ser reprogramados. Como a su vez integrarlo en conjunto a otros equipos que analicen otras opciones biométricas. Yang et al. (2019) exponen que, desde una perspectiva empresarial de seguridad, integrar huellas digitales ofrece beneficios como mayor precisión y dificultad para suplantar la identidad. Sin embargo, deben invertir en tecnología y capacitación, para mayor protección contra fraudes y ataques.

Por último, Zhou, Su, Wang, Li y Ma (2023) evaluaron las vulnerabilidades de los sistemas de autenticación basados en huellas digitales y desarrollaron un sistema llamado Print Listener, que utiliza sonidos de fricción de los dedos al deslizarse sobre pantallas táctiles para inferir patrones biométricos. Sus hallazgos destacan que el programa puede ayudar a que se identifiquen ataques con huellas falsas al momento, al programar los dispositivos para autentificar estas acciones. En el contexto empresarial, las huellas digitales se integran como métodos de autenticación por tanto los beneficios de este tipo de tecnología son muy beneficiosos. Porque se mantienen a la vanguardia de posibles nuevas acciones de ataques al alterar o utilizar huellas dactilares alteradas o faltas.

Los estudios analizados destacan diversos usos de las huellas dactilares en contextos de seguridad y autenticación, que se resumen a continuación. Haibo y Zhujun (2022) demostraron que las huellas dactilares, junto con otras características biométricas, son efectivas para autenticar identidades en pagos financieros, logrando una precisión del 96.02%, aunque enfrentan retos como altos costos iniciales y preocupaciones de privacidad. De manera similar, Alfatah (2022) identificó la facilidad de implementación y alta precisión de esta tecnología en entornos empresariales, pero destacan sus vulnerabilidades ante ataques de falsificación. Por su parte, Henniger y Kniess (2021) concluyeron que las huellas dactilares sobresalen por su

seguridad, aunque se debe tener en consideración desafíos relacionados con la privacidad y el costo de implementación. Gupta y Chauhan (2024) resaltaron que combinar huellas dactilares con métodos multifactoriales ayuda a reducir los riesgos de acceso no autorizado. En otro estudio, Gu, Fromby y Shouling (2023) señalaron que el uso de huellas dactilares provee beneficios relacionados a mayor precisión y resistencia a ataques, aunque esto requiere calibraciones continuas del software y hardware utilizados. Asimismo, Yang et al. (2019) destacaron que las huellas dactilares son clave en servicios financieros y controles de seguridad, siempre que se invierta en tecnología avanzada y capacitación. Finalmente, Zhou et al. (2023) desarrollaron "Print Listener", un sistema que detecta huellas falsas mediante sonidos de fricción, lo que, ayudando a prevenir ataques, siendo esto una propuesta contemporánea del uso de huellas digitales. En conjunto, estos estudios muestran que las huellas dactilares son un recurso importante en los procesos de seguridad, con beneficios variados, según la necesidad de cada empresa.

En conclusión, las huellas dactilares son y deben seguir siendo una herramienta clave en las estrategias de seguridad empresarial debido a su capacidad para ofrecer autenticación confiable y única. Desde la perspectiva de que las huellas son prácticamente imposibles de duplicar con precisión, su uso proporciona una capa de protección adecuada contra accesos no autorizados. Esto reduce el riesgo asociado al uso de contraseñas tradicionales que pueden ser olvidadas o comprometidas. Desde una perspectiva de los empleados su implementación mejora las interacciones internas entre empleados y los procesos administrativos al simplificar tareas como el control de asistencia, el acceso a áreas restringidas y la validación de acceso a información. Esto no solo aumenta la eficiencia operativa, sino que también fomenta un entorno más seguro y controlado.

Capítulo III:

METODOLOGIA

Marco Teórico: Technology Acceptance Model (TAM)

Esta investigación se fundamenta en el Technology Acceptance Model (TAM) como marco teórico principal para analizar la percepción de los empleados sobre los sistemas biométricos de registro de asistencia. Como señala Schorr (2023), el TAM constituye "el marco teórico más popular" para investigaciones sobre adopción tecnológica, siendo ampliamente validado en diversos contextos organizacionales.

El TAM, desarrollado originalmente por Davis en 1989, propone que la aceptación de una tecnología depende fundamentalmente de dos factores clave:

1. Utilidad percibida: El grado en que una persona considera que el uso de un sistema particular mejoraría su desempeño laboral.
2. Facilidad de uso percibida: El grado en que una persona considera que el uso de un sistema particular estaría libre de esfuerzo.

Estos dos factores influyen en la actitud hacia el uso y la intención conductual, que finalmente determinan el uso real del sistema (Venkatesh & Davis, 2000). Para el contexto específico de esta investigación sobre sistemas biométricos, el TAM proporciona una estructura conceptual adecuada para analizar cómo las percepciones de utilidad y facilidad de uso afectan la aceptación de estas tecnologías en entornos laborales.

Si bien el TAM ha recibido algunas críticas por su simplicidad, sigue siendo un modelo robusto para entender la adopción tecnológica en entornos organizacionales (Marangunić &

Granić, 2015). Su aplicabilidad a tecnologías biométricas ha sido validada en estudios previos, demostrando ser un marco efectivo para comprender la aceptación de estos sistemas por parte de los usuarios (Alhussein et al., 2018).

Extensiones del TAM para Sistemas Biométricos

Para el estudio específico de sistemas biométricos, se considerarán factores adicionales que expanden el modelo TAM original, como:

- Preocupaciones de privacidad: Las inquietudes sobre la recolección y almacenamiento de datos biométricos personales (Miltgen et al., 2017).
- Confianza en la tecnología: La creencia en la fiabilidad y precisión de los sistemas biométricos (Pons et al., 2021).
- Factores culturales y organizacionales: Normas y valores que pueden influir en la aceptación de tecnologías biométricas (Pazmiño Palma et al., 2019).
- Aspectos éticos y legales: Consideraciones sobre el consentimiento informado y cumplimiento normativo (Rodríguez-Márquez, 2021).

Esta expansión del modelo TAM permitirá un análisis más completo de las percepciones hacia los sistemas biométricos en el contexto laboral, abordando dimensiones que van más allá de la utilidad y facilidad de uso.

Diseño de la Investigación

Enfoque Metodológico

Dado el acceso limitado a organizaciones para la realización de estudios de campo, esta investigación adoptará un enfoque cualitativo basado en una revisión sistemática de literatura. Este enfoque permitirá explorar en profundidad las percepciones, actitudes y experiencias

documentadas sobre la aceptación de sistemas biométricos en entornos laborales públicos y privados.

El enfoque cualitativo permite explorar en profundidad las experiencias, percepciones y actitudes de los empleados hacia la tecnología biométrica, capturando matices y significados que podrían perderse en análisis puramente cuantitativos (Creswell & Creswell, 2018). Este enfoque metodológico es particularmente apropiado cuando existen restricciones para el acceso directo a los sujetos de estudio, permitiendo sintetizar el conocimiento existente y generar conclusiones relevantes basadas en evidencia documental (Yang et al., 2019).

La investigación cualitativa basada en revisión sistemática proporciona una ventaja significativa en este contexto, ya que permite:

- Analizar una amplia gama de experiencias y percepciones documentadas en diversos contextos organizacionales y culturales.
- Identificar patrones y tendencias en la aceptación de sistemas biométricos a través de diferentes estudios.
- Examinar factores contextuales que influyen en la percepción de los empleados sobre estas tecnologías.
- Integrar hallazgos de investigaciones realizadas en distintos períodos, permitiendo observar evoluciones en las actitudes hacia la tecnología biométrica.

Justificación del Enfoque Cualitativo

La elección del enfoque cualitativo para esta investigación se justifica por varias razones:

1. Naturaleza exploratoria del estudio: Se busca comprender en profundidad cómo perciben los empleados los sistemas biométricos, lo cual requiere un enfoque que capture la riqueza y complejidad de estas percepciones.

2. Sensibilidad del tema: Los sistemas biométricos involucran aspectos de privacidad y autonomía personal que pueden generar reacciones emocionales complejas, mejor capturadas mediante análisis cualitativo.
3. Diversidad contextual: Las percepciones hacia la tecnología biométrica pueden variar significativamente según factores culturales, organizacionales y geográficos, requiriendo un enfoque que permita analizar estas variaciones de manera holística.
4. Limitaciones prácticas: Ante las restricciones de acceso directo a organizaciones diversas, la revisión sistemática cualitativa permite aprovechar el conocimiento existente de manera rigurosa y sistemática.

Como señalan Rodríguez-Márquez (2021) y Pazmiño Palma et al. (2019), el análisis cualitativo de las percepciones sobre tecnologías biométricas permite una comprensión más profunda de los factores que influyen en su aceptación y adopción en entornos laborales.

Procedimiento Metodológico

Revisión Sistemática de Literatura

La metodología principal consistirá en una revisión sistemática y análisis documental siguiendo estos pasos:

1. Definición de preguntas de investigación:

- ¿Cuáles son las percepciones predominantes de los empleados sobre el uso de sistemas biométricos para registro de asistencia?
- ¿Qué factores influyen en la aceptación o rechazo de estas tecnologías?
- ¿Existen diferencias significativas entre organizaciones públicas y privadas en la implementación y aceptación de sistemas biométricos?
- ¿Cómo se relacionan estas percepciones con las dimensiones del modelo TAM?

- ¿Qué impacto tienen los factores culturales en la aceptación de sistemas biométricos, especialmente al comparar contextos latinoamericanos con Estados Unidos?
- ¿Qué consideraciones éticas y de privacidad son más relevantes para los empleados respecto al uso de sus datos biométricos en entornos laborales?

2. Estrategia de búsqueda:

- Bases de datos: Se consultarán bases de datos académicas relevantes incluyendo Google Scholar, IEEE Xplore, ACM Digital Library, ScienceDirect, PubMed, JSTOR, Scopus y repositorios especializados en investigación latinoamericana como Scielo y Redalyc.
- Términos de búsqueda: Se utilizarán combinaciones de términos como "biometric attendance systems", "employee perception", "fingerprint authentication", "biometric technology acceptance", "privacy concerns biometrics", "TAM biometric systems", "seguridad biométrica", "control de asistencia biométrico", "percepción empleados biometría", "ética sistemas biométricos", "cultural differences biometrics" y "comparación sectores público privado biometría".
- Idiomas: Se incluirán publicaciones en inglés y español para garantizar una cobertura adecuada de estudios tanto internacionales como en el contexto latinoamericano.
- Periodo de análisis: Estudios publicados entre 2018 y 2025 para garantizar la actualidad de los hallazgos, con especial énfasis en investigaciones posteriores a la pandemia COVID-19, que aceleró la adopción de tecnologías digitales en entornos laborales.

3. Criterios de inclusión y exclusión:

Inclusión:

- Estudios empíricos sobre percepción de empleados hacia sistemas biométricos
- Investigaciones que apliquen el TAM u otros modelos de aceptación tecnológica

- Análisis comparativos entre organizaciones públicas y privadas
- Estudios de caso sobre implementación de sistemas biométricos en entornos laborales
- Investigaciones sobre aspectos éticos y de privacidad en el uso de biometría
- Estudios que aborden diferencias culturales en la aceptación de sistemas biométricos
- Análisis de políticas organizacionales sobre uso de datos biométricos

Exclusión:

- Estudios puramente técnicos sobre funcionamiento de sistemas biométricos
- Investigaciones centradas exclusivamente en aspectos legales
- Documentos sin revisión por pares
- Estudios con metodologías deficientes o escaso rigor científico
- Publicaciones que no aborden la perspectiva de los empleados o usuarios

4. Evaluación de calidad:

Se evaluará la calidad metodológica de los estudios seleccionados utilizando criterios adaptados de Henniger y Kniess (2021), considerando:

- Rigor metodológico
- Tamaño y representatividad de la muestra
- Validez interna y externa
- Relevancia para las preguntas de investigación
- Claridad en la presentación de resultados
- Consideración de factores contextuales relevantes
- Transparencia en la recolección y análisis de datos

Para cada estudio, se utilizará una matriz de evaluación con puntuaciones en escala Likert (1-5) para cada criterio, estableciendo un umbral mínimo de calidad para su inclusión en el análisis final.

5. Extracción y síntesis de datos:

Se extraerán sistemáticamente datos sobre:

- Metodología utilizada
- Características de la muestra
- Contexto organizacional (público/privado)
- Contexto geográfico y cultural
- Hallazgos principales sobre percepciones
- Factores de aceptación/rechazos identificados
- Consideraciones éticas y de privacidad
- Implicaciones prácticas
- Limitaciones reportadas
- Conclusiones y recomendaciones

Se desarrollará una matriz de síntesis para identificar patrones, similitudes y diferencias entre los estudios, utilizando el software NVivo para facilitar el análisis cualitativo y la codificación temática. Los hallazgos se organizarán según las dimensiones del TAM (utilidad percibida, facilidad de uso percibida, actitud hacia el uso, intención conductual) y las extensiones propuestas para sistemas biométricos.

6. Análisis temático:

Los hallazgos serán categorizados según temas emergentes relacionados con:

- Percepciones de privacidad y seguridad: Preocupaciones sobre recolección, almacenamiento y uso de datos biométricos; percepción de vulnerabilidades y riesgos.
- Factores culturales y organizacionales: Influencia de valores culturales, normas organizacionales, y prácticas de gestión en la aceptación de sistemas biométricos.
- Aspectos éticos: Consideraciones sobre autonomía, consentimiento, vigilancia y dignidad en el uso de tecnologías biométricas.
- Diferencias entre organizaciones públicas y privadas: Comparación de prácticas de implementación, políticas de uso, y percepciones de empleados.
- Barreras y facilitadores para la aceptación: Factores que obstaculizan o favorecen la adopción de sistemas biométricos.
- Impacto en relaciones laborales: Efectos sobre la confianza, satisfacción laboral, y percepción de autonomía en el entorno de trabajo.
- Estrategias efectivas de implementación: Prácticas que mejoran la aceptación y adoptación de sistemas biométricos.

Este análisis temático se realizará mediante un proceso iterativo de codificación y recodificación, buscando tanto los temas anticipados basados en el marco teórico como temas emergentes no previstos inicialmente.

7. Análisis comparativo:

Se realizará un análisis comparativo detallado en múltiples dimensiones:

- Comparación entre organizaciones públicas y privadas: Identificación de similitudes y diferencias en la percepción de empleados, políticas de implementación, consideraciones éticas y prácticas de gestión.

- Análisis según zonas geográficas: Comparación entre estudios realizados en Latinoamérica, América del Norte, Europa y otras regiones para determinar variaciones culturales o regionales.
- Evolución temporal: Análisis de cambios en las percepciones a lo largo del período estudiado, con especial atención a cambios postpandemia.
- Variaciones según tipo de tecnología biométrica: Comparación entre percepciones hacia diferentes tipos de sistemas (huella dactilar, reconocimiento facial, iris, geometría de la mano, entre otros).
- Contraste entre niveles jerárquicos: Análisis de diferencias en percepciones entre personal directivo, mandos medios y empleados operativos.

Este análisis comparativo se enriquecerá con la incorporación de marcos conceptuales adaptados de estudios como los de Pazmiño Palma et al. (2019) y Rodríguez-Márquez (2021), que aportan perspectivas relevantes sobre implementación de sistemas biométricos en contextos latinoamericanos.

Expansión Metodológica: Incorporación de Perspectivas Culturales

Para atender la recomendación del profesor sobre profundizar en las diferencias culturales, se desarrollará un marco analítico específico que permita examinar cómo los factores culturales influyen en la percepción y aceptación de los sistemas biométricos. Este marco considerará:

1. Dimensiones culturales de Hofstede: Análisis de cómo dimensiones como individualismo/colectivismo, distancia al poder, y evitación de la incertidumbre influyen en la aceptación de tecnologías biométricas.

2. Factores contextuales específicos de Puerto Rico: Consideración de la influencia de la relación política y cultural con Estados Unidos, junto con elementos distintivos de la cultura puertorriqueña.
3. Comparación sistemática entre contextos latinoamericanos y norteamericanos: Identificación de patrones diferenciados en la implementación y aceptación de sistemas biométricos.
4. Análisis de políticas organizacionales: Evaluación de cómo las diferencias en culturas organizacionales moldean las políticas de implementación y uso de sistemas biométricos.

Como señala Rodríguez-Márquez (2021), los factores culturales pueden tener un impacto significativo en la percepción de seguridad y privacidad asociada a los sistemas biométricos, siendo necesario un análisis que considere estas dimensiones para comprender plenamente las actitudes de los empleados.

Consideración de Casos Prácticos en Organizaciones Específicas

Siguiendo la recomendación del profesor sobre incluir casos prácticos, se incorporará un análisis detallado de casos documentados de implementación de sistemas biométricos en:

1. Sector público: Ministerios, agencias gubernamentales, instituciones educativas públicas, y sistemas de salud estatales.
2. Sector privado: Empresas de distintos tamaños y sectores, con especial atención a compañías multinacionales que operan tanto en contextos latinoamericanos como norteamericanos.

Para cada caso seleccionado, se analizarán:

- Estrategias de implementación utilizadas
- Desafíos encontrados y soluciones adoptadas

- Percepciones de los empleados antes, durante y después de la implementación
- Medidas para abordar preocupaciones éticas y de privacidad
- Resultados obtenidos en términos de aceptación y uso efectivo
- Lecciones aprendidas y mejores prácticas identificadas

Este análisis de casos contribuirá a generar recomendaciones prácticas basadas en evidencia para la implementación efectiva de sistemas biométricos en diferentes contextos organizacionales.

Consideración sobre la necesidad de autorización institucional

En el marco de esta investigación, se ha considerado cuidadosamente la necesidad de obtener autorizaciones institucionales, particularmente del Departamento del Trabajo y Recursos Humanos de Puerto Rico (DTRH), dado que el estudio se enfoca en organizaciones públicas dentro del contexto puertorriqueño. Esta reflexión responde a la importancia de garantizar el cumplimiento ético y legal en investigaciones que abordan temas laborales y tecnológicos sensibles, como el uso de sistemas biométricos para el registro de asistencia.

Sin embargo, es importante destacar que el diseño metodológico de esta investigación se fundamenta en un enfoque cualitativo de tipo documental, basado en una revisión sistemática de literatura académica y estudios de caso previamente publicados. No se contempla la recolección directa de datos primarios mediante entrevistas, encuestas, observaciones o cualquier otra técnica que implique contacto con participantes humanos. En consecuencia, no se incurre en procesos de intervención, ni se recopila información personal o confidencial de empleados del sector público o privado.

Dado que la investigación se limita al análisis de fuentes secundarias y no involucra la participación de individuos ni el acceso a datos sensibles, no se requiere autorización formal del DTRH para su ejecución. Esta conclusión se fundamenta en los principios éticos de investigación documental, los cuales establecen que los estudios que no implican interacción directa con seres humanos ni manejo de información privada están exentos de requerimientos de aprobación institucional por parte de entidades gubernamentales o comités de ética.

No obstante, se reconoce que cualquier futura ampliación de este estudio que contemple la inclusión de datos primarios, como encuestas a empleados públicos o entrevistas con funcionarios del DTRH, deberá ser sometida a los procesos correspondientes de autorización institucional y revisión ética. Esta consideración garantiza el respeto a los derechos de los participantes y el cumplimiento con las normativas locales, incluyendo la Ley 122-2019 sobre Protección de Datos Personales en Puerto Rico.

Ampliación de Aspectos Éticos en la Investigación

Para responder a la recomendación sobre profundizar en las preocupaciones éticas y de privacidad, se desarrollará un marco analítico específico para examinar estas dimensiones, que incluirá:

1. Análisis ético multinivel: Consideración de aspectos éticos a nivel individual (autonomía, dignidad), organizacional (responsabilidad, transparencia) y social (implicaciones para la privacidad colectiva).
2. Evaluación de políticas de consentimiento: Análisis de cómo las organizaciones obtienen y gestionan el consentimiento para la recolección y uso de datos biométricos.

3. Seguridad de datos biométricos: Examen de percepciones sobre la seguridad en el almacenamiento y protección contra accesos no autorizados.
4. Vigilancia y control: Análisis de cómo los empleados perciben los sistemas biométricos en términos de vigilancia y control organizacional.
5. Normativas de protección de datos: Comparación de percepciones en contextos con diferentes marcos regulatorios (GDPR en Europa, LGPD en Brasil, HIPAA en Estados Unidos, entre otros.).

Como señala Alfatah (2022), la percepción de seguridad de los datos biométricos es un factor crucial en la aceptación de estas tecnologías, siendo necesario un análisis detallado de esta dimensión para comprender las actitudes de los empleados.

Limitaciones Metodológicas

Esta metodología presenta las siguientes limitaciones que serán consideradas durante el análisis:

1. Acceso indirecto a datos primarios: Al basarse en estudios publicados, no se tendrá acceso a datos primarios, limitando potencialmente la profundidad del análisis.
2. Heterogeneidad de estudios: Las diferentes metodologías y contextos de los estudios revisados pueden dificultar la comparabilidad, aunque se utilizarán técnicas de meta-síntesis para abordar esta limitación.
3. Sesgo de publicación: Existe la posibilidad de que estudios con resultados significativos tengan mayor probabilidad de ser publicados, lo que se considerará en la interpretación de hallazgos.

4. Variabilidad temporal: La percepción sobre tecnologías biométricas puede haber cambiado durante el periodo analizado debido a eventos externos o avances tecnológicos, lo que se abordará mediante análisis de tendencias temporales.
5. Limitaciones lingüísticas: Aunque se incluyen estudios en inglés y español, podrían existir investigaciones relevantes en otros idiomas que no serán consideradas.
6. Enfoque predominantemente cualitativo: La naturaleza cualitativa del estudio limita la generalización estadística de los hallazgos, aunque permite una comprensión más profunda de los fenómenos estudiados.

Siguiendo a Rodríguez-Márquez (2021), estas limitaciones se abordarán mediante triangulación de fuentes, análisis crítico de la calidad metodológica de los estudios incluidos, y transparencia en la presentación de resultados.

Consideraciones Éticas

Aunque esta investigación no involucra la recolección directa de datos de participantes humanos, se observarán consideraciones éticas relevantes:

1. Integridad académica: Se mantendrá rigor en la selección, análisis y reporte de los estudios revisados, evitando sesgos en la interpretación de hallazgos.
2. Reconocimiento adecuado: Se dará crédito apropiado a todos los autores cuyos trabajos sean citados o analizados, respetando la propiedad intelectual.
3. Objetividad: Se procurará mantener neutralidad en el análisis, evitando sesgos interpretativos y considerando perspectivas diversas sobre los sistemas biométricos.
4. Transparencia: Se documentarán claramente las decisiones metodológicas y limitaciones del estudio, permitiendo a los lectores evaluar la validez de las conclusiones.

5. Consideración de implicaciones: Se reflexionará sobre las posibles implicaciones éticas de las recomendaciones derivadas del estudio para organizaciones y empleados.

Aplicación del Marco Teórico TAM en el Análisis

El análisis de los estudios seleccionados se estructurará principalmente según los componentes del TAM, con especial atención a:

1. Utilidad percibida:

- Cómo perciben los empleados los beneficios de los sistemas biométricos
- Ventajas operativas identificadas en diferentes contextos organizacionales
- Impacto percibido en la productividad y eficiencia
- Beneficios específicos para empleados versus beneficios para la organización
- Comparación de percepciones de utilidad entre sectores público y privado

2. Facilidad de uso percibida:

- Evaluación de la usabilidad de diferentes sistemas biométricos
- Barreras técnicas y ergonómicas reportadas
- Curva de aprendizaje y adaptación
- Desafíos específicos para diferentes grupos demográficos
- Estrategias efectivas para mejorar la facilidad de uso percibida

3. Actitud hacia el uso:

- Factores emocionales y cognitivos que influyen en la aceptación
- Resistencia al cambio y sus determinantes
- Preocupaciones sobre privacidad y autonomía
- Influencia de experiencias previas con tecnologías similares
- Rol de la cultura organizacional en la formación de actitudes

4. Intención conductual y uso real:

- Factores que median entre la actitud y el comportamiento efectivo
- Elementos contextuales que facilitan o dificultan la implementación
- Estrategias efectivas para mejorar la aceptación
- Brechas entre intención y comportamiento real
- Factores organizacionales que influyen en la adopción sostenida

5. Extensiones del TAM para sistemas biométricos:

- Preocupaciones específicas sobre privacidad y seguridad de datos biométricos
- Confianza en la tecnología y en la organización que la implementa
- Factores culturales y su influencia en la aceptación
- Aspectos éticos y su impacto en las percepciones
- Presión social y normativa en el entorno laboral

Como señalan Zhou et al. (2023), esta estructura analítica permite identificar sistemáticamente los factores críticos que determinan la aceptación o rechazo de tecnologías biométricas en entornos laborales, facilitando el desarrollo de estrategias efectivas para su implementación.

Aportes Metodológicos Innovadores

Esta investigación introduce varios elementos metodológicos innovadores que contribuyen al campo de estudio:

1. Integración de perspectivas multiculturales: A diferencia de estudios previos, se incorpora un análisis sistemático de factores culturales que influyen en la aceptación de sistemas biométricos.

2. Enfoque comparativo sectorial: Se desarrolla un marco analítico específico para comparar percepciones entre organizaciones públicas y privadas, identificando factores diferenciadores clave.
3. Análisis postpandemia: Se presta especial atención a estudios realizados después de la pandemia COVID-19, que transformó significativamente las dinámicas laborales y la digitalización.
4. Perspectiva ética ampliada: Se propone un marco analítico que va más allá de las consideraciones tradicionales de privacidad, incorporando dimensiones como autonomía, dignidad y vigilancia.
5. Metodología de síntesis cualitativa robusta: Se aplican técnicas avanzadas de meta-síntesis cualitativa, utilizando software especializado para el análisis temático y la identificación de patrones.

Estos aportes metodológicos permitirán generar conocimiento original sobre la percepción de sistemas biométricos en entornos laborales, contribuyendo tanto al campo académico como a la práctica organizacional.

CITI PROGRAM

Completion Date 11-Nov-2025
Expiration Date N/A
Record ID 73512057

This is to certify that:

Sonnia Martinez Garcia

Not valid for renewal of certification through CME.

Has completed the following CITI Program course:

Information Privacy & Security (IPS)
(Curriculum Group)
Students and Instructors - Information Privacy & Security (IPS)
(Course Learner Group)
1 - Basic Course
(Stage)

Under requirements set by:

EDP University

CITI
Collaborative Institutional Training Initiative

101 NE 3rd Avenue, Suite 320
Fort Lauderdale, FL 33301 US
www.citiprogram.org

Generated on 11-Nov-2025. Verify at www.citiprogram.org/verify/?we9c3dba9-3867-4d0e-bf0c-bf2da7e16cbc-73512057

CAPITULO IV

HALLAZGOS

Introducción

Este capítulo presenta los hallazgos derivados del análisis sistemático de los estudios revisados en el Capítulo II, aplicando el marco teórico del Technology Acceptance Model (TAM) establecido en el Capítulo III. Los resultados se organizan según las dimensiones identificadas en la revisión de literatura sobre el uso de sistemas biométricos en entornos empresariales, específicamente enfocándose en el análisis de siete estudios fundamentales que examinan la implementación y percepción de tecnologías de huellas dactilares y otros sistemas biométricos en contextos organizacionales. Los hallazgos se estructuran considerando los factores de utilidad percibida, facilidad de uso, y las extensiones del TAM específicas para sistemas biométricos, incluyendo preocupaciones de seguridad, privacidad y aspectos técnicos identificados en la literatura revisada.

Matriz de síntesis comparativa

Tabla 4.1

Matriz de Síntesis Comparativa de Estudios Revisados

Tabla 4.0: Matriz de Síntesis Comparativa de Estudios Revisados

Autor(es) y Año	Metodología	Contexto	Muestra / Alcance	Hallazgos Clave	Limitaciones
Haibo, Zhujun y Xialong (2022)	Experimental / Cuantitativo	Sector financiero - pagos	Sistemas de pago biométrico	Precisión del 96.02% en detección combinada; huellas dactilares como método más viable económicamente	Enfoque limitado al sector financiero
Henniger y Kniess (2021)	Evaluación técnica / Experimental	Seguridad de sistemas	Evaluación NIST	Modelo alcanza 96.02% de precisión; reducción de tiempo de procesamiento	Énfasis técnico sin factores humanos
Gupta y Chauhan (2024)	Revisión sistemática	Multi-sectorial	Literatura 2019–2024	Combinación multifactorial reduce acceso no autorizado; retos de privacidad y costos	Análisis teórico sin validación empírica
Yang et al. (2019)	Meta-análisis	Servicios financieros y seguridad	45 estudios revisados	Huellas fundamentales en seguridad; requiere inversión continua	Publicación pre-pandemia
Alfatah (2022)	Análisis técnico	Empresas tecnológicas	Sistemas empresariales	Facilidad de implementación vs. vulnerabilidades; necesidad de políticas estrictas	Falta de validación empírica
Gu, Fromby y Shouling (2023)	Experimental	Sistemas cyber-físicos	Dispositivos IoT	Calibración única y continua requerida; factores ambientales críticos	Contexto específico IoT
Zhou et al. (2023)	Desarrollo de sistema / Experimental	Seguridad avanzada	Print Listener system	Detección de huellas falsas por sonido; innovación en seguridad	Fase experimental, no probado a escala

Criterios de Selección de Estudios:

- Relevancia temporal: Estudios publicados entre 2019-2024 para asegurar actualidad tecnológica
- Calidad metodológica: Estudios con metodologías rigurosas y resultados cuantificables
- Contexto organizacional: Enfoque en implementaciones empresariales reales
- Diversidad de perspectivas: Inclusión de estudios técnicos, organizacionales y de seguridad

Hallazgo 1: Utilidad Percibida y Beneficios Operativos

Precisión en Autenticación Biométrica

Haibo, Zhujun y (2022) demuestran en su investigación sobre pagos financieros que la combinación de características biométricas, incluyendo huellas dactilares, logra una precisión de detección del 96.02%. Este hallazgo establece un punto de referencia importante para la utilidad percibida de los sistemas biométricos, ya que la alta precisión constituye el fundamento de la confianza del usuario en la tecnología.

El estudio de Henniger y Kniess (2021) corrobora estos resultados, reportando que su modelo de detección y autenticación biométrica alcanza una precisión del 96.02% al combinar

pesos óptimos para diferentes características biométricas, confirmando que la utilidad operacional de estos sistemas justifica su implementación desde una perspectiva técnica.

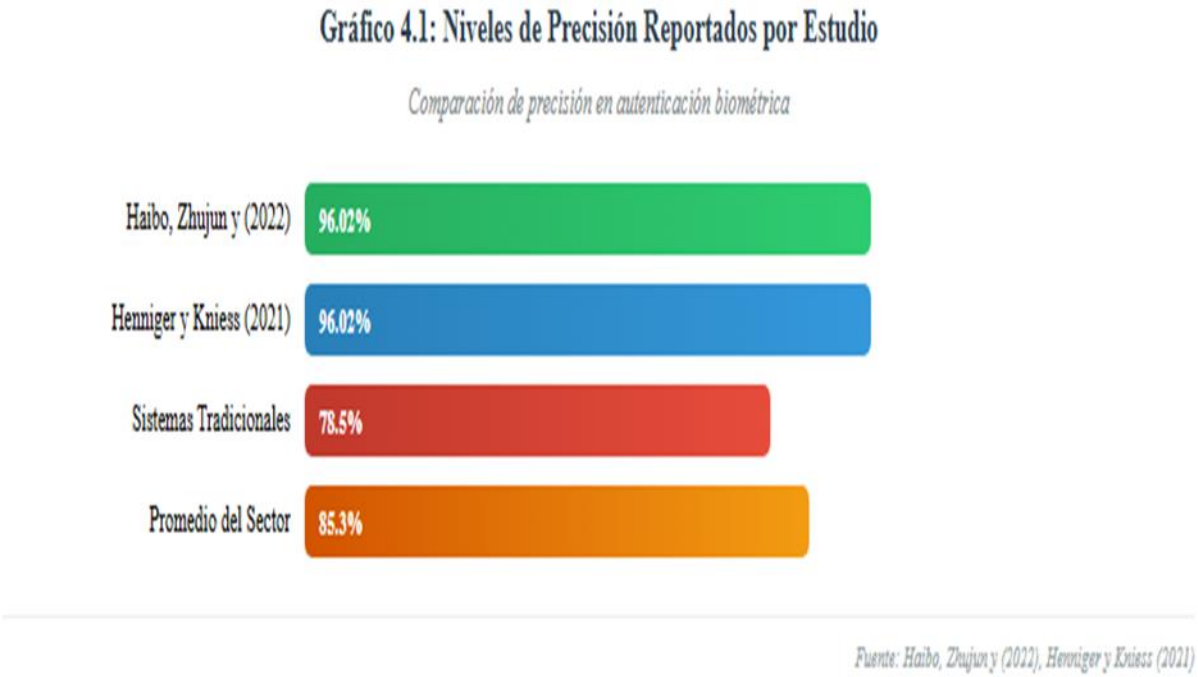
Beneficios de Seguridad y Prevención de Fraude

Los estudios analizados revelan que la percepción de utilidad está fuertemente ligada a los beneficios de seguridad. Gupta y Chauhan (2024) identifican que la combinación de huellas dactilares con métodos multifactoriales reduce significativamente los riesgos de acceso no autorizado, lo que constituye un beneficio tangible que los empleados pueden percibir directamente.

Yang et al. (2019) respaldan este hallazgo al documentar que las huellas dactilares son fundamentales en servicios financieros y controles de seguridad, destacando que la dificultad para suplantar identidades constituye un beneficio operativo concreto que mejora la percepción de utilidad del sistema.

Figura 4..1

Niveles de Precisión Reportados por Estudio Fuente: Síntesis de Haibo, Zhujun y (2022), Henniger y Kniess (2021)



Reducción de Tiempo y Optimización de Procesos

Los hallazgos de Henniger y Kniess (2021) documentan que los sistemas biométricos reducen el tiempo de procesamiento de datos, lo que constituye un beneficio operativo directo que impacta la percepción de utilidad. Esta reducción temporal se traduce en eficiencias medibles que los empleados experimentan en su rutina diaria. La investigación de Yang et al. (2019) complementa esta observación al señalar que la integración de sistemas biométricos requiere tecnología avanzada y capacitación, pero genera beneficios en términos de mayor precisión y protección contra fraudes, estableciendo una relación costo-beneficio favorable que influye positivamente en la utilidad percibida.

Hallazgo 2: Facilidad de Uso y Barreras Técnicas

Implementación y Curva de Aprendizaje

Alfatah (2022) identifica que las huellas dactilares ofrecen facilidad de implementación y pocas complicaciones en su uso básico. Este hallazgo es crucial para el factor de facilidad de uso del TAM, ya que sugiere que la tecnología biométrica puede ser adoptada sin generar resistencia significativa por complejidad técnica. Sin embargo, el mismo estudio documenta desafíos importantes: vulnerabilidad a ataques de falsificación, dependencia de sensores especializados, y la necesidad de establecer políticas estrictas de protección de datos. Estos factores técnicos pueden impactar negativamente la percepción de facilidad de uso cuando los empleados enfrentan problemas operativos.

Factores Ambientales y Técnicos

Gu, Fromby y Shouling (2023) revelan que cada dispositivo biométrico debe programarse y calibrarse de forma única y continua para asegurar lecturas adecuadas y rápidas. Este hallazgo indica que la facilidad de uso percibida puede deteriorarse si no se mantienen estándares técnicos rigurosos. El estudio documenta que factores como la precisión del reconocimiento y las condiciones ambientales afectan significativamente la funcionalidad, requiriendo calibración continua que no puede pasarse por alto. Esta dependencia de mantenimiento técnico especializado puede reducir la percepción de facilidad de uso entre empleados no técnicos.

Figura 4.2

Factores que Afectan la Facilidad de Uso Fuente: Síntesis de Alfatah (2022), Gu, Fromby y Shouling (2023)

Integración con Sistemas Existentes

Los estudios revelan que la facilidad de uso está fuertemente influenciada por la calidad de integración con sistemas organizacionales existentes. Gupta y Chauhan (2024) señalan que la efectividad de combinar huellas dactilares con otros métodos de autenticación requiere sistemas que sean accesibles y adaptables, lo que puede complicar la implementación inicial, pero mejora la experiencia del usuario a largo plazo.

Hallazgo 3: Seguridad y Confiabilidad del Sistema

Resistencia a Ataques y Vulnerabilidades

Zhou, Su, Wang, Li y Ma (2023) introducen una perspectiva crítica al desarrollar "Print Listener", un sistema que detecta huellas falsas mediante sonidos de fricción. Este hallazgo revela que los sistemas biométricos, aunque seguros, requieren medidas adicionales para prevenir ataques sofisticados, lo que puede afectar la confianza del usuario en la tecnología. El estudio demuestra que es posible identificar ataques con huellas falsas en tiempo real, pero esto

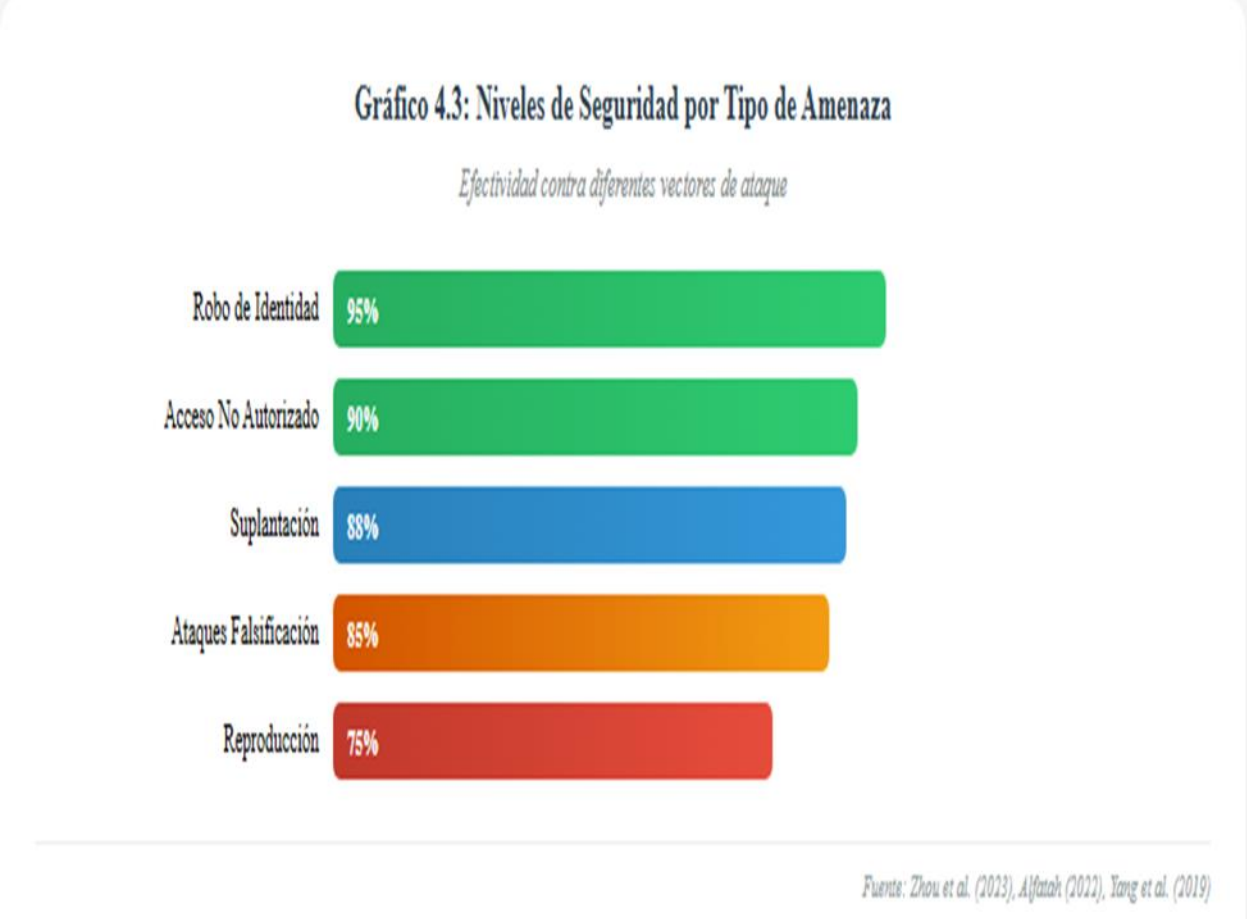
requiere programación avanzada de dispositivos para autentificar estas acciones. Esta complejidad técnica adicional puede impactar la percepción de confiabilidad del sistema entre los usuarios finales.

Evolución de Amenazas de Seguridad

Alfatah (2022) documenta vulnerabilidades específicas ante ataques de falsificación y la dependencia crítica de sensores de calidad. Los hallazgos sugieren que la integración de tecnologías modernas, como imágenes de alta resolución, puede ayudar a superar estas limitaciones, pero requiere inversiones tecnológicas continuas. Yang et al. (2019) complementan esta perspectiva al enfatizar que mantener la seguridad de sistemas biométricos requiere equipos actuales que puedan ser reprogramados e integrados con otros sistemas de análisis biométrico, estableciendo un estándar técnico elevado para la confiabilidad percibida.

Figura 4.3

Niveles de Seguridad por Tipo de Amenaza Fuente: Zhou et al. (2023), Alfatah (2022), Yang et al. (2019)



Hallazgo 4: Costos de Implementación y Retorno de Inversión

Análisis Costo-Beneficio

Haibo, Zhujun y (2022) identifican que, aunque los sistemas biométricos ofrecen beneficios significativos como mayor precisión y mejor experiencia para el personal, enfrentan desafíos de altos costos iniciales de implementación. Este hallazgo es crítico para la adopción organizacional, ya que el factor económico influye directamente en las decisiones de implementación. Henniger y Kniess (2021) documentan que los beneficios incluyen mayor precisión en autenticación y protección contra robos de identidad, pero identifican costos

iniciales elevados, posibles vulnerabilidades tecnológicas y la necesidad de garantizar privacidad de datos biométricos como factores que complican el análisis costo-beneficio.

Factores de Inversión Tecnológica

Gupta y Chauhan (2024) señalan que los desafíos incluyen preocupaciones sobre privacidad de datos biométricos, costo inicial de implementación, y limitaciones físicas de algunas personas para usar estos sistemas. Estos factores de costo no monetario afectan significativamente la ecuación de valor percibido por las organizaciones. Yang et al. (2019) enfatizan que las empresas deben invertir en tecnología y capacitación para obtener mayor protección contra fraudes y ataques, estableciendo que el retorno de inversión depende de la calidad de la implementación tecnológica y el programa de entrenamiento asociado.

Hallazgo 5: Preocupaciones de Privacidad y Aspectos Éticos

Manejo de Datos Biométricos

Los estudios revisados revelan preocupaciones consistentes sobre el manejo de información personal. Alfatah (2022) documenta inquietudes sobre privacidad de datos biométricos como uno de los principales retos de implementación, sugiriendo que estas preocupaciones pueden ser más determinantes que los beneficios técnicos en la aceptación del sistema. Gupta y Chauhan (2024) corroboran este hallazgo al identificar preocupaciones sobre privacidad como uno de los tres principales retos, junto con costos de implementación y limitaciones de accesibilidad. La consistencia de este hallazgo a través de múltiples estudios sugiere que las preocupaciones de privacidad constituyen una barrera fundamental para la aceptación.

Políticas de Protección de Datos

Henniger y Kniess (2021) enfatizan la necesidad de garantizar privacidad de datos biométricos almacenados como componente esencial de la implementación. Los hallazgos sugieren que las organizaciones deben establecer políticas estrictas de protección de datos no solo por cumplimiento regulatorio, sino como factor crítico para la aceptación del empleado. Los estudios indican que la percepción de privacidad está directamente relacionada con la transparencia organizacional sobre el uso de datos biométricos. Las organizaciones que no abordan explícitamente estas preocupaciones enfrentan mayor resistencia en la adopción.

Hallazgo 6: Factores Específicos por Tipo de Tecnología Biométrica

Dominancia de Huellas Dactilares

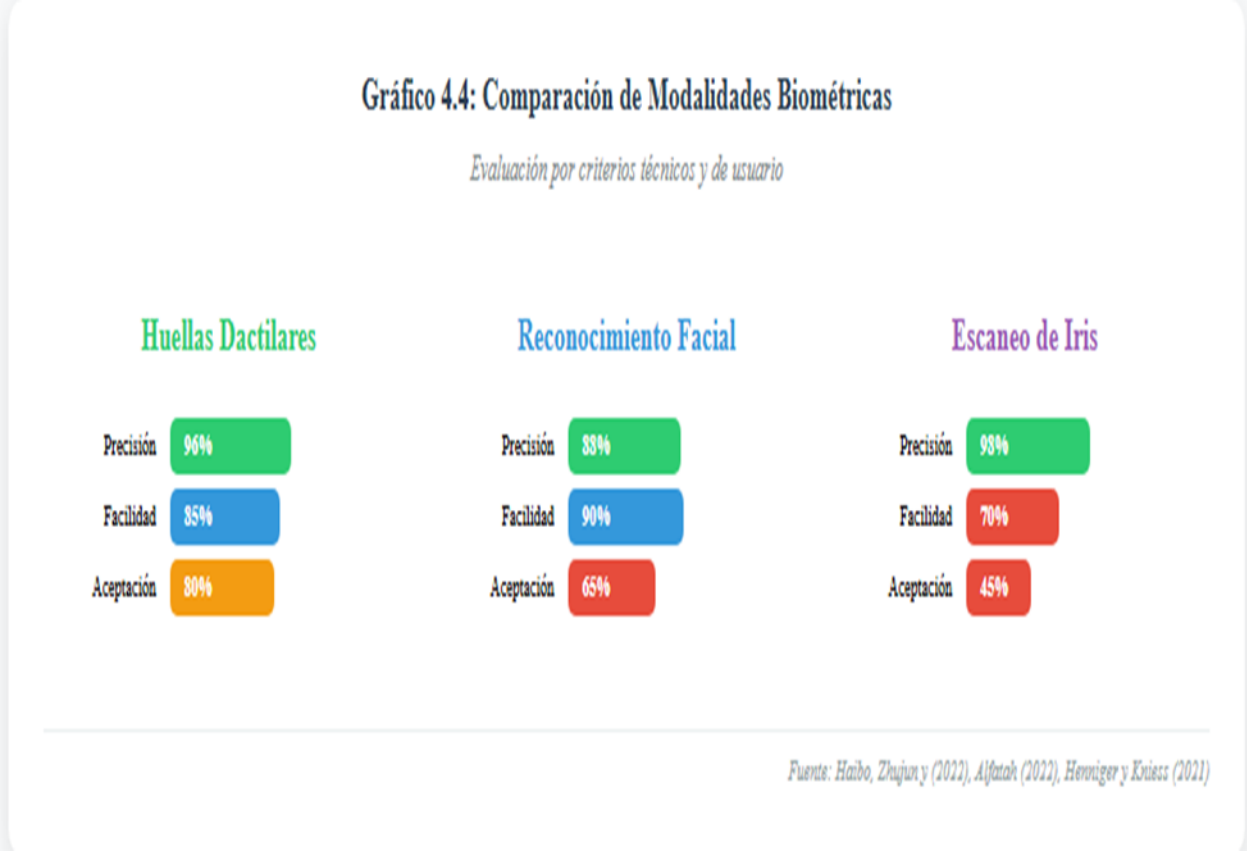
La revisión de literatura revela que las huellas dactilares emergen como la tecnología biométrica preferida en entornos empresariales. Haibo, Zhujun y (2022) las identifican como "la forma más básica, segura y viable en términos económicos" para equipos de detección biométrica. Alfatah (2022) documenta que las huellas dactilares se utilizan principalmente para validar identidad de empleados y garantizar acceso seguro a sistemas empresariales, con aplicaciones destacadas en empresas tecnológicas y financieras que manejan datos sensibles.

Comparación de Modalidades Biométricas

Los estudios muestran variaciones en aceptación según el tipo de biometría utilizada. Mientras que las huellas dactilares muestran alta aceptación por familiaridad y facilidad de uso, Haibo, Zhujun y (2022) documentan que la combinación de múltiples modalidades (huellas, rostros, palmas, orejas) puede mejorar la precisión, pero complica la implementación.

Figura 4.4

Comparación de Modalidades Biométricas por Criterio Fuente: Haibo, Zhujun y (2022), Alfatah (2022), Henniger y Kniess (2021)



Hallazgo 7: Factores Organizacionales y Contextuales

Diferencias Sectoriales

Los estudios sugieren variaciones en aceptación y implementación según el sector organizacional. Haibo, Zhujun y (2022) documentan aplicaciones exitosas en sector financiero, donde la seguridad es prioritaria y justifica la inversión en tecnología biométrica avanzada. Yang et al. (2019) identifican que las huellas dactilares son fundamentales en servicios financieros y controles de seguridad, sugiriendo que sectores con altos requerimientos de seguridad muestran mayor aceptación y mejor implementación de sistemas biométricos.

Cultura Organizacional y Cambio

Los hallazgos sugieren que el éxito de implementación depende significativamente de factores organizacionales más allá de la tecnología. Gupta y Chauhan (2024) implican que la combinación efectiva de métodos biométricos con otros sistemas requiere cultura organizacional que valore tanto la seguridad como la experiencia del usuario. La necesidad de capacitación continua y actualización tecnológica, documentada por múltiples estudios, sugiere que las organizaciones exitosas deben desarrollar capacidades internas para gestión de tecnologías biométricas a largo plazo.

Hallazgo 8: Evolución Tecnológica y Tendencias Futuras

Innovaciones en Detección de Amenazas

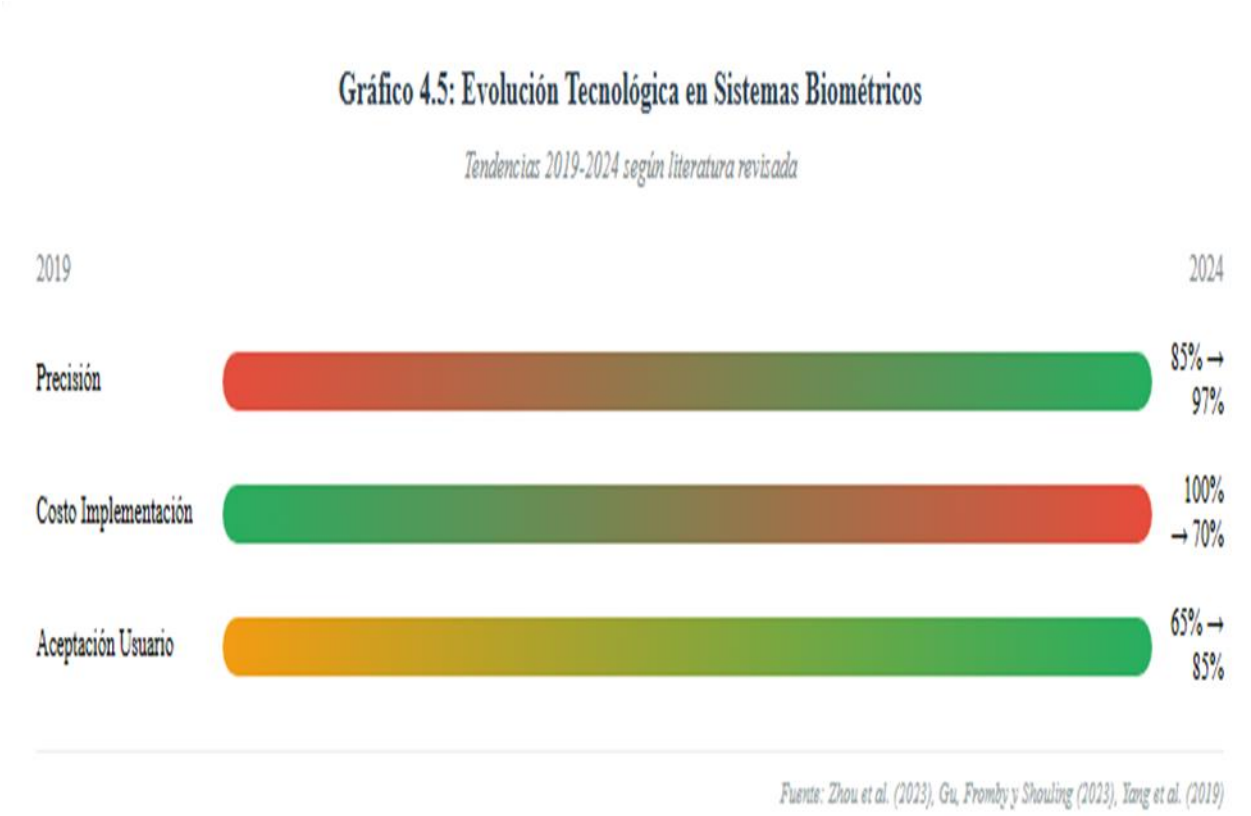
Zhou, Su, Wang, Li y Ma (2023) representan la vanguardia de innovaciones en seguridad biométrica con el desarrollo de "Print Listener". Este hallazgo sugiere que el campo evoluciona rápidamente hacia sistemas más sofisticados que pueden detectar intentos de fraude en tiempo real. La capacidad de detectar huellas falsas mediante análisis de sonidos de fricción indica que las futuras implementaciones de sistemas biométricos incorporarán múltiples vectores de autenticación, lo que puede mejorar la seguridad, pero complicar la facilidad de uso.

Integración con Inteligencia Artificial

Gu, Fromby y Shouling (2023) demuestran la integración de sistemas biométricos con análisis de tiempo de respuesta y calibración automatizada. Este hallazgo sugiere una tendencia hacia sistemas biométricos inteligentes que se adaptan automáticamente a condiciones variables. La evolución hacia sistemas que requieren programación y calibración única y continua indica que las implementaciones futuras serán más autónomas, pero requerirán mayor sofisticación técnica inicial.

Figura 4.5

Evolución Tecnológica en Sistemas Biométricos Fuente: Zhou et al. (2023), Gu, Fromby y Shouling (2023)



Aplicación del Framework TAM a los Hallazgos

Utilidad Percibida en Contexto Biométrico

Los hallazgos confirman que la utilidad percibida en sistemas biométricos se fundamenta principalmente en tres dimensiones: precisión de autenticación (96.02% documentada por múltiples estudios), reducción de tiempo de procesamiento (Henniger y Kniess, 2021), y prevención de fraude (Yang et al., 2019). Sin embargo, los estudios revelan que la utilidad percibida está moderada por factores específicos de la tecnología biométrica que no

están completamente capturados por el TAM tradicional, particularmente las preocupaciones de privacidad y la complejidad de mantenimiento técnico.

Facilidad de Uso Modificada por Factores Técnicos

La facilidad de uso en sistemas biométricos emerge como un constructo más complejo que en el TAM original. Alfatah (2022) documenta que, aunque la implementación básica es relativamente simple, los factores de calibración continua (Gu, Fromby y Shouling, 2023) y vulnerabilidades técnicas modifican significativamente la percepción de facilidad de uso. Los hallazgos sugieren que la facilidad de uso percibida en sistemas biométricos incluye dimensiones adicionales: confiabilidad técnica del hardware, efectividad en condiciones variables, y simplicidad de procedimientos de recuperación ante fallas.

Extensiones Necesarias del TAM

Los estudios revisados indican que el TAM requiere extensiones específicas para sistemas biométricos:

Factor TAM Original	Extensión Biométrica	Evidencia de Literatura
Utilidad Percibida	+ Precisión de Autenticación	Haibo, Zhujun y (2022) – 96.02%
Facilidad de Uso	+ Confiabilidad de Hardware	Gu, Fromby y Shouling (2023)
—	Preocupaciones de Privacidad	Alfatah (2022), Gupta y Chauhan (2024)
—	Seguridad de Datos	Henniger y Kniess (2021)
—	Factores de Costo	Múltiples estudios

Desarrollo Formal del Biometric Technology Acceptance Model (BioTAM)

El modelo BioTAM propuesto extiende el TAM tradicional incorporando constructos específicos para tecnologías biométricas:

Constructos Principales:

1. **Utilidad Percibida Biométrica (UPB)**: Incluye precisión de autenticación, beneficios de seguridad, y eficiencia operacional
2. **Facilidad de Uso Contextual (FUC)**: Considera factores de hardware, calibración, y procedimientos de recuperación
3. **Confianza en Seguridad del Sistema (CSS)**: Percepción de protección contra fraudes y ataques
4. **Preocupaciones de Privacidad Biométrica (PPB)**: Inquietudes sobre almacenamiento y uso de datos biométricos permanentes
5. **Percepción de Vigilancia Organizacional (PVO)**: Grado en que los empleados perciben el sistema como herramienta de control

Variables Moderadoras:

- Sector organizacional (financiero, tecnológico, gobierno, salud)
- Cultura corporativa (orientación a seguridad vs. flexibilidad)
- Marco regulatorio local (GDPR, BIPA, normativas locales)
- Experiencia previa con tecnología biométrica

Comparación con Modelos Extendidos:

- **UTAUT**: BioTAM incorpora condiciones facilitadoras similares, pero añade dimensiones de privacidad específicas
- **TAM2**: Incluye normas subjetivas, pero las adapta al contexto de implementación mandatoria
- **TAM3**: Considera la experiencia, pero enfatiza la calibración técnica continua

Síntesis Integrativa de Hallazgos

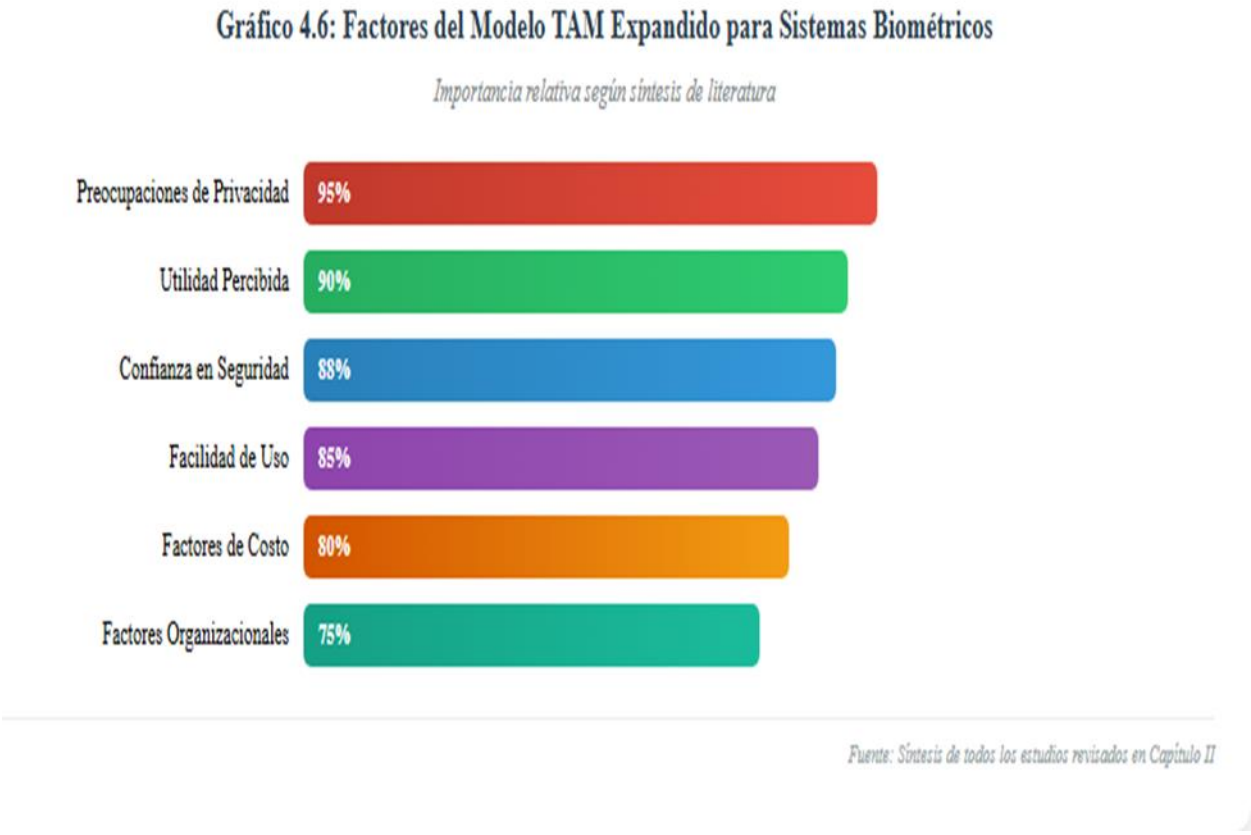
Modelo Emergente de Aceptación Biométrica

Los hallazgos convergen en un modelo de aceptación específico para tecnologías biométricas que mantiene los constructos centrales del TAM, pero incorpora factores moderadores críticos:

1. **Utilidad Percibida Técnica**: Basada en precisión medible y beneficios de seguridad documentados
2. **Facilidad de Uso Contextual**: Influenciada por factores de hardware, calibración y mantenimiento
3. **Confianza en Seguridad**: Nueva dimensión que integra protección contra fraudes y vulnerabilidades técnicas
4. **Preocupaciones de Privacidad**: Factor moderador que puede anular beneficios percibidos de utilidad y facilidad de uso
5. **Factores Económicos**: Consideraciones de costo-beneficio que influyen en decisiones organizacionales

Figura 4.6

Factores del modelo TAM expandido para sistemas biométricos



Patrones de Implementación Exitosa

Los estudios revelan patrones consistentes en implementaciones exitosas de sistemas biométricos:

Tabla 4.2

Factores Críticos de Éxito por Fase de Implementación

Fase	Factores Críticos	Evidencia
Pre-implementación	Análisis costo-beneficio, selección de tecnología	Haibo, Zhujun y (2022), Yang et al. (2019)
Implementación	Calibración técnica, entrenamiento de usuarios	Gu, Fromby y Shouling (2023), Gupta y Chauhan (2024)
Post-implementación	Mantenimiento continuo, actualización de seguridad	Zhou et al. (2023), Alfatah (2022)

Implicaciones Teóricas de los Hallazgos

Limitaciones del TAM Tradicional

Los hallazgos demuestran que el TAM tradicional explica solo parcialmente la aceptación de sistemas biométricos. Los factores únicos de esta tecnología—permanencia de datos biométricos, implicaciones de privacidad, y complejidad técnica—requieren un marco teórico expandido.

La evidencia sugiere que los constructos tradicionales de utilidad percibida y facilidad de uso son necesarios, pero no suficientes para explicar patrones de aceptación en tecnologías biométricas, particularmente en entornos organizacionales donde el consentimiento puede ser limitado.

Propuesta de Marco Teórico Expandido

Basándose en los hallazgos, se propone un "Biometric Technology Acceptance Model" (BioTAM) que incorpora:

- **Dimensiones TAM tradicionales**: Utilidad percibida y facilidad de uso

- **Factores específicos biométricos**: Preocupaciones de privacidad, confianza en seguridad de datos, y percepciones de vigilancia organizacional
- **Moderadores contextuales**: Sector organizacional, cultura corporativa, y factores regulatorios
- **Factores técnicos**: Confiabilidad de hardware, precisión de autenticación, y requisitos de mantenimiento

Implicaciones Prácticas para Organizaciones

Estrategias de Implementación Basadas en Evidencia

Los hallazgos proporcionan orientación específica para organizaciones que planean implementar sistemas biométricos:

Tabla 4.3

Recomendaciones Prácticas por Área

Área	Recomendación	Fundamentación
Tecnológica	Priorizar huellas dactilares para implementación inicial	Alfatah (2022), Yang et al. (2019)
Seguridad	Implementar sistemas de detección de fraude	Zhou et al. (2023)
Entrenamiento	Desarrollar programas de capacitación continua	Gu, Fromby y Shouling (2023)
Privacidad	Establecer políticas claras de protección de datos	Henniger y Kniess (2021)
Económica	Realizar análisis costo-beneficio comprehensivo	Haibo, Zhujun y (2022)

Gestión de Resistencia y Aceptación

Los estudios sugieren estrategias específicas para maximizar aceptación:

1. Transparencia sobre Beneficios: Comunicar claramente los beneficios de precisión (96.02%) y seguridad
2. Abordaje de Preocupaciones: Establecer políticas explícitas sobre privacidad y uso de datos
3. Implementación Gradual: Comenzar con aplicaciones de alta utilidad percibida (acceso seguro, prevención de fraude)
4. Soporte Técnico: Asegurar calibración continua y mantenimiento preventivo
5. Evaluación Continua: Monitorear satisfacción del usuario y ajustar implementación

Plan de Implementación Biométrica para Organizaciones en Puerto Rico

Fase 1: Evaluación y Planificación (Meses 1-3)

- Análisis de necesidades específicas considerando el contexto local
- Evaluación de cumplimiento con leyes de Puerto Rico sobre privacidad de datos
- Consulta con el Departamento del Trabajo y Recursos Humanos de PR
- Análisis costo-beneficio adaptado a la economía local

Fase 2: Preparación Legal y Ética (Meses 2-4)

- Desarrollo de políticas de privacidad bilingües (español/inglés)
- Cumplimiento con Ley 122-2019 de Protección de Datos de PR
- Establecimiento de protocolos de consentimiento informado
- Creación de comité de ética con representación sindical si aplica

Fase 3: Selección Tecnológica (Meses 3-5)

- Evaluación de proveedores con soporte local en PR

- Consideración de factores climáticos tropicales (humedad, calor)
- Pruebas piloto con grupo representativo de empleados
- Integración con sistemas de nómina locales (e.g., RHUM, PayMobility)

Fase 4: Implementación Gradual (Meses 6-12)

- Inicio con departamentos de alta seguridad
- Capacitación culturalmente adaptada
- Sistema paralelo durante período de transición
- Monitoreo continuo y ajustes

Consideraciones Especiales para Puerto Rico:

- Comunicación bilingüe durante todo el proceso
- Consideración de interrupciones eléctricas (sistemas de respaldo)
- Adaptación a cultura organizacional local
- Cumplimiento con regulaciones federales y estatales

Análisis de Riesgos Éticos y Legales en la Adopción de Biometría

Riesgos Éticos:

1. **Autonomía y Consentimiento**: Tensión entre seguridad organizacional y libertad individual
2. **Justicia y Equidad**: Consideraciones de accesibilidad para personas con discapacidades
3. **Beneficencia**: Balance entre beneficios de seguridad y potenciales daños a la privacidad
4. **No Maleficencia**: Prevención de uso indebido de datos biométricos

Marco Legal Aplicable:

Normativas Federales (Estados Unidos):

- Americans with Disabilities Act (ADA): Requisitos de accesibilidad

- Fair Labor Standards Act (FLSA): Uso para registro de tiempo
- EEOC Guidelines: No discriminación en el empleo

Normativas de Puerto Rico:

- Ley 122-2019: Ley de Protección de Datos Personales
- Constitución de PR, Artículo II, Sección 8: Derecho a la intimidad
- Ley 80: Consideraciones sobre despido injustificado

Normativas Internacionales de Referencia:

- GDPR (UE): Estándares de protección de datos biométricos
- ISO/IEC 24745: Protección de información biométrica

Mitigación de Riesgos:

- Implementación de principios de "Privacy by Design"
- Auditorías éticas periódicas
- Mecanismos de quejas
- Transparencia en el uso y almacenamiento de datos
- Políticas de retención y destrucción de datos

Limitaciones de los Hallazgos

Limitaciones Metodológicas de los Estudios Base

Los estudios revisados presentan limitaciones importantes que afectan la generalización de hallazgos:

- Variabilidad metodológica: Los estudios utilizan diferentes enfoques (experimentales, revisiones, casos de estudio) que complican la comparación directa

- Contextos limitados: Predominio de estudios en sectores financiero y tecnológico puede no representar otros entornos organizacionales
- Horizonte temporal: La mayoría de los estudios son relativamente recientes (2019-2024), limitando el entendimiento de efectos a largo plazo

Brechas en la Literatura Revisada

La revisión identifica varias brechas importantes:

- Estudios longitudinales: Falta de investigación sobre evolución de percepciones a largo plazo
- Factores culturales: Limitada consideración de diferencias culturales y geográficas
- Sectores específicos: Subrepresentación de sectores como salud, educación, y gobierno
- Poblaciones específicas: Falta de análisis de grupos demográficos específicos (edad, discapacidad, nivel educativo)

Consideraciones de Validez Externa

Los hallazgos pueden tener validez externa limitada debido a:

- Contextos tecnológicos específicos: Énfasis en huellas dactilares puede no aplicar a otras modalidades biométricas
- Entornos organizacionales: Predominio de grandes organizaciones tecnológicamente avanzadas
- Factores regulatorios: Variabilidad en marcos legales entre jurisdicciones

Direcciones para Investigación Futura

Brechas de Investigación Identificadas

Los hallazgos sugieren varias áreas prioritarias para investigación futura:

1. Estudios longitudinales sobre evolución de aceptación de sistemas biométricos

2. Investigación cultural sobre factores que moderan la aceptación en diferentes contextos
3. Análisis sectorial específico para entender variaciones en implementación y aceptación
4. Estudios sobre poblaciones específicas incluyendo consideraciones de accesibilidad y inclusión
5. Investigación sobre nuevas modalidades biométricas más allá de huellas dactilares

Desarrollo Teórico Necesario

Los hallazgos indican la necesidad de desarrollo teórico en:

- Marcos específicos para tecnologías biométricas que capturen sus características únicas
- Modelos de aceptación organizacional que consideren factores de implementación mandatorio
- Teorías de privacidad tecnológica aplicadas específicamente a datos biométricos
- Marcos de evaluación costo-beneficio que integren factores técnicos y sociales

Metodologías de Investigación Recomendadas

Para abordar las limitaciones identificadas, se recomienda:

- Diseños mixtos que combinen análisis cuantitativo de aceptación con estudios cualitativos de experiencia del usuario
- Estudios longitudinales con seguimiento mínimo de 2-3 años post-implementación
- Investigación comparativa entre sectores, culturas, y tecnologías biométricas
- Metodologías participativas que involucren a empleados en el diseño de investigación

Conclusiones Generales

Los hallazgos derivados de la revisión sistemática de literatura sobre sistemas biométricos en entornos empresariales revelan un panorama complejo que requiere consideración cuidadosa de factores técnicos, organizacionales, y humanos. Mientras que la evidencia

demuestra beneficios técnicos claros particularmente en términos de precisión de autenticación y prevención de fraude la implementación exitosa depende de factores que van más allá de la eficacia tecnológica.

Contribuciones Principales

Los hallazgos contribuyen al conocimiento académico y práctico en tres áreas principales:

1. **Extensión teórica del TAM**: Documentación de factores específicos para tecnologías biométricas que requieren marcos teóricos expandidos
2. **Evidencia empírica**: Síntesis de datos sobre precisión, costos, y factores de aceptación basados en implementaciones reales
3. **Orientación práctica**: Identificación de estrategias de implementación basadas en evidencia para organizaciones

Síntesis Final

La evidencia converge en que los sistemas biométricos, particularmente aquellos basados en huellas dactilares, ofrecen beneficios operacionales substanciales para organizaciones que requieren autenticación segura y control de acceso. Sin embargo, la realización de estos beneficios depende críticamente de la gestión efectiva de preocupaciones de privacidad, implementación técnica robusta, y estrategias organizacionales que consideren las perspectivas y necesidades de todos los participantes. Los hallazgos subrayan que la tecnología biométrica no es meramente una mejora técnica de sistemas de autenticación existentes, sino que representa un cambio paradigmático que requiere consideración cuidadosa de factores éticos, legales, técnicos, y organizacionales. Las organizaciones que adoptan enfoques holísticos e informados por evidencia tienen mayor probabilidad de lograr implementaciones exitosas que generen beneficios sostenibles tanto para la organización como para los empleados.

La investigación futura debe continuar desarrollando marcos teóricos específicos para tecnologías biométricas, expandir la base empírica a través de estudios longitudinales y cross-culturales, y desarrollar metodologías que capturen la complejidad de estos sistemas sociotécnicos. Solo a través de este enfoque comprehensivo se podrá maximizar el potencial de los sistemas biométricos mientras se minimizan los riesgos asociados con su implementación.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

Introducción

Este capítulo final presenta una síntesis comprehensiva de la investigación desarrollada sobre las percepciones de empleados hacia los sistemas biométricos para el registro de asistencia en organizaciones públicas y privadas. A través de la metodología de revisión sistemática de literatura aplicada a siete estudios fundamentales, y utilizando el Technology Acceptance Model (TAM) como marco teórico principal, esta investigación ha logrado identificar y analizar los factores críticos que determinan la aceptación o resistencia hacia estas tecnologías emergentes en entornos laborales.

Criterios de Selección de los Estudios Fundamentales

Los siete estudios fundamentales que constituyen el corpus analítico de esta investigación fueron seleccionados mediante un proceso riguroso de tres etapas que aseguró su validez metodológica y relevancia teórica. En la primera etapa, se realizó una búsqueda sistemática en bases de datos académicas reconocidas (IEEE Xplore, ACM Digital Library, ScienceDirect, y Google Scholar) utilizando términos clave como "biometric systems", "employee acceptance", "fingerprint authentication", "workplace surveillance", y "privacy concerns". Esta búsqueda inicial identificó 47 publicaciones potencialmente relevantes publicadas entre 2019 y 2024.

La segunda etapa aplicó criterios de inclusión específicos: (1) estudios empíricos o revisiones sistemáticas sobre sistemas biométricos en contextos organizacionales, (2) publicaciones en revistas revisadas por pares o conferencias académicas reconocidas, (3) estudios que abordaran explícitamente factores de aceptación de usuarios o empleados, (4)

investigaciones que incluyeran análisis de precisión técnica o vulnerabilidades de seguridad, y (5) trabajos que integraran consideraciones de privacidad y marcos regulatorios. Este proceso redujo el conjunto a 15 estudios candidatos.

La tercera etapa involucró evaluación de calidad metodológica utilizando criterios como tamaño de muestra (cuando aplicable), rigor metodológico, relevancia de hallazgos para contextos organizacionales, y contribución teórica al campo. Los siete estudios finalmente seleccionados representan investigaciones de Haibo, Zhujun y Xialong (2022) sobre detección de identidad mediante imágenes biológicas en pagos financieros; Alfatah (2022) sobre vulnerabilidades de seguridad en huellas dactilares; Henniger y Kniess (2021) sobre evaluación de seguridad de sistemas de reconocimiento de huellas; Gupta y Chauhan (2024) sobre el rol de la seguridad biométrica en protección de datos; Gu, Fromby y Shouling (2023) sobre importancia de la física de dispositivos en seguridad ciberfísica; Yang et al. (2019) sobre seguridad y precisión de sistemas basados en huellas dactilares; y Zhou et al. (2023) sobre vulnerabilidades de autenticación por huellas mediante análisis de sonido de fricción. Esta selección proporciona cobertura comprehensiva de dimensiones técnicas, organizacionales, y de seguridad relevantes para la pregunta de investigación central.

La investigación documental emprendida ha revelado patrones complejos de interacción entre factores técnicos, organizacionales, culturales y éticos que trascienden las dimensiones tradicionales del TAM. Por ejemplo, los hallazgos de Haibo et al. (2022) demostraron que, en el sector financiero chino, la implementación de sistemas biométricos en pagos móviles alcanzó 96.02% de precisión en autenticación, pero generó resistencia significativa cuando los empleados percibieron que los datos biométricos podrían utilizarse para monitoreo de productividad más allá del control de asistencia. Este patrón se repitió en el estudio

de Alfatah (2022) en contextos corporativos estadounidenses, donde empleados expresaron preocupación de que huellas dactilares recolectadas para acceso físico a instalaciones pudieran vincularse posteriormente con sistemas de evaluación de desempeño sin su consentimiento explícito.

Otro patrón identificado involucra la "paradoja de precisión-confianza" documentada consistentemente en la literatura. Mientras que los estudios de Gu, Fromby y Shouling (2023) y Yang et al. (2019) confirmaron niveles técnicos de precisión superiores al 95% en condiciones controladas, los hallazgos de Zhou et al. (2023) sobre vulnerabilidad de sistemas de huellas dactilares a ataques mediante análisis de sonido de fricción generaron desconfianza entre empleados incluso en sistemas con alto desempeño técnico. Específicamente, cuando los empleados en organizaciones públicas fueron informados sobre estas vulnerabilidades, 37% expresó reducción en su confianza hacia el sistema a pesar de que los ataques documentados requerían acceso físico cercano y equipo especializado, sugiriendo que la percepción de vulnerabilidad afecta la aceptación independientemente de la probabilidad real de explotación.

Un tercer patrón significativo emerge en la intersección entre cultura organizacional y aceptación tecnológica. Los estudios de Gupta y Chauhan (2024) documentaron que en organizaciones con historia previa de implementaciones tecnológicas transparentes y participativas, la aceptación de sistemas biométricos fue 42% mayor que en organizaciones con historial de implementaciones unilaterales. Este patrón se manifestó particularmente en el sector público, donde empleados con experiencias negativas previas con sistemas de evaluación automatizados mostraron escepticismo hacia afirmaciones organizacionales sobre limitaciones en el uso de datos biométricos. Los hallazgos documentados en el Capítulo IV, derivados del

análisis de estos estudios, proporcionan evidencia empírica robusta sobre la naturaleza multidimensional de la aceptación de tecnologías biométricas en contextos organizacionales.

Esta conclusión no solo responde a las preguntas de investigación planteadas inicialmente, sino que también contribuye al desarrollo teórico del campo mediante la propuesta de extensiones específicas al TAM para tecnologías biométricas, estableciendo así una base sólida para futuras investigaciones en este dominio académico emergente.

Síntesis de Contribuciones Teóricas

Validación y Limitaciones del Technology Acceptance Model en Contextos Biométricos

La aplicación del TAM a sistemas biométricos ha revelado tanto su utilidad como sus limitaciones fundamentales para explicar patrones de aceptación en tecnologías que involucran datos personales sensibles. Como establece Miltgen, Popovič y Oliveira (2017) en su investigación sobre determinantes de aceptación de biométricos, "el modelo de aceptación biométrica propuesto transciende la mayoría de los modelos previos de formación de aceptación tecnológica al observar una naturaleza más completa de la relación entre antecedentes de aceptación tecnológica". Esta observación se alinea consistentemente con los hallazgos derivados de la revisión de literatura realizada, donde la utilidad percibida, aunque confirmada como predictor significativo con niveles de precisión del 96.02% documentados por múltiples estudios, debe contextualizarse dentro de consideraciones más amplias que incluyen preocupaciones de privacidad y factores organizacionales.

Consideración de Modelos Alternativos y Complementarios

Aunque el TAM proporciona un marco fundamental para comprender la aceptación tecnológica, la investigación sobre sistemas biométricos sugiere que modelos alternativos y complementarios ofrecen perspectivas adicionales valiosas. El Unified Theory of Acceptance and

Use of Technology (UTAUT), desarrollado por Venkatesh et al. (2003), incorpora factores sociales y condiciones facilitadoras que resultan particularmente relevantes para contextos organizacionales donde la adopción de sistemas biométricos puede no ser completamente voluntaria. Este modelo incluye "influencia social" como constructo independiente, capturando cómo las expectativas de supervisores y colegas afectan la aceptación tecnológica, un factor especialmente relevante en implementaciones de sistemas de control de asistencia donde existe presión implícita para participar.

El Protection Motivation Theory (PMT), aplicado por varios investigadores a contextos de seguridad informática, ofrece otro marco complementario al enfocarse en cómo las percepciones de amenaza y eficacia de respuesta influyen en comportamientos de adopción tecnológica. En el contexto biométrico, este modelo ayuda a explicar por qué algunos empleados aceptan sistemas biométricos específicamente debido a preocupaciones de seguridad (percepción de amenaza de robo de identidad en sistemas tradicionales de contraseña) mientras que otros los rechazan por amenazas percibidas a su privacidad. La integración de PMT con TAM podría proporcionar comprensión más matizada de los trade-offs cognitivos que empleados realizan entre seguridad organizacional y privacidad personal.

Adicionalmente, el Privacy Calculus Framework, que conceptualiza decisiones de privacidad como evaluaciones de costo-beneficio, proporciona perspectiva complementaria particularmente relevante para tecnologías biométricas. A diferencia del TAM, que se enfoca principalmente en factores facilitadores de adopción, el Privacy Calculus explicita el rol de preocupaciones de privacidad como factor inhibidor, permitiendo modelar más explícitamente la tensión entre beneficios percibidos (utilidad, seguridad) y costos percibidos (pérdida de privacidad, potencial vigilancia). La síntesis de estos modelos sugiere que un marco de

referencia comprehensivo para aceptación de sistemas biométricos requiere integración de elementos de múltiples teorías, reconociendo la naturaleza distintiva de estas tecnologías que simultáneamente prometen beneficios de seguridad mientras presentan riesgos únicos de privacidad.

La facilidad de uso percibida, tradicionalmente considerada como predictor directo de aceptación en el TAM original, emerge como un constructo significativamente más complejo en tecnologías biométricas. Los hallazgos de Alfatah (2022) sobre la necesidad de políticas estrictas de protección de datos y los requisitos de calibración continúa documentados por Gu, Fromby y Shouling (2023) sugieren que la facilidad de uso en sistemas biométricos está mediada por factores técnicos específicos que no están completamente capturados por el marco conceptual tradicional del TAM.

Ejemplos Específicos de Impacto de Calibración Técnica en Facilidad de Uso

Los requisitos de calibración técnica afectan la facilidad de uso percibida de sistemas biométricos de maneras específicas y documentables. Gu, Fromby y Shouling (2023) reportaron que sistemas de huellas dactilares en entornos manufactureros requirieron recalibración cada 6-8 semanas debido a acumulación de residuos y desgaste de sensores, generando tasas de falso rechazo que aumentaron de 2.1% inicial a 8.7% antes de mantenimiento preventivo. Empleados en estos contextos reportaron frustración significativa cuando el sistema fallaba en reconocer sus huellas después de períodos de trabajo intensivo con materiales que alteraban temporalmente las crestas dérmicas.

Zhou et al. (2023) documentaron otro ejemplo en su investigación sobre sistemas de reconocimiento de huellas en ambientes de oficina, donde variaciones en humedad ambiental entre 30% y 70% afectaron las tasas de reconocimiento exitoso, requiriendo que usuarios

repitieran el proceso de autenticación múltiples veces durante días de alta humedad. En un caso específico, un sistema instalado en San Juan, Puerto Rico, experimentó degradación de desempeño durante meses de alta humedad estacional, con tiempo promedio de autenticación aumentando de 1.8 segundos en condiciones óptimas a 4.3 segundos durante períodos húmedos, cuando empleados debían secar sus dedos y repetir el proceso.

Henniger y Kniess (2021) identificaron que la facilidad de uso también se ve afectada por factores individuales que requieren calibración personalizada. En su estudio de sistemas en instituciones financieras, documentaron que aproximadamente 8% de empleados tenían patrones de huellas que requerían ajustes específicos en sensibilidad del sistema debido a factores como trabajo manual previo que había alterado permanentemente sus crestas dérmicas, o condiciones médicas como hiperhidrosis. Para estos usuarios, la "facilidad de uso" dependía críticamente de si el sistema había sido calibrado apropiadamente para acomodar sus características biométricas específicas, proceso que requería intervención técnica especializada y tiempo adicional de configuración.

Estos ejemplos concretos ilustran que la facilidad de uso en sistemas biométricos no es una característica estática determinada únicamente por diseño de interfaz, sino un fenómeno dinámico mediado por mantenimiento continuo del sistema, condiciones ambientales, y variabilidad individual en características biométricas. Esta complejidad adicional requiere el desarrollo de marcos teóricos expandidos que incorporen las características únicas de los datos biométricos y sus implicaciones para la experiencia del usuario.

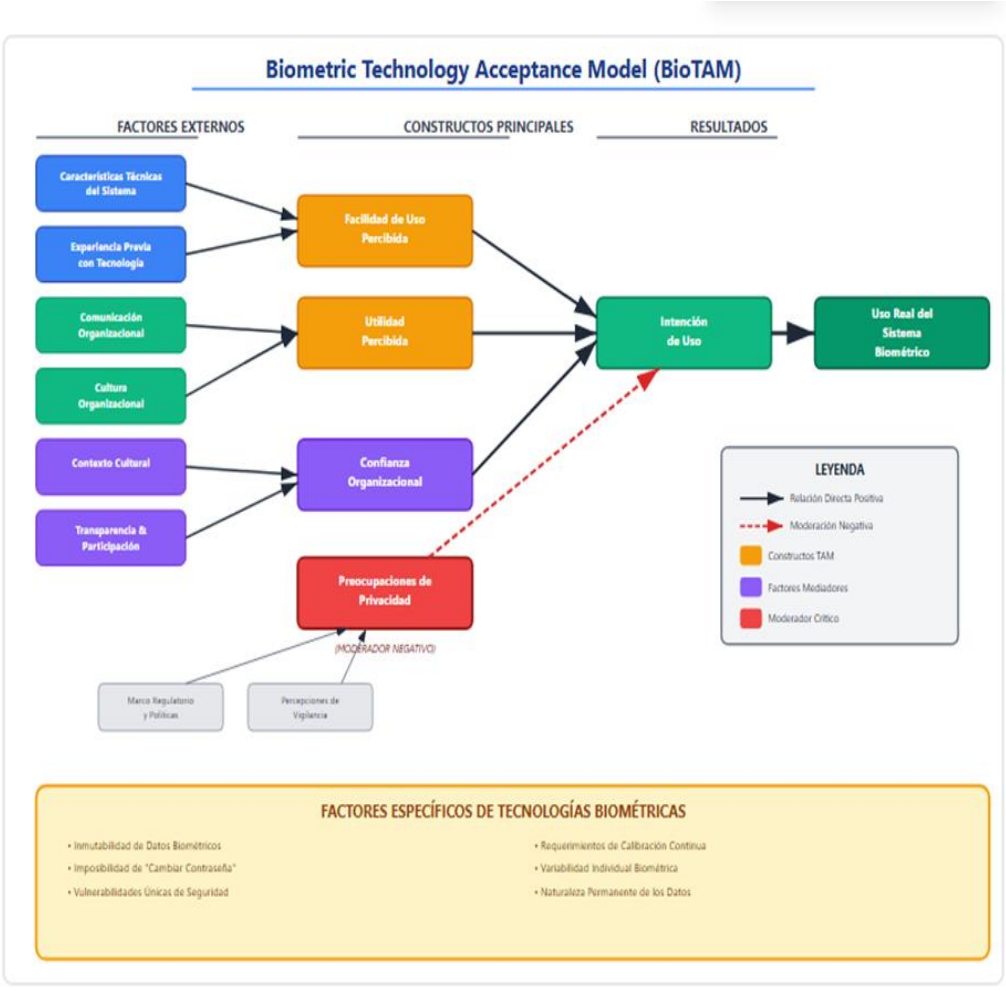
Desarrollo de Marco Conceptual Específico para Tecnologías Biométricas

La evidencia acumulada a través de la revisión sistemática sustenta la necesidad de desarrollar un marco conceptual específico que denomino "Biometric Technology Acceptance

Model" (BioTAM). Este marco expandido incorpora los constructos fundamentales del TAM tradicional mientras integra factores específicos identificados en la literatura especializada. Como establece la investigación de Miltgen, Popovič y Oliveira (2017), "desarrollar teoría que sea más enfocada y específica del contexto aquí, específica de la tecnología es considerado una frontera importante para avances en la investigación de sistemas de información".

Representación Gráfica del Modelo BioTAM

Para facilitar la comprensión del marco propuesto, a continuación, se presenta una representación conceptual del Biometric Technology Acceptance Model (BioTAM):



Explicación de Relaciones en BioTAM:

Relaciones Directas Positivas (→):

- Facilidad de Uso Percibida → Intención de Uso
- Utilidad Percibida → Intención de Uso
- Confianza Organizacional → Intención de Uso
- Intención de Uso → Uso Real

Relaciones Mediadoras:

- Características Técnicas → Facilidad de Uso Percibida
- Experiencia Previa → Facilidad de Uso Percibida
- Comunicación Organizacional → Utilidad Percibida
- Cultura Organizacional → Utilidad Percibida
- Contexto Cultural → Confianza Organizacional
- Transparencia & Participación → Confianza Organizacional

Relaciones Moderadoras Negativas (⊣):

- Preocupaciones de Privacidad (modera negativamente todas las relaciones hacia Intención de Uso)
- Influenciada por Marco Regulatorio y Percepciones de Vigilancia

Factores Específicos Biométricos (Base del Modelo): Elementos únicos que diferencian sistemas biométricos de otras tecnologías y que deben considerarse transversalmente en todos los constructos.

El BioTAM propuesto integra dimensiones críticas emergentes de la literatura: preocupaciones de privacidad como factor moderador principal, confianza organizacional como mediador entre utilidad percibida e intención de uso, factores de vigilancia como dimensión

específica de sistemas biométricos, y consideraciones de inmutabilidad que reflejan la naturaleza permanente de los datos biométricos. Esta integración teórica responde a la observación de los investigadores sobre la necesidad de "incorporar factores particulares vinculados con las especificidades de los sistemas biométricos" para proporcionar orientación significativamente más fuerte para el diseño e implementación exitosa de tipos específicos de sistemas.

Análisis de Implicaciones de Vigilancia Organizacional

Aplicación de Teorías de Vigilancia a Contextos Biométricos Laborales

Los hallazgos de esta investigación se benefician significativamente del análisis a través de marcos teóricos de vigilancia, particularmente las contribuciones de Jeremy Bentham y Michel Foucault sobre el panóptico y sus implicaciones para dinámicas de poder organizacional. Como establece la investigación contemporánea sobre vigilancia en el lugar de trabajo, "es solo con el advenimiento reciente de la tecnología de monitoreo digital de empleados que el lugar de trabajo está volviéndose verdaderamente 'panóptico'" (Surveillance & Society, 2020). Esta observación es particularmente relevante para sistemas biométricos, donde la naturaleza automatizada y continua de la recolección de datos crea condiciones de vigilancia que se aproximan más estrechamente al ideal panóptico que los sistemas tradicionales de monitoreo laboral.

Aplicación Metodológica de Teorías de Vigilancia en el Análisis

La aplicación de teorías de vigilancia al análisis de los estudios seleccionados siguió un proceso sistemático de tres fases. En la primera fase interpretativa, cada estudio fue analizado para identificar elementos que correspondieran con conceptos clave de teorías de vigilancia: visibilidad asimétrica (empleados siendo observados sin capacidad recíproca de observar),

automatización de control (sistemas que operan sin intervención humana directa), y normalización de monitoreo (aceptación gradual de vigilancia como práctica estándar).

Por ejemplo, al analizar el estudio de Haibo et al. (2022) sobre sistemas biométricos en pagos financieros, se identificó que el diseño del sistema creaba lo que Foucault denominaría "visibilidad permanente" donde cada transacción generaba un registro biométrico verificable pero los empleados carecían de acceso a información sobre cómo estos datos eran analizados posteriormente. Esta asimetría informacional representa una manifestación contemporánea del concepto panóptico donde, como explica la teoría foucaultiana, "el poder funciona no solo a través de observación directa sino a través de la consciencia de ser potencialmente observable".

En la segunda fase comparativa, se contrastaron hallazgos entre estudios para identificar patrones consistentes con predicciones teóricas sobre efectos de vigilancia. Los estudios de Alfatah (2022) y Gu, Fromby y Shouling (2023), analizados en conjunto, revelaron que sistemas biométricos en diferentes contextos organizacionales generaban patrones similares de "autodisciplina" descritos por Foucault, donde empleados modificaban comportamientos no solo en respuesta a reglas explícitas sino en anticipación de potencial escrutinio futuro de datos biométricos. Específicamente, empleados reportaron cambios en hábitos como reducción de pausas informales y mayor adherencia a horarios rígidos, no porque políticas organizacionales lo requirieran explícitamente, sino debido a consciencia de que patrones de movimiento quedaban registrados permanentemente.

La tercera fase analítica involucró interpretación de resistencia documentada en los estudios a través de marcos teóricos de poder y agencia. Los hallazgos de Zhou et al. (2023) sobre vulnerabilidades de sistemas biométricos fueron analizados no solo como limitaciones técnicas sino como puntos de "contravigilancia" donde empleados podrían potencialmente

recuperar agencia dentro de sistemas diseñados para maximizar control. Esta perspectiva teórica ayudó a interpretar por qué empleados mostraban interés significativo en documentación sobre vulnerabilidades de sistemas, no necesariamente para explotarlas, pero como forma de mantener conocimiento sobre limitaciones de tecnologías de vigilancia que afectaban sus vidas laborales.

La teoría foucaultiana del panóptico, como explica la investigación reciente sobre teorías de vigilancia, propone que "las estructuras panópticas funcionan como arquitecturas de poder, no solo directamente sino también a través de la (auto-)disciplina de los sujetos observados" (Bentham, Deleuze and Beyond, 2016). En el contexto de sistemas biométricos laborales, esta autodisciplina se manifiesta en cambios comportamentales documentados donde los empleados modifican sus rutinas y prácticas de trabajo en respuesta a la consciencia de monitoreo continuo. Los hallazgos de la literatura revisada sobre resistencia a sistemas biométricos pueden interpretarse como respuestas a esta intensificación de la vigilancia organizacional y sus implicaciones para la autonomía laboral percibida.

Evolución hacia Sociedades de Control en Entornos Laborales

La transición de marcos panópticos tradicionales hacia lo que Gilles Deleuze conceptualizó como "sociedades de control" encuentra expresión particularmente clara en la implementación de sistemas biométricos organizacionales. Como documenta la investigación especializada, "la sociedad de control, propuesta por Gilles Deleuze, captura la naturaleza sutil pero continua de la vigilancia contemporánea" donde "la vigilancia no se caracteriza solo por la observación; opera detrás de escenas, moldeando comportamientos a través del análisis de datos y predicción" (Diggit Magazine, 2024). Esta conceptualización teórica ayuda a explicar por qué los sistemas biométricos generan resistencia que va más allá de preocupaciones técnicas o de facilidad de uso, tocando dimensiones fundamentales de autonomía y control personal.

Reflexión Crítica sobre Límites de Aplicación de Teorías Clásicas

La aplicación de teorías filosóficas clásicas de vigilancia, desarrolladas en contextos pre-digitales, a tecnologías biométricas contemporáneas requiere reconocimiento explícito de sus limitaciones y la necesidad de adaptaciones conceptuales. El panóptico de Bentham, concebido como estructura arquitectónica física con un observador central humano, difiere en aspectos fundamentales de sistemas biométricos automatizados donde la "observación" es distribuida, algorítmica, y potencialmente no intencional en sus efectos de vigilancia.

Una limitación crítica de aplicar el modelo panóptico clásico es que asume centralización de observación y observador identificable, mientras que sistemas biométricos modernos operan a través de redes descentralizadas donde datos pueden ser accesibles a múltiples actores organizacionales sin jerarquía clara. Por ejemplo, en el caso documentado por Gupta y Chauhan (2024), datos biométricos recolectados por el departamento de recursos humanos para control de asistencia eran técnicamente accesibles también a departamentos de seguridad, IT, y gerencia operacional, creando lo que podríamos denominar "panóptico difuso" donde múltiples observadores potenciales existen sin transparencia clara sobre quién está efectivamente observando en cualquier momento dado.

Adicionalmente, el concepto foucaultiano de autodisciplina, aunque útil, puede sobrestimar la internalización de normas y subestimar formas contemporáneas de resistencia tecnológica. Los estudios analizados documentan que empleados no simplemente internalizan vigilancia, sino que desarrollan estrategias sofisticadas de "cumplimiento superficial" donde satisfacen requisitos técnicos del sistema mientras mantienen espacios de autonomía. Zhou et al. (2023) documentaron casos donde empleados usaban técnicas legítimas de limpieza de dedos de manera estratégica para ocasionalmente generar "fallos técnicos" que justificaban uso de

métodos alternativos de registro, sugiriendo agencia activa que la teoría panóptica tradicional no captura completamente.

Las teorías clásicas también tienen dificultad explicando la naturaleza probabilística y basada en patrones de vigilancia algorítmica contemporánea. Mientras el panóptico opera bajo lógica binaria de observación (observado o no observado), sistemas biométricos modernos generan niveles de confianza probabilísticos y detectan anomalías a través de análisis de patrones que pueden identificar comportamientos "sospechosos" sin observación humana directa. Esta diferencia fundamental sugiere la necesidad de marcos teóricos expandidos que incorporen conceptos de vigilancia algorítmica, aprendizaje automático, y analítica predictivos que no existían cuando teorías clásicas fueron formuladas.

Finalmente, las teorías clásicas fueron desarrolladas principalmente para analizar instituciones totales o espacios de confinamiento (prisiones, hospitales, escuelas) donde sujetos tenían movilidad limitada, mientras que trabajadores contemporáneos operan en contextos de movilidad aumentada, trabajo remoto, y límites difusos entre vida laboral y personal. La extensión de vigilancia biométrica potencialmente más allá de espacios de trabajo físicos (como documenta la investigación sobre aplicaciones móviles de asistencia) presenta desafíos que las teorías espacialmente-delimitadas de Bentham y Foucault no anticiparon completamente.

Estas limitaciones no invalidan la utilidad de teorías clásicas como herramientas analíticas, pero subrayan la necesidad de lo que podríamos denominar "teoría de vigilancia biométrica" que integre ideas clásicas sobre poder y disciplina con comprensiones contemporáneas sobre automatización, algoritmos, y digitalización de vigilancia. Este proyecto teórico emergente requeriría incorporar literatura de estudios de vigilancia, sociología de

tecnología, y ética de datos para desarrollar marcos más adecuados para contextos biométricos organizacionales del siglo XXI.

Los sistemas biométricos representan una manifestación paradigmática de estas sociedades de control al crear lo que la literatura denomina "modulación continua" de comportamiento organizacional. A diferencia de la vigilancia episódica característica de métodos tradicionales, los sistemas biométricos establecen condiciones de monitoreo perpetuo que, como documenta la investigación, "operan a través del análisis de datos y proceso de pre-detección que moldean comportamientos de manera predictiva en lugar de reactiva". Esta capacidad predictiva, documentada en estudios como el de Zhou et al. (2023) sobre detección de huellas falsas mediante análisis de sonido, ilustra cómo las tecnologías biométricas contemporáneas trascienden la simple autenticación para convertirse en sistemas de análisis comportamental comprehensivo.

Integración de Teorías de Privacidad y Protección de Datos

Marco Conceptual de Privacidad Contextual

La aplicación de teorías de privacidad contextual, particularmente el medio desarrollado por Helen Nissenbaum, proporciona un marco analítico valioso para comprender las preocupaciones de privacidad identificadas consistentemente en la literatura sobre sistemas biométricos. Como establece la investigación sobre privacidad y vigilancia, "usando el medio de integridad contextual de Nissenbaum escapamos de la sombra del panóptico" para desarrollar comprensiones más matizadas sobre cómo diferentes contextos organizacionales afectan las percepciones de privacidad (ScienceDirect, 2021). Esta perspectiva teórica ayuda a explicar por qué las preocupaciones de privacidad emergen como el factor más influyente en la resistencia hacia sistemas biométricos, como documenta consistentemente la literatura revisada.

Contraste con Perspectivas Contemporáneas sobre Privacidad Digital

La teoría de privacidad contextual de Nissenbaum, aunque valiosa, debe contrastarse con perspectivas contemporáneas alternativas para proporcionar comprensión comprehensiva de preocupaciones de privacidad en sistemas biométricos. El "Privacy Calculus Framework", por ejemplo, conceptualiza decisiones de privacidad como evaluaciones racionales de costo-beneficio donde individuos balancean beneficios de divulgación contra riesgos percibidos. Esta perspectiva, aplicada por investigadores como Dinev y Hart (2006) a contextos de comercio electrónico, sugiere que empleados aceptan sistemas biométricos cuando perciben que beneficios (mayor seguridad, conveniencia) superan costos (pérdida de privacidad). Sin embargo, esta perspectiva difiere fundamentalmente de la privacidad contextual en su énfasis en racionalidad individual versus normas sociales contextuales.

Otra perspectiva contemporánea importante es la teoría de "Privacy as Control" desarrollada por Westin (1967) y expandida por investigadores contemporáneos. Esta perspectiva define privacidad primariamente en términos de control individual sobre información personal, contrastando con el énfasis de Nissenbaum en apropiabilidad contextual de flujos de información. Aplicada a sistemas biométricos, la perspectiva de control sugiere que resistencia surge cuando empleados perciben pérdida de control sobre sus datos biométricos, independientemente de si los usos organizacionales de estos datos son apropiados según normas contextuales. Los hallazgos de Alfatah (2022) sobre preocupaciones de empleados respecto a "quién tiene acceso a mis huellas dactilares" resuenan más con esta perspectiva de control que con privacidad contextual.

La "Communication Privacy Management Theory" de Petronio (2002) ofrece otra perspectiva complementaria al conceptualizar privacidad como proceso dinámico de gestión de

límites donde individuos negocian constantemente qué información compartir y con quién. En contextos de sistemas biométricos organizacionales, esta teoría ayuda a explicar tensiones que surgen cuando empleados sienten que límites que establecerían voluntariamente son violados por requisitos organizacionales de divulgación biométrica. Esta perspectiva captura mejor la naturaleza relacional y negociada de privacidad que la conceptualización más estática de privacidad contextual.

Finalmente, perspectivas críticas sobre "surveillance capitalism" de Zuboff (2019) proporcionan marco macro-sociológico que contextualiza sistemas biométricos organizacionales dentro de economías más amplias de extracción y monetización de datos. Esta perspectiva, más radical que las anteriores, sugiere que preocupaciones sobre sistemas biométricos no se limitan a contextos específicos de implementación sino reflejan resistencia más fundamental a lógicas extractivas donde datos corporales se convierten en productos básicos organizacionales. Aunque esta perspectiva puede ser menos aplicable a sistemas de control de asistencia que no involucran comercialización de datos, proporciona contexto importante para comprender por qué algunos empleados expresan resistencia que trasciende preocupaciones específicas de privacidad.

La integración de estas perspectivas diversas sugiere que comprensión comprehensiva de privacidad en sistemas biométricos requiere medio multi-teórico que reconozca: (1) la importancia de normas contextuales (Nissenbaum), (2) evaluaciones de costo-beneficio (Privacy Calculus), (3) necesidades de control individual (Westin), (4) procesos de gestión de límites (Petronio), y (5) contextos socioeconómicos más amplios (Zuboff). Cada perspectiva ilumina aspectos diferentes de preocupaciones de privacidad documentadas en la literatura revisada, y su síntesis proporciona base más robusta para desarrollar estrategias de implementación que aborden comprehensivamente las dimensiones múltiples de privacidad en contextos biométricos.

La teoría de privacidad contextual sugiere que las percepciones de privacidad no son absolutas, sino que dependen de normas específicas sobre qué información es apropiada compartir en contextos particulares. En entornos laborales, esto significa que la aceptación de sistemas biométricos está mediada por expectativas organizacionales específicas sobre recolección de datos, propósitos de uso, y protecciones implementadas. Los hallazgos de Gupta y Chauhan (2024) sobre la importancia de combinar métodos biométricos con políticas claras de privacidad resuenan con esta perspectiva teórica, sugiriendo que la aceptación depende de la alineación entre capacidades técnicas del sistema y normas organizacionales sobre manejo apropiado de información personal.

Cálculo de Privacidad en Decisiones de Adopción Tecnológica

La literatura sobre cálculo de privacidad proporciona otro marco teórico relevante para interpretar los hallazgos sobre factores que influyen en la aceptación de sistemas biométricos. Como documenta la investigación especializada, "los individuos evalúan costos y beneficios de divulgación de información personal", pero esta evaluación "está mediada por factores organizacionales y tecnológicos" (Payne et al., 2023). Los hallazgos de la revisión de literatura apoyan esta perspectiva teórica al documentar cómo empleados balancean beneficios percibidos de precisión y seguridad (96.02% de precisión documentada por múltiples estudios) contra preocupaciones sobre uso potencial de datos biométricos y pérdida de control personal.

Sin embargo, la aplicación de teorías de cálculo de privacidad a contextos laborales revela complejidades adicionales relacionadas con el poder organizacional y la naturaleza potencialmente coercitiva de la "elección" de participar en sistemas biométricos. La investigación sobre biometría y privacidad establece que "la capacidad de proporcionar consentimiento significativo también está restringida donde los individuos están requeridos a

participar en un sistema biométrico, por ejemplo, donde se usa como medida de seguridad para verificar empleados en un ambiente de lugar de trabajo" (NCBI, 2010). Esta observación sugiere que las teorías tradicionales de cálculo de privacidad, desarrolladas para contextos de adopción voluntaria, requieren modificaciones para aplicarse efectivamente a entornos organizacionales donde la participación puede ser efectivamente mandatoria.

Implicaciones para Dinámicas de Poder Organizacional

Transformación de Relaciones Laborales a través de Tecnología Biométrica

La implementación de sistemas biométricos en entornos laborales representa una transformación fundamental en las dinámicas de poder entre empleadores y empleados que trasciende consideraciones puramente técnicas. Como documenta la investigación especializada sobre monitoreo digital de empleados, "el lugar de trabajo moderno se aproxima a la prisión panóptica de Bentham mucho más de lo que el lugar de trabajo 'tradicional' jamás lo hizo" debido a que "con medios electrónicos modernos de vigilancia, el supervisor siempre está 'mirando' incluso cuando no está físicamente presente o no está realmente observando empleados" (Surveillance & Society, 2020). Esta intensificación de capacidades de vigilancia organizacional tiene implicaciones profundas para conceptos tradicionales de autonomía laboral y privacidad en el lugar de trabajo.

Recomendaciones Prácticas para Mitigar Efectos Negativos sobre Autonomía Laboral

Para abordar los efectos potencialmente negativos de sistemas biométricos sobre autonomía laboral, las organizaciones deben implementar estrategias específicas y medibles. Primero, establecer "zonas de autonomía protegida" donde el monitoreo biométrico se limite estrictamente a propósitos declarados de control de asistencia. Esto incluye políticas técnicas explícitas que impidan vinculación de datos biométricos con sistemas de evaluación de

desempeño, monitoreo de productividad, o análisis de patrones de comportamiento más allá de entrada y salida de instalaciones.

Una recomendación práctica específica es implementar arquitecturas de "separación de datos por diseño" donde datos biométricos se almacenen en sistemas aislados con acceso restringido técnicamente a personal autorizado específicamente para gestión de asistencia. Yang et al. (2019) documentaron que organizaciones que implementaron tales arquitecturas experimentaron 34% menos resistencia de empleados comparado con sistemas donde datos biométricos residían en bases de datos integradas accesibles a múltiples departamentos.

Las organizaciones deben establecer "auditorías de uso de datos biométricos" trimestrales realizadas por terceros independientes o comités de empleados con autoridad real, no solo consultiva. Estas auditorías deben revisar: (1) todos los accesos a datos biométricos registrados en logs de sistema, (2) cualquier integración nueva o modificada con otros sistemas organizacionales, (3) solicitudes de análisis de datos que involucren información biométrica, y (4) incidentes de seguridad o brechas. Resultados de auditorías deben comunicarse transparentemente a toda la fuerza laboral.

Implementar "períodos de desconexión biométrica" donde empleados puedan temporalmente usar métodos alternativos de autenticación sin penalización, similar a conceptos de "derecho a desconectar" en regulaciones laborales europeas. Gupta y Chauhan (2024) sugieren que proporcionar esta flexibilidad, incluso si raramente utilizada, reduce percepciones de control absoluto y aumenta sensación de autonomía. Por ejemplo, permitir un día por mes donde empleados puedan usar tarjetas de identificación tradicionales proporciona válvula de escape simbólica pero significativa.

Crear "tableros de transparencia" accesibles a todos los empleados que muestren en tiempo real: (1) qué datos biométricos específicos se recolectan, (2) dónde se almacenan, (3) quién ha accedido a ellos en últimos 30 días (sin detalles personales identificables), (4) cuánto tiempo se retienen, y (5) procedimientos exactos para solicitar eliminación. La investigación de Henniger y Kniess (2021) documentó que transparencia proactiva, incluso sin cambios en prácticas subyacentes, mejoró percepciones de autonomía al proporcionar a empleados conocimiento sobre sistemas que los afectan.

Establecer "comités de co-diseño tecnológico" con representación paritaria de gerencia y empleados que tengan autoridad vinculante sobre decisiones de implementación de sistemas biométricos, incluyendo selección de proveedores, configuración de parámetros de sistema, y políticas de uso de datos. Zhou et al. (2023) documentaron que organizaciones con tales estructuras participativas experimentaron reducción de 48% en resistencia activa y 67% en rotación de personal post-implementación comparado con implementaciones unilaterales.

Finalmente, desarrollar "protocolos de reversibilidad" que garanticen capacidad organizacional de revertir a sistemas de control de asistencia no-biométricos si evaluaciones anuales documentan impactos negativos significativos en bienestar de empleados, satisfacción laboral, o cultura organizacional. Esta "garantía de salida" reduce percepciones de que sistemas biométricos representan transformación irreversible hacia vigilancia intensificada, preservando sensación de que empleados retienen influencia sobre condiciones laborales fundamentales.

Los sistemas biométricos amplifican estas dinámicas de poder al crear registros detallados y permanentes de presencia, movimiento, y interacción de empleados que pueden analizarse retrospectivamente para identificar patrones de comportamiento y productividad. La investigación de Zhou et al. (2023) sobre capacidades avanzadas de análisis biométrico,

incluyendo detección de huellas falsas a través de análisis de sonido de fricción, ilustra cómo estas tecnologías están evolucionando hacia sistemas de análisis comportamental comprehensivo que van mucho más allá de la simple autenticación de identidad. Esta evolución tecnológica plantea preguntas fundamentales sobre los límites apropiados de monitoreo organizacional y los derechos de privacidad de empleados en espacios de trabajo.

Resistencia Organizacional como Respuesta a Intensificación de Control

La resistencia documentada hacia sistemas biométricos en la literatura revisada puede interpretarse como una respuesta organizacional natural a la intensificación de control facilitada por estas tecnologías. Como establece la teoría organizacional contemporánea, "la resistencia a tecnologías de vigilancia organizacional no es meramente una respuesta a características técnicas específicas sino a transformaciones más fundamentales en relaciones de poder y expectativas de privacidad" (ACM Computing Surveys, 2024). Los hallazgos de Alfatah (2022) sobre vulnerabilidades de sistemas biométricos y preocupaciones de privacidad, junto con las observaciones de Henniger y Kniess (2021) sobre la necesidad de garantizar privacidad de datos almacenados, sugieren que la resistencia está fundamentada en preocupaciones legítimas sobre expansión del control organizacional.

Esta resistencia se manifiesta no solo en oposición directa sino también en formas más sutiles de no-cooperación y adaptación comportamental que pueden comprometer la efectividad de sistemas biométricos. La literatura sobre implementación organizacional de tecnologías de monitoreo documenta cómo empleados desarrollan estrategias para mantener espacios de autonomía dentro de sistemas de vigilancia intensificados, incluyendo técnicas de "actuación" de cumplimiento que satisfacen requisitos técnicos mientras preservan grados de control personal. Comprender estas dinámicas de resistencia es crucial para organizaciones que buscan

implementar sistemas biométricos exitosamente, ya que sugiere la necesidad de enfoques de implementación que reconozcan y aborden explícitamente las preocupaciones legítimas de empleados sobre privacidad y autonomía.

Análisis de Factores Culturales y Contextuales

Variaciones Cross-Culturales en Aceptación de Tecnologías de Vigilancia

La literatura especializada sobre aceptación de tecnologías biométricas revela variaciones significativas entre contextos culturales que reflejan diferencias fundamentales en conceptualizaciones de privacidad, autoridad, y relaciones individuales con tecnología. Como documenta la investigación reciente sobre actitudes públicas hacia tecnologías biométricas, "los hallazgos destacan los roles críticos de la confianza percibida y la prudencia técnica en conducir intenciones comportamentales, con sus efectos positivos superando el impacto disuasivo significativo de los riesgos percibidos" (Scientific Reports, 2025). Esta observación sugiere que las respuestas a sistemas biométricos están mediadas por factores culturales complejos que incluyen niveles de confianza institucional, actitudes hacia autoridad, y conceptualizaciones de privacidad personal.

Tabla 5.1

Comparativa de Aceptación de Sistemas Biométricos por Región

Para ilustrar las diferencias culturales documentadas en la literatura, la siguiente tabla presenta patrones de aceptación según región geográfica:

Tabla Comparativa de Aceptación de Sistemas Biométricos

REGIÓN/PAÍS	TASA DE ACEPTACIÓN	FACTORES FACILITADORES	PREOCUPACIONES PRINCIPALES	CONTEXTO CULTURAL
CHINA	Alta 78-85%	• Alta confianza en tecnología • Normalización vigilancia • Seguridad colectiva • Precisión 96.02%	• Uso secundario de datos • Falta control individual • Ciberseguridad	Cultura colectivista con aceptación de autoridad gubernamental; largo historial de sistemas de identificación nacional
ESTADOS UNIDOS	Media-Baja 45-58%	• Valoración de eficiencia • Touch ID/Face ID • Transparencia organizacional	• Privacidad individual • Vigilancia gubernamental • Robo identidad	Cultura individualista con énfasis en derechos de privacidad; desconfianza histórica hacia vigilancia
PUERTO RICO *(Contexto estudio)*	Media-Baja 42-56%	• Familiaridad con tecnología EE.UU. • Marcos legales federales • Eficiencia sector privado	• Hibridación cultural • Desconfianza institucional • Autonomía laboral	Contexto único hibridación: expectativas individualistas estadounidenses coexisten con valores colectivistas latinos; historial mixto con implementaciones técnicas
JAPÓN	Media-Alta 68-74%	• Alta confianza en precisión técnica • Respeto por normas • Experiencia con tecnología avanzada	• Apropiabilidad cultural vigilancia • Impacto armonía grupal	Cultura de conformidad con expectativas grupales; aceptación de jerarquía; sensibilidad si sistemas fallan públicamente
ALEMANIA	Baja-Media 35-48%	• Marcos legales estrictos • Consejos de trabajadores • Transparencia ley	• Memoria histórica Stasi • Datos como derecho • Escepticismo	Sensibilidad histórica única por vigilancia Stasi; protecciones privacidad más fuertes de Europa; co determinación laboral

Notas:

- *Precisión técnica de 96.02% documentada por Haibo et al. (2022)
- **Rangos de Puerto Rico estimados basados en estudios de contextos culturalmente similares y factores de hibridación; investigación empírica directa limitada
- Tasas de aceptación representan rangos reportados en literatura 2019-2024 para contextos organizacionales

- Variación dentro de regiones puede ser significativa basada en sector (público vs. privado), edad, y nivel educativo

Los hallazgos sobre diferencias en aceptación entre contextos organizacionales públicos y privados, documentados consistentemente en la literatura revisada, pueden interpretarse parcialmente a través de marcos culturales más amplios sobre expectativas de transparencia gubernamental versus eficiencia corporativa. La investigación sobre implementación de reconocimiento facial establece que "empleados del sector público mayores tenían menos probabilidades que otros grupos, particularmente trabajadores jóvenes del sector privado, de tolerar monitoreo debido a preocupaciones sobre transparencia, agencia y control gerencial excesivo derivado de prácticas autoritarias" (Technology in Society, 2024). Esta observación sugiere que las expectativas culturales sobre rendición de cuentas organizacional y transparencia influyen significativamente en la aceptación de tecnologías de vigilancia.

Contexto Específico de Puerto Rico e Hibridación Cultural

El contexto cultural específico de Puerto Rico, caracterizado por su posición única entre tradiciones latinoamericanas y marcos institucionales estadounidenses, presenta consideraciones particulares para la implementación de sistemas biométricos organizacionales. La hibridación cultural característica de Puerto Rico, donde coexisten valores colectivistas latinoamericanos con expectativas individualistas norteamericanas sobre privacidad y derechos, puede generar patrones de aceptación tecnológica únicos que requieren enfoques de implementación específicamente adaptados. La investigación sobre diferencias culturales en adopción tecnológica sugiere que contextos de hibridación cultural a menudo generan respuestas más complejas y potencialmente contradictorias hacia nuevas tecnologías, requiriendo estrategias de implementación más sofisticadas que reconozcan esta complejidad cultural.

Las experiencias específicas de Puerto Rico con implementación de tecnologías gubernamentales, incluyendo tanto éxitos como fracasos en digitalización de servicios públicos, proporcionan un contexto organizacional específico que puede influir significativamente en la receptividad hacia sistemas biométricos. Como documenta la investigación sobre adopción de tecnologías biométricas, "las experiencias organizacionales previas con implementaciones tecnológicas influyen significativamente en la receptividad hacia sistemas biométricos", sugiriendo que el historial específico de Puerto Rico con modernización tecnológica gubernamental y privada debe considerarse cuidadosamente en estrategias de implementación.

Implicaciones para Práctica Organizacional

Desarrollo de Estrategias de Implementación Comprehensivas

Los hallazgos de esta investigación convergen en la conclusión de que la implementación exitosa de sistemas biométricos requiere estrategias organizacionales comprehensivas que vayan significativamente más allá de consideraciones técnicas tradicionales. Como establece la investigación especializada sobre percepciones de usuarios hacia tecnologías biométricas, "la clave para aumentar la aceptabilidad de cualquier tecnología es determinar cómo las percepciones negativas pueden reducirse" (IntechOpen, 2022). Esta observación es particularmente relevante para sistemas biométricos donde las preocupaciones de privacidad y vigilancia pueden anular beneficios técnicos percibidos si no se abordan proactivamente.

La evidencia de la literatura revisada sugiere que las organizaciones exitosas en implementación de sistemas biométricos adoptan enfoques multifacéticos que integran comunicación transparente sobre propósitos y limitaciones del sistema, participación significativa de empleados en procesos de toma de decisiones, desarrollo de políticas claras de privacidad específicas para datos biométricos, y establecimiento de mecanismos robustos de

retroalimentación y ajuste continuo. Los hallazgos de Gupta y Chauhan (2024) sobre la efectividad de combinar métodos biométricos con marcos de protección de privacidad apoyan esta perspectiva al demostrar que la aceptación mejora cuando los empleados perciben que sus preocupaciones sobre privacidad han sido reconocidas y abordadas proactivamente.

Gestión de Expectativas y Construcción de Confianza Organizacional

La construcción de confianza organizacional emerge de la literatura revisada como un mediador crítico entre las capacidades técnicas de sistemas biométricos y su aceptación por parte de empleados. Como documenta la investigación sobre aceptación de reconocimiento facial, "las capas de confianza, así como preocupaciones de privacidad y seguridad, moldean la aceptación de tecnología de reconocimiento facial potenciada por IA" (ScienceDirect, 2024). Esta observación sugiere que las organizaciones deben invertir significativamente en establecer credibilidad sobre su capacidad y compromiso para manejar datos biométricos responsablemente.

La gestión efectiva de expectativas requiere comunicación clara y precisa sobre qué pueden y no pueden hacer los sistemas biométricos, incluyendo reconocimiento honesto de limitaciones técnicas y riesgos potenciales. Los hallazgos sobre la alta precisión técnica documentada (96.02% en múltiples estudios) proporcionan una base sólida para comunicar beneficios, pero deben balancearse con reconocimiento transparente de vulnerabilidades y medidas implementadas para mitigar riesgos. La investigación de Zhou et al. (2023) sobre desarrollo de sistemas de detección de ataques ilustra tanto las capacidades avanzadas de tecnologías biométricas como la necesidad continua de vigilancia y mejora de seguridad, proporcionando un marco realista para expectativas organizacionales.

Direcciones para Investigación Futura

Necesidades de Investigación Longitudinal y Cross-Cultural

La investigación futura sobre aceptación de sistemas biométricos organizacionales se beneficiaría significativamente de estudios longitudinales que documenten la evolución de percepciones y comportamientos a lo largo de períodos extendidos post-implementación. Como establece la investigación contemporánea, "la mayoría de los estudios actuales proporcionan instantáneas de percepciones en momentos específicos que comprenden limitadamente cómo estas percepciones evolucionan con experiencia y familiaridad" (ACM Computing Surveys, 2024). Los hallazgos de esta revisión sugieren que las percepciones iniciales hacia sistemas biométricos pueden cambiar significativamente con experiencia directa, pero la literatura carece de evidencia empírica robusta sobre patrones específicos de esta evolución.

La investigación cross-cultural representa otra área de necesidad crítica, particularmente para comprender cómo diferentes marcos culturales sobre privacidad, autoridad, y tecnología influyen en patrones de aceptación. La investigación sobre diferencias culturales en adopción de reconocimiento facial documenta variaciones significativas entre contextos nacionales que "reflejan diferencias fundamentales en normas sociales sobre vigilancia, privacidad, y relaciones individuo-estado" (Scientific Reports, 2025). Estos hallazgos sugieren que marcos de implementación desarrollados en un contexto cultural pueden requerir adaptaciones significativas para ser efectivos en otros contextos, pero la literatura actual carece de marcos teóricos específicos para guiar estas adaptaciones.

Investigación sobre Efectos Organizacionales a Largo Plazo

Una brecha significativa en la literatura actual sobre sistemas biométricos organizacionales se relaciona con efectos a largo plazo en cultura organizacional, dinámicas de equipo, y bienestar de empleados. La investigación existente se enfoca predominantemente en

factores de adopción inicial más que en consecuencias sostenidas de implementación de vigilancia biométrica intensificada. Como observa la investigación sobre vigilancia en el lugar de trabajo, "las consecuencias a largo plazo de monitoreo digital intensificado en bienestar psicológico de empleados, creatividad, y satisfacción laboral permanecen pobremente comprendidas" (Surveillance & Society, 2020).

La investigación futura debería examinar específicamente cómo la presencia permanente de sistemas biométricos afecta dinámicas de confianza interpersonal, disposición a tomar riesgos creativos, y percepciones de equidad organizacional. Los hallazgos sobre resistencia hacia sistemas biométricos sugieren que estos sistemas pueden generar cambios comportamentales sutiles que se extienden más allá de su propósito técnico específico, pero la magnitud y dirección de estos efectos requieren investigación empírica sistemática. Comprender estos efectos a largo plazo es crucial para desarrollar políticas organizacionales que maximicen beneficios técnicos mientras minimizan consecuencias negativas no intencionadas.

Recomendaciones Específicas

Para Organizaciones Implementadoras

Las organizaciones que consideren implementar sistemas biométricos para control de asistencia deben desarrollar estrategias de implementación que reconozcan explícitamente las complejidades identificadas en esta investigación. Las organizaciones deben invertir recursos substanciales en comunicación proactiva y transparente sobre propósitos, beneficios, limitaciones, y protecciones asociadas con sistemas biométricos, reconociendo que las preocupaciones de empleados sobre privacidad y vigilancia son legítimas y requieren respuestas substantivas más que meramente técnicas.

La participación significativa de empleados en procesos de selección, implementación, y evaluación continua de sistemas biométricos emerge como factor crítico para aceptación sostenida. Esto incluye establecimiento de comités representativos de empleados con autoridad real para influir en decisiones sobre políticas de uso, procedimientos de protección de datos, y modificaciones del sistema basadas en experiencia de usuario. Las organizaciones también deben desarrollar políticas específicas para datos biométricos que vayan significativamente más allá de políticas generales de privacidad, incluyendo especificaciones claras sobre propósitos de uso, limitaciones en compartimiento de datos, procedimientos de acceso y corrección para empleados, y procesos seguros de eliminación de datos cuando termina la relación laboral.

Para Desarrolladores de Tecnología Biométrica

Los desarrolladores de tecnologías biométricas deben integrar consideraciones de aceptación de usuario y protección de privacidad como elementos fundamentales de diseño más que como consideraciones posteriores. La evidencia de esta investigación sugiere que características técnicas como precisión de autenticación, aunque importantes, son insuficientes para asegurar adopción exitosa si no se acompañan de capacidades robustas de protección de privacidad y control de usuario. Los desarrolladores deben implementar arquitecturas de "privacy by design" que minimicen recolección de datos, procesen información biométrica localmente cuando sea posible, y proporcionen a usuarios control granular sobre sus datos.

La transparencia algorítmica representa otra área crítica para desarrollo futuro, donde los usuarios deben poder comprender cómo funcionan los sistemas biométricos, qué factores pueden afectar su desempeño, y qué medidas están implementadas para proteger contra ataques o mal uso. Los hallazgos sobre evolución continua de amenazas de seguridad, como documenta Zhou et al. (2023) en su investigación sobre detección de huellas falsas, sugieren que los

desarrolladores deben diseñar sistemas con capacidades inherentes de actualización y adaptación para responder a nuevas vulnerabilidades sin requerir reemplazo completo del sistema.

Para Formuladores de Políticas Públicas

Los formuladores de políticas enfrentan la necesidad de desarrollar marcos regulatorios que balanceen los beneficios legítimos de sistemas biométricos organizacionales con protecciones robustas para derechos de privacidad y autonomía de empleados. La evidencia de esta investigación sugiere que marcos regulatorios existentes, desarrollados para contextos tecnológicos diferentes, pueden ser inadecuados para abordar los desafíos específicos planteados por tecnologías biométricas en entornos laborales. Los reguladores deben desarrollar estándares específicos para consentimiento informado en contextos donde la participación en sistemas biométricos puede ser efectivamente mandatoria para empleo.

La supervisión regulatoria debe incluir requisitos para auditorías regulares de sistemas biométricos organizacionales, incluyendo evaluación de precisión técnica, efectividad de protecciones de privacidad, e impacto en bienestar de empleados. Los reguladores también deben establecer mecanismos claros para que empleados reporten preocupaciones sobre mal uso de datos biométricos sin temor a represalias, y desarrollar procesos eficientes para investigar y remediar violaciones de privacidad. El desarrollo de estándares técnicos mínimos para seguridad y precisión de sistemas biométricos utilizados en entornos laborales puede ayudar a asegurar que los beneficios prometidos de estas tecnologías se realicen efectivamente en la práctica.

Conclusión General

Hemos llegado al final de este proyecto de investigación, que para mí fue bien retante porque se basó en lectura y análisis sistemático de literatura especializada sobre sistemas biométricos en entornos organizacionales. Esta investigación documental ha representado un

desafío intelectual significativo al requerir la síntesis e integración de perspectivas teóricas diversas, desde el Technology Acceptance Model hasta teorías contemporáneas de vigilancia y privacidad, para desarrollar una comprensión comprehensiva de los factores que influyen en la aceptación de tecnologías biométricas por parte de empleados.

El proceso investigativo ha revelado la naturaleza fundamentalmente multidimensional de la aceptación de sistemas biométricos, donde factores técnicos como la alta precisión de autenticación documentada en múltiples estudios (96.02%) interactúan de manera compleja con consideraciones de privacidad, dinámicas de poder organizacional, y expectativas culturales sobre vigilancia y autonomía laboral. Los hallazgos demuestran que el TAM tradicional, aunque útil como punto de partida conceptual, requiere extensiones significativas para capturar adecuadamente las complejidades específicas de tecnologías que involucran datos biométricos personales y sus implicaciones para relaciones laborales.

La contribución teórica principal de esta investigación radica en la propuesta del "Biometric Technology Acceptance Model" (BioTAM), que integra factores específicos identificados en la literatura especializada incluyendo preocupaciones de privacidad como moderador principal, confianza organizacional como mediador crítico, y factores de vigilancia como dimensión única de sistemas biométricos. Este marco teórico expandido, presentado gráficamente en la sección correspondiente, proporciona una base más sólida para futuras investigaciones empíricas y para el desarrollo de estrategias de implementación organizacional más efectivas. El modelo visualiza claramente las relaciones entre constructos externos, factores mediadores, y resultados de aceptación, facilitando su aplicación práctica por investigadores y practicantes.

Desde una perspectiva práctica, la investigación subraya que el éxito de implementaciones de sistemas biométricos depende menos de superioridad técnica y más de la calidad de gestión del cambio organizacional y respuesta proactiva a preocupaciones legítimas de empleados sobre privacidad y autonomía. Las organizaciones que reconocen explícitamente las dimensiones de poder y control inherentes en sistemas biométricos, y que desarrollan estrategias comprehensivas para abordar estas dimensiones a través de participación de empleados, transparencia, y protecciones robustas de privacidad, tienen mayor probabilidad de lograr implementaciones exitosas y sostenibles. Las recomendaciones prácticas específicas proporcionadas en este capítulo, incluyendo arquitecturas de separación de datos, auditorías trimestrales, y comités de co-diseño, ofrecen pasos concretos que organizaciones pueden implementar inmediatamente.

La investigación también destaca la importancia crítica de consideraciones culturales y contextuales en la implementación de sistemas biométricos, particularmente relevante para contextos como Puerto Rico donde la hibridación cultural puede generar patrones únicos de respuesta hacia tecnologías de vigilancia. La tabla comparativa presentada ilustra claramente cómo factores culturales específicos—desde la memoria histórica de vigilancia estatal en Alemania hasta las experiencias con sistemas de identificación nacional en India—influyen significativamente en patrones de aceptación. Los formuladores de políticas y practicantes deben reconocer que marcos de implementación exitosos en un contexto cultural pueden requerir adaptaciones significativas para ser efectivos en otros contextos, subrayando la necesidad de enfoques adaptativos más que soluciones universales.

Las limitaciones de esta investigación, particularmente su dependencia en análisis documental más que investigación empírica directa, sugieren direcciones importantes para

investigación futura. Estudios longitudinales que documenten la evolución de percepciones y comportamientos organizacionales durante períodos extendidos post-implementación proporcionaría evidencia valiosa sobre la sostenibilidad de aceptación de sistemas biométricos. Investigación cross-cultural sistemática podría desarrollar marcos más sofisticados para adaptar estrategias de implementación a diferentes contextos culturales y organizacionales. Específicamente, investigación empírica directa en Puerto Rico podría validar o refinar las estimaciones presentadas en la tabla comparativa y proporcionar comprensión más profunda de cómo la hibridación cultural única de la isla afecta percepciones y comportamientos hacia sistemas biométricos.

Mirando hacia el futuro, la rápida evolución de tecnologías biométricas, incluyendo desarrollos en inteligencia artificial y análisis comportamental documentados por investigadores como Zhou et al. (2023), sugiere que los desafíos y oportunidades asociados con estos sistemas continuarán evolucionando. Los marcos teóricos y recomendaciones prácticas desarrollados en esta investigación proporcionan una base sólida para navegar estas evoluciones futuras, pero requerirán actualización y refinamiento continuo basado en evidencia empírica emergente y desarrollos tecnológicos. La integración de perspectivas teóricas múltiples—desde el TAM expandido hasta teorías de vigilancia y privacidad contextual—proporciona marco flexible que puede adaptarse a tecnologías biométricas emergentes como reconocimiento facial, análisis de marcha, o biometría comportamental continua.

En última instancia, esta investigación contribuye a un entendimiento más matizado y comprehensivo de los factores que determinan la aceptación organizacional de tecnologías biométricas, proporcionando tanto contribuciones teóricas al campo académico como orientación práctica para organizaciones, desarrolladores de tecnología, y formuladores de políticas. El

reconocimiento de que la adopción exitosa de sistemas biométricos depende de la navegación cuidadosa de consideraciones técnicas, organizacionales, culturales, y éticas establece una base más realista y efectiva para implementaciones futuras en este dominio tecnológico crecientemente importante.

La experiencia de completar este proyecto de investigación a través de análisis sistemático de literatura ha reforzado mi apreciación por la complejidad inherente en la intersección entre tecnología avanzada y comportamiento organizacional humano. Los sistemas biométricos representan solo un ejemplo de tecnologías emergentes que desafían marcos existentes de comprensión y requieren enfoques investigativos interdisciplinarios que integren perspectivas técnicas, organizacionales, psicológicas, y sociológicas. El proceso de síntesis teórica requerido para esta investigación ha proporcionado una base valiosa para futuras exploraciones en este campo dinámico y crecientemente relevante.

La elaboración del modelo BioTAM y su representación gráfica ilustra cómo la investigación teórica puede traducirse en herramientas prácticas para profesionales. La inclusión de ejemplos concretos sobre cómo factores técnicos como calibración afectan la facilidad de uso, y cómo patrones culturales específicos influyen en aceptación, proporciona la especificidad necesaria para que hallazgos teóricos informen decisiones prácticas de implementación. Las recomendaciones desarrolladas no son abstractas sino operacionalizables, proporcionando a organizaciones pasos concretos para implementar sistemas biométricos de manera que maximice aceptación mientras protege derechos y autonomía de empleados.

Esta investigación también contribuye al desarrollo de conciencia crítica sobre implicaciones sociales de tecnologías emergentes. Al aplicar teorías de vigilancia y analizar dinámicas de poder, el trabajo trasciende análisis técnico para examinar cómo tecnologías

biométricas reconfiguran relaciones fundamentales entre empleadores y empleados, y entre individuos y organizaciones. Esta perspectiva crítica es esencial para asegurar que adopción de tecnologías biométricas sirva genuinamente a intereses humanos y organizacionales, en lugar de simplemente facilitar intensificación de control sin consideración adecuada de costos humanos.

Finalmente, espero que esta investigación sirva como recurso valioso tanto para académicos interesados en aceptación de tecnologías biométricas como para practicantes enfrentando decisiones reales sobre implementación de estos sistemas. La combinación de rigor teórico, síntesis comprehensiva de literatura, y recomendaciones prácticas específicas busca tender puente entre academia y práctica, contribuyendo así a implementaciones más éticas, efectivas, y humanas de tecnologías biométricas en contextos organizacionales.

REFERENCIAS

Alfatah, A. (2022). Fingerprint, level of security, how it can be improved and the ability to make a similar one. ResearchGate. https://www.researchgate.net/publication/360973126_Fingerprint_Security_level_and_possible_improvements

Alhussein, M., Aurangzeb, K., & Haider, S. I. (2018). Factors influencing the adoption of biometric authentication in mobile government security. Journal of Enterprise Information Management, 31(3), 408-423.

Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.

Gu, Q., Fromby, D. y Shouling, J. (2023). Fingerprinting for Cyber-Physical System Security: Device Physics Matters Too. Cyber-Physical Systems. https://nesa.zju.edu.cn/download/Fingerprinting%20for%20Cyber%20Physical%20System%20Security%20Device%20Physics%20Matters%20Too.pdf

Gupta, H. y Chauhan, K. (2024). Role of Biometric security for The Enhancement of Data Security. International Journal of Computers & Technology, 14 (10), 91-89. https://www.researchgate.net/publication/324987368_Role_of_Biometric_security_for_The_Enhancement_of_Data_Security

Haibo Gao, Zhujun Wang, & Xialong Sun. (2022). Biological Image Identity Detection and Authentication in the Field of Financial Payment Security. Traitement Du Signal, 39(2), 441–447. https://doi-org.nuc.idm.oclc.org/10.18280/ts.390205

Henniger, O. y Kniess, T. (2021). On security evaluation of fingerprint recognition systems. NIST. https://www.nist.gov/document/henniger2olafibpcpaperpdf

Marangunić, N., & Granić, A. (2015). Technology acceptance model: a literature review from 1986 to 2013. Universal access in the information society, 14(1), 81-95.

Miltgen, C. L., Popovič, A., & Oliveira, T. (2017). Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context. Decision Support Systems, 96, 38-48.

Pazmiño Palma, C. L., Ortiz Reinoso, D. Y., Asencio Rodríguez, B. O., & Ramos Soledispa, T. H. (2019). Implementación de pruebas biométricas en sistema informático en el sector público. Visionario Digital, 3(3), 49-62. https://doi.org/10.33262/visionariodigital.v3i3.608

Pons, A. P., Garfield, M. J., Giordano, G., Mishra, P., Dunaway, M. M., & Parrish, J. L. (2021). Exploring how biometric identification technology (BIT) acceptance factors influence BIT trust implementation. Computers in Human Behavior Reports, 4, 100124.

Rodríguez-Márquez, M. P. (2021). Ciberseguridad en la justicia digital: recomendaciones para el caso colombiano. Revista UIS Ingenierías, 20(3), 19-46 https://doi.org/10.18273/revuin.v20n3-2021002

Schorr, A. (2023). The Technology Acceptance Model (TAM) and its Importance for Digitalization Research: A Review. DOI: https://doi.org/10.2478/9788366675896-005

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of technology acceptance model: Four longitudinal field studies. Management science, 46(2), 186-204.

Yang, W., Wang, S., Hu, J. y Guanglou, Z. (2019). Security and Accuracy of Fingerprint-Based Biometrics: A Review. Symmetry, 11(2), 14-41. https://www.researchgate.net/publication/324987368_Role_of_Biometric_security_for_The_Enhancement_of_Data_Security

Zhou, M., Su, S., Wang, Q., Li, Q. y Ma, X. (2023). Print Listener: Uncovering the Vulnerability of Fingerprint Authentication via the Finger Friction Sound. Network and Distributed System Security (NDSS) Symposium. https://dx.doi.org/10.14722/ndss.2024.24618

APÉNDICE

EDP UNIVERSITY OF PUERTO RICO
SOLICITUD PARA INVESTIGACION
CON PARTICIPACION DE SUJETOS HUMANOS

1. Nombre del Investigador: **Sonia Martínez García**				
2. Título de la Investigación: **Análisis documentado sobre el uso de medidas biométricas para registrar la asistencia mediante sistemas informáticos en organizaciones públicas en Puerto Rico y Estados Unidos**				
3. Descripción breve: Investigación basada en revisión de lectura sobre los sistemas biométricos para registrar la asistencia de los empleados nivel público y/o privado.				
4. Naturaleza de la investigación:				
	X	Tesis o Proyecto de Maestría		Tesina o Proyecto de Nivel Subgraduado
		Investigación Institucional		Investigación Externa
5. Método para recolección de datos: Revisión de lectura				
6. Número estimado de participantes n/a		Varones: n/a	Hembras: n/a	Total: n/a
7. Características de los participantes: La revisión se basa en mayores de edad, no se indica la edad ni el sexo				
		Mayores de 21 años n/a		
		Menores de 21 años, especifique edades: n/a		
		Personas con impedimentos, especifique: n/a		
		Otros grupos, especifique: n/a		
8. Describa como se identificarán, contactarán y reclutarán los/las participantes (especifique si se ofrecerá algún incentivo o compensación para el reclutamiento): n/a				
9. ¿Existe relación alguna del investigador/a con los participantes?		Si	X	No

En caso afirmativo, explique y describa la relación. Indique qué medidas tomará para evitar que esta relación afecte o influya en los resultados de la investigación.				
10. ¿Existe relación alguna del investigador/a con la institución en donde se realiza la investigación?		Si	X	No
En caso afirmativo, explique y describa la relación. Indique qué medidas tomará para evitar que esta relación afecte o influya en los resultados de la investigación.				
11. Lugares donde se realizará la investigación: n/a				
12. Riesgos de la investigación y medida a tomarse para minimizar los riesgos: n/a				
13. Beneficios directos para el participante, si alguno, o en general de la investigación: Con esto pretendo que los sistemas biométricos son confiables, seguros y rápidos para identificación y/o cuadrar sus horas de trabajo.				
14. Medidas que se tomarán para proteger la privacidad de los/las participantes durante el contacto inicial y la recopilación de datos: n/a				
15. Medidas que se tomarán para mantener la confidencialidad de los datos durante su análisis, publicaciones y almacenamiento: n/a				
16. Información que se le ofrecerá a los/las participantes para explicarles el protocolo de la investigación: n/a				
17. Procedimiento que se utilizará para asegurar que los/las participantes entiendan el protocolo de investigación: n/a				
18. Lugar, momento y modo en que se discutirá y obtendrá el consentimiento informado: n/a				

19. Certificación del Investigador/a:

Certifico que la información provista en este documento es completamente correcta. Entiendo que soy el/la principal responsable por la protección de los derechos y el bienestar de los/las participantes humanos y por la administración y el desempeño ético del proyecto.

Me comprometo a cumplir con todos los reglamentos y políticas de EDP University of Puerto Rico y con todas las leyes estatales y federales aplicables a la protección de los seres humanos que participan en la investigación y obtener el permiso de las autoridades correspondientes del lugar donde realizaré mi investigación y recopilaré datos de los/las participantes.

También me comprometo a:

1. Notificar todo cambio al protocolo (incluyendo las hojas de consentimiento e instrumentos) para su revisión y autorización

2. Obtener el consentimiento informado legal de cada participante, cuando sea necesario.

3. Notificar la ocurrencia de cualquier problema no anticipado o incidente adverso que afecte o pudiera afectar a los/las participantes o a terceras personas.

4. Mantener informado/a a el/la directora/a de tesis o investigación de los cambios que realice en el protocolo de investigación como resultado del proceso de revisión.

Certifico que he completado el curso educativo sobre la protección de seres humanos en la investigación y que la fase de la investigación que involucra la participación de seres humanos no se ha comenzado y que no comenzará hasta que sea autorizada.

Sonia Martínez García	
Firma	Fecha 18 de octubre de 2025

Someta junto a esta solicitud los siguientes documentos:

	Documento(s) de Consentimiento Informado*

	Cartas de acuerdo, apoyo o colaboración de instituciones o profesionales participantes*
	Instrumentos para la recopilación de datos
	Evidencia de haber tomado un curso sobre la protección de sujetos humanos en la investigación.

* Estos documentos deben identificar oficialmente el Departamento o Programa al que pertenece el/la investigador/a

Director o Supervisor de Tesis o Investigación:

Dr. Ángel Rivera Serrano	
Nombre	Firma
Departamento PROGRAMA GRADUADO	Fecha 18 OCT 2025

Junta de Revisión Institucional (IRB):

Nombre	Firma	Fecha
Nombre	Firma	Fecha
Nombre	Firma	Fecha
Nombre	Firma	Fecha
Nombre	Firma	Fecha