



Herramientas digitales de control de identidad para la prevención delictiva en Lima Perú

Digital identity control tools for crime prevention in Lima, Peru.

Recepción del artículo: 15/12/2023 | Aceptación para publicación: 04/03/2025 | Publicación: 17/03/2025



Carlos Artemio Altamirano Quintana
09455675@escpograpnp.com



Jorge Luis Peché del Carpio
10014073@escpograpnp.com



Nelson Weberbauer Salvatierra-Lavado
08275068@escpograpnp.com

Escuela de Posgrado de la Policía Nacional del Perú

Resumen

La presente investigación tuvo como objetivo analizar la implementación de herramientas digitales para el control de identidad en la prevención del delito por el Escuadrón Verde en Lima durante el año 2024. El estudio adoptó un enfoque mixto con diseño transformativo concurrente y alcance descriptivo. La muestra estuvo conformada por 357 oficiales del Escuadrón Verde de Lima para el componente cuantitativo, y 30 oficiales para el cualitativo, seleccionados mediante muestreo no probabilístico por conveniencia. Se emplearon como técnicas de recolección de datos la entrevista semiestructurada, la encuesta y el análisis documental, utilizando como instrumentos una guía de entrevista, un cuestionario de escala valorativa y fichas de análisis documental. Los resultados evidenciaron una percepción predominantemente positiva sobre la eficacia de las herramientas digitales, con más del 80% de los encuestados respaldando su utilidad en la prevención del delito. Los sistemas biométricos integrados y las bases de datos interconectadas mostraron particular efectividad, aunque se identifican desafíos significativos en términos de privacidad y protección de datos. Se concluyó que la implementación de estas herramientas ha transformado significativamente las estrategias de control de identidad del Escuadrón Verde, mejorando su capacidad para prevenir y combatir el delito, si bien requiere un equilibrio cuidadoso entre la eficacia operativa y la protección de derechos individuales.

Palabras clave: identidad, tecnología, escuadrón verde, control, biometría.

Abstract

The present research aimed to analyze the implementation of digital tools for identity control in crime prevention by the Green Squad in Lima during the year 2024. The study adopted a mixed approach with a concurrent transformative design and a descriptive scope. The sample consisted of 357 officers from the Lima Green Squad for the quantitative component, and 30 officers for the qualitative component, selected through non-probabilistic convenience sampling. The semi-structured interview, survey, and documentary analysis techniques were used as data collection techniques, using an interview guide, a rating scale questionnaire, and documentary analysis sheets as instruments. The results showed a predominantly positive perception of the effectiveness of digital tools, with more than 80% of respondents supporting their usefulness in crime prevention. Integrated biometric systems and interconnected databases showed particular effectiveness, although significant challenges were identified in terms of privacy and data protection. It was concluded that the implementation of these tools has significantly transformed the Green Squad's identity control strategies, improving its ability to prevent and combat crime, although it requires a careful balance between operational effectiveness and the protection of individual rights.

Keywords: identity, technology, green squad, control, biometrics.

Para citar:

Altamirano, C., et al. (2025). Herramientas digitales de control de identidad para la prevención delictiva en Lima Perú. *ESCPOGRA PNP*, 4(2), 182-192. <https://doi.org/10.59956/escpograpnpv4n2.12>





Introducción

La evolución tecnológica ha transformado los paradigmas de seguridad pública, particularmente en lo referente al control de identidad y la prevención del delito. En este contexto, la implementación de herramientas digitales se ha convertido en un elemento fundamental para las fuerzas del orden en su lucha contra la criminalidad. Las instituciones policiales a nivel global enfrentan el desafío de adaptarse a un entorno donde la tecnología juega un papel cada vez más crucial en la identificación y seguimiento de actividades delictivas.

El control de identidad, como procedimiento fundamental en la policía laboral, ha experimentado una notable evolución gracias a la incorporación de tecnologías digitales. Este proceso, que normalmente se fundamentaba en la verificación manual de documentos, ahora integra sistemas biométricos avanzados, bases de datos interconectadas y técnicas de rastreo digital. Como señalan García et al. (2023), estas capacidades han revolucionado la forma en que las agencias de seguridad abordan la prevención del delito, transitando de un enfoque reactivo a uno proactivo y predictivo.

En el contexto peruano, la Defensoría del Pueblo (2019) ha documentado que aproximadamente el 50% de las intervenciones policiales por control de identidad presentan irregularidades, incluyendo la solicitud de identificación sin motivos fundados o la retención prolongada de individuos sin justificación legal. Esta situación ha generado preocupación respecto a la necesidad de modernizar y optimizar los procedimientos de control de identidad mediante el uso de tecnologías que permitan una mayor precisión y eficiencia.

Las estadísticas revelan la magnitud del desafío: durante 2022, se realizaron 135.938 operativos de control de identidad a nivel nacional, representando el 19,60% del total de operativos policiales. En estos procedimientos se intervino a más de 14 millones de personas, de las cuales 139,388 fueron detenidas (Policía Nacional del Perú, 2022). Estos números enfatizan la importancia de contar con herramientas tecnológicas que permitan realizar estos controles de manera más eficiente y precisa.

Las herramientas digitales para el control de identidad representan un conjunto integrado de tecnologías diseñadas para optimizar la identificación y verificación de individuos en el contexto de la seguridad pública. De acuerdo con Gutiérrez et al. (2023), estas herramientas proporcionan una mayor precisión y rapidez en la identificación de personas sospechosas, contribuyendo a la prevención y persecución de delitos.

La implementación de estas tecnologías requiere un enfoque integral que considere tanto los aspectos técnicos como los éticos y legales. Torres et al. (2023) enfatizan que la efectividad de estas herramientas depende no solo de su sofisticación tecnológica, sino también de la existencia de un marco legal y ético sólido que regula su uso. Este marco debe equilibrar la necesidad de seguridad con la protección de los derechos individuales y la privacidad.





Las herramientas digitales han demostrado particular utilidad en la colaboración internacional para combatir el crimen transnacional. Según datos de INTERPOL (2023), la adopción de estándares comunes en estas tecnologías ha resultado en un incremento del 45% en la detección de criminales internacionales en puntos fronterizos de países participantes.

Los sistemas biométricos integrados constituyen un componente fundamental en la modernización del control de identidad policial. Según Aguinaga (2023), estos sistemas aprovechan características físicas únicas e inherentemente personales, como huellas dactilares, rasgos faciales, patrones de iris o características vocales, para verificar la identidad de manera precisa y confiable. La integración de múltiples modalidades biométricas ha significado un avance significativo en la precisión de la identificación. Rodríguez et al. (2022) han demostrado que la combinación de diferentes modalidades biométricas, como el reconocimiento facial y la huella dactilar, puede alcanzar tasas de precisión superiores al 99,9%, superando significativamente los métodos tradicionales. Esta alta precisión resulta crucial en contextos de seguridad pública donde la correcta identificación es esencial.

Un aspecto particularmente relevante de los sistemas biométricos integrados es su capacidad de adaptación a diferentes niveles de seguridad. Pérez y Martínez (2024) señalan que estos sistemas pueden configurarse para proporcionar diferentes niveles de verificación según el contexto, desde controles básicos hasta verificaciones multinivel para situaciones de alta seguridad. Esta flexibilidad permite optimizar los recursos mientras se mantienen los estándares de seguridad necesarios.

La incorporación de inteligencia artificial y aprendizaje automático ha potenciado significativamente las capacidades de estos sistemas. Torres y Vega (2023) han documentado que los sistemas biométricos con IA incorporados pueden detectar intentos de suplantación de identidad con una eficacia 30% superior a los sistemas convencionales. Esta mejora en la detección de fraudes resulta crucial para la prevención del delito.

Las bases de datos interconectadas representan otro pilar en la modernización del control de identidad. Vivas (2022) las define como sistemas que permiten la vinculación e intercambio de información entre diferentes repositorios de datos, facilitando la centralización y coordinación de información crucial para la identificación de individuos y la prevención del delito. Su efectividad radica en su capacidad para proporcionar acceso inmediato a información crítica. Según González y Martínez (2023), la implementación de bases de datos interconectadas en sistemas de control fronterizo ha resultado en un incremento del 50% en la detección de documentos fraudulentos y personas buscadas por la justicia.

Sin embargo, la implementación de estas tecnologías presenta desafíos. Leiva (2020) identifica como principales retos la interoperabilidad entre sistemas, la calidad y consistencia de los datos, y la necesidad de implementar medidas robustas de seguridad. Páez (2023) enfatiza la importancia de establecer mecanismos adecuados para salvar la confidencialidad y





respetar los derechos individuales, equilibrando la necesidad de acceso a la información con la protección de datos personales.

El rastreo digital surge como una herramienta fundamental en el arsenal tecnológico para el control de identidad y la prevención del delito. Como señala Villaplana (2021), esta tecnología permite el seguimiento y monitoreo sistemático de actividades y comunicaciones digitales, facilitando la detección temprana y prevención de comportamientos delictivos. La capacidad de analizar patrones de comportamiento en tiempo real ha transformado significativamente las capacidades preventivas de las fuerzas del orden.

Rodríguez y Gómez (2023) han documentado que la implementación de técnicas avanzadas de rastreo digital ha conducido a un incremento del 40% en la detección de actividades delictivas en línea relacionadas con el fraude de identidad. Esta mejora en la capacidad de detección se atribuye a la combinación de tecnologías de análisis de datos y algoritmos de reconocimiento de patrones.

La integración de inteligencia artificial en las técnicas de rastreo digital ha amplificado significativamente su eficacia. López y Sánchez (2024) demuestran que los sistemas de rastreo basados en IA pueden detectar intentos de suplantación de identidad con una precisión 60% superior a los métodos tradicionales. Un aspecto crucial es su capacidad para triangular información de múltiples fuentes. Según INTERPOL (2024), la integración de datos diversos, incluyendo registros de redes sociales, transacciones financieras y metadatos de comunicaciones, puede aumentar la precisión en la identificación de actividades delictivas en línea hasta en un 70%. Esta capacidad de análisis multifuente resulta fundamental para la construcción de perfiles de riesgo precisos.

La implementación de herramientas digitales para el control de identidad ha sido objeto de diversos estudios que demuestran su impacto en la prevención del delito. Llerena y Zelada (2022) identifican deficiencias en la comunicación entre comisarías y limitaciones en el acceso a información policial, sugiriendo la necesidad de implementar soluciones tecnológicas integradas para mejorar la eficacia operativa. En el ámbito internacional, Blanco (2022) analiza las diferentes figuras procesales de identificación, destacando la importancia de contar con marcos normativos adecuados que regulan el uso de tecnologías de control de identidad. De igual forma, Duce y Lillo (2020) aportan una perspectiva empírica sobre el uso de controles de identidad, evidenciando un incremento significativo en su aplicación tras reformas legislativas, aunque sin una mejora proporcional en las tasas de eficacia. Sus hallazgos sugieren la necesidad de complementar los procedimientos tradicionales con herramientas tecnológicas que mejoren la precisión y eficiencia.

La transformación digital del control de identidad representa un cambio paradigmático en la prevención del delito. Como señala Vargas y Mendoza (2022), la efectividad de estos sistemas depende en gran medida de la infraestructura tecnológica disponible y el acceso a dispositivos digitales, factores que pueden variar entre diferentes regiones y contextos





socioeconómicos. Los desafíos en la implementación de estas tecnologías son múltiples y complejos. Fernández y Ortiz (2024) enfatizan la importancia de la inversión continua en investigación y desarrollo para mantener la efectividad de las herramientas de control de identidad frente a amenazas emergentes.

La formación y capacitación del personal se plantea como un factor crítico para el éxito en la implementación de estas herramientas. López y Sánchez (2023) demuestran que los programas de capacitación intensiva pueden incrementar la eficiencia en el uso de estas tecnologías hasta en un 60%, mejorando significativamente la tasa de detección de documentos fraudulentos y actividades sospechosas.

Resultados

Los hallazgos de la investigación revelan patrones en la implementación y efectividad de las herramientas digitales para el control de identidad en el Escuadrón Verde de Lima. El análisis de las entrevistas y encuestas realizadas proporciona una visión integral de la situación actual.

El análisis de los datos cuantitativos revela una percepción altamente positiva sobre la eficacia de los sistemas biométricos integrados. Un 47.9% de los encuestados expresó su total acuerdo sobre la efectividad de estas herramientas en la verificación de identidad para la prevención del delito, mientras que un 40.6% mostró un acuerdo considerable. Esta evaluación positiva se refuerza con la percepción sobre la precisión de las modalidades biométricas específicas, donde un 51.5% de los participantes manifestó su total acuerdo con la confiabilidad del reconocimiento facial y las huellas dactilares.

Las entrevistas cualitativas proporcionarán información valiosa sobre la implementación práctica de estos sistemas. Un oficial superior del Escuadrón Verde comentó: "La integración de múltiples modalidades biométricas ha revolucionado nuestra capacidad de identificación. Podemos verificar identidades en cuestión de segundos con un alto grado de confiabilidad". Otro participante enfatizó: "El sistema biométrico integrado nos permite detectar intentos de suplantación de identidad que serían prácticamente imposibles de identificar con métodos tradicionales".

Sin embargo, los resultados también revelan preocupaciones sobre la privacidad y protección de datos. Un 44.3% de los encuestados reconoció la existencia de desafíos importantes en este ámbito. Como expresó un entrevistado oficial: "Debemos mantener un equilibrio delicado entre la eficacia operativa y la protección de los derechos individuales. La seguridad de los datos biométricos es una preocupación constante."

La investigación revela una valoración positiva de las bases de datos interconectadas como herramienta para la prevención del delito. Un 39.2% de los participantes expresó su total acuerdo con la eficacia de estas herramientas para facilitar la compartición de información relevante, mientras que un 47.9% mostró un acuerdo considerable.





Las entrevistas revelaron aspectos cruciales sobre la implementación práctica. Un oficial destacó: "La capacidad de acceder instantáneamente a información de múltiples fuentes ha transformado nuestra capacidad de respuesta. Podemos tomar decisiones informadas en tiempo real." Otro participante señaló: "La interconexión de bases de datos nos permite identificar patrones y conexiones que antes habrían pasado desapercibidos".

La optimización de recursos y la evitación de duplicidades es referenciado como un beneficio, con un 36.1% de acuerdo total y un 48.2% de acuerdo considerable. Sin embargo, los desafíos de interoperabilidad y seguridad son reconocidos por un 48,5% de los encuestados como preocupaciones significativas.

El análisis de los datos revela una alta valoración del rastreo digital como herramienta para la identificación y seguimiento de actividades delictivas. Los resultados cuantitativos muestran que un 40.1% de los encuestados expresó su total acuerdo con la eficacia de esta herramienta, mientras que un 45.9% mostró un acuerdo considerable. Particularmente significativa es la percepción sobre su utilidad en la detección de comportamientos delictivos, donde un 34.5% manifestó total acuerdo y un 52.1% un acuerdo significativo.

Las entrevistas cualitativas proporcionarán una comprensión más profunda de la implementación práctica del rastreo digital. Un oficial experimentado señaló: "Las herramientas de rastreo digital nos permiten anticipar patrones de comportamiento criminal y actuar de manera preventiva. La capacidad de análisis predictivo ha transformado nuestra aproximación a la prevención del delito." Otro entrevistado destacó: "La integración de tecnologías de rastreo con otras herramientas digitales nos proporciona una visión más completa y precisa de las actividades sospechosas."

La recopilación de evidencias digitales es reportada como un beneficio crucial, con un 39,2% de acuerdo total y un 50,4% de acuerdo considerable sobre su utilidad en investigaciones criminales. Sin embargo, las preocupaciones éticas y de privacidad son significativas, con un 20.2% de los encuestados expresando total acuerdo y un 29.7% mostrando acuerdo considerable sobre el potencial invasivo de estas técnicas.

El análisis integral de la implementación de herramientas digitales en el Escuadrón Verde revela un panorama de transformación significativa en las prácticas de control de identidad y prevención del delito. La integración de sistemas biométricos, bases de datos interconectadas y técnicas de rastreo digital ha creado un ecosistema tecnológico que potencia las capacidades operativas de la unidad.

Las entrevistas revelan una percepción generalizada de mejora en la eficacia operativa. Un oficial superior comentó: "La integración de estas herramientas ha revolucionado nuestra capacidad de respuesta. Podemos identificar y prevenir amenazas con una precisión y rapidez que antes eran imposibles". Otro participante enfatizó: "El impacto más significativo ha sido en nuestra capacidad de predictivo. Podemos anticipar patrones delictivos y actuar proactivamente".





Los datos cuantitativos respaldan esta percepción positiva. En promedio, más del 80% de los encuestados manifestaron acuerdo o total acuerdo con la efectividad de las herramientas digitales en la prevención del delito. La capacidad de integración entre diferentes sistemas emerge como un factor crucial, con un 48,7% de total acuerdo sobre su importancia en la mejora de la precisión en la identificación.

Sin embargo, los resultados también identifican desafíos significativos en la implementación. La necesidad de equilibrar la eficacia operativa con la protección de derechos individuales emerge como una preocupación constante. Un entrevistado señaló: "El mayor reto es mantener un equilibrio entre la efectividad en la prevención del delito y el respeto a la privacidad y derechos individuales. Es un equilibrio delicado que requiere atención constante".

La gestión de datos y la seguridad de la información se revelan como aspectos críticos. Un 44,3% de los encuestados reconoce desafíos significativos en la protección de datos personales, mientras que un 48,5% identifica la interoperabilidad y seguridad de sistemas como preocupaciones importantes. Las entrevistas sugieren que estos desafíos requieren una aproximación integral que combine soluciones técnicas con políticas y procedimientos robustos.

Discusión

Los hallazgos de esta investigación revelan patrones en la implementación de herramientas digitales para el control de identidad, que merecen un análisis detallado en relación con la literatura existente y las implicaciones prácticas para la prevención del delito.

Los resultados sobre la efectividad de los sistemas biométricos integrados coinciden con lo planteado por Rodríguez et al. (2022), quienes señalan que la combinación de diferentes modalidades biométricas puede alcanzar tasas de precisión superiores al 99,9%. La alta valoración de estas herramientas por parte de los oficiales del Escuadrón Verde (88.5% de aprobación combinada) respalda esta afirmación teórica. Sin embargo, se observa una divergencia interesante con la percepción de vulnerabilidad. Mientras que García y López (2022) enfatizan primordialmente los riesgos de seguridad de datos, los hallazgos revelan una preocupación más equilibrada entre la seguridad técnica y las implicaciones éticas del uso de datos biométricos. Esta diferencia podría atribuirse al contexto específico de implementación en el Escuadrón Verde, donde la experiencia práctica ha revelado dimensiones adicionales de la problemática.

La capacidad de los sistemas biométricos para adaptarse a distintos niveles de seguridad, señalada por Pérez y Martínez (2024), se refleja en los hallazgos cualitativos. Las entrevistas evidencian que esta flexibilidad es especialmente valorada en operaciones policiales, aunque también revelan la necesidad de protocolos más definidos para determinar el nivel de verificación adecuado en cada situación.

En cuanto a las bases de datos interconectadas, los resultados amplían lo planteado por González y Martínez (2023) sobre su eficacia en la detección de documentos fraudulentos.





Mientras estos autores reportan un incremento del 50% en la detección, las entrevistas indican que su impacto no se limita a la identificación de fraudes, sino que también fortalece la coordinación interinstitucional y mejora la toma de decisiones operativas.

Si bien estudios previos, como el de Leiva (2020), han centrado el análisis en desafíos técnicos, los hallazgos destacan el papel del factor humano en la efectividad de estos sistemas. La preocupación por la interoperabilidad, expresada por el 48.5% de los encuestados, sugiere que los problemas no son exclusivamente tecnológicos, sino que también involucran aspectos operativos y organizacionales.

La inquietud sobre privacidad y protección de datos, identificada por Páez (2023), se confirma en los testimonios del personal policial, aunque con matices relevantes. Los resultados indican que los oficiales del Escuadrón Verde han desarrollado una comprensión más precisa sobre el equilibrio entre eficacia operativa y protección de derechos individuales, lo que evidencia una visión más integral del problema.

Por otro lado, los hallazgos sobre rastreo digital presentan puntos de convergencia y divergencia con la literatura existente. El alto nivel de aprobación (86%) respecto a su eficacia coincide con lo señalado por Rodríguez y Gómez (2023) sobre el incremento del 40% en la detección de actividades delictivas en línea. Sin embargo, los testimonios destacan que su utilidad no se limita a la detección, sino que también desempeña un rol estratégico en la prevención del delito.

La incorporación de inteligencia artificial en el rastreo digital, señalada por López y Sánchez (2024), se refleja en las entrevistas, indicando que, si bien la IA incrementa la capacidad de detección, los oficiales resaltan la importancia del criterio humano en la interpretación de los datos. Esta perspectiva cuestiona la automatización absoluta en el trabajo policial y plantea la necesidad de una supervisión activa en su aplicación.

Uno de los aspectos distintivos respecto a estudios previos es la percepción sobre los dilemas éticos. Mientras que García y Pérez (2023) destacan los riesgos de invasión a la privacidad, los resultados sugieren una preocupación más amplia. Los entrevistados reconocen la necesidad de equilibrar la eficacia operativa con la protección de derechos individuales.

El análisis de la implementación de herramientas digitales permite identificar patrones que complementan y amplían la comprensión actual del tema. La alta tasa de aprobación (más del 80%) concuerda con lo expresado por Torres et al. (2023) sobre la necesidad de contar con un marco técnico y normativo sólido. Sin embargo, se evidencia que la aplicación práctica enfrenta desafíos adicionales, como la interoperabilidad entre sistemas y la capacitación del personal, aspectos poco abordados en la literatura.

Un elemento central en esta discusión es la interconexión entre diversas herramientas digitales. Mientras que estudios como el de Fernández y Ortiz (2024) analizan cada tecnología de manera aislada, los resultados indican que la combinación de sistemas biométricos, bases de





datos y rastreo digital incrementa la eficacia en la prevención del delito. La integración de estos recursos no solo optimiza el acceso a la información, sino que también fortalece la capacidad de respuesta ante situaciones delictivas.

Otro factor determinante en la implementación de estas tecnologías es la adaptación organizacional. Los hallazgos revelan que el éxito en su aplicación no depende exclusivamente de los avances tecnológicos, sino también de la capacidad institucional para modificar sus procesos y estructuras operativas. La gestión del cambio se presenta como un elemento clave, ya que la resistencia interna y la falta de formación pueden limitar los beneficios esperados.

Finalmente, los resultados muestran una evolución en la concepción de la seguridad digital. Mientras que INTERPOL (2024) enfatiza principalmente los aspectos técnicos de la protección de datos, las entrevistas reflejan una visión más amplia. La seguridad se entiende no solo como una cuestión tecnológica, sino como el equilibrio entre protección de la información, eficiencia operativa y garantía de los derechos individuales.

La capacitación y el desarrollo de competencias se manifiestan como un factor importante, coincidiendo con lo planteado por López y Sánchez (2023), aunque con un énfasis adicional en la importancia de la experiencia práctica y el aprendizaje continuo. Los resultados sugieren que la efectividad de las herramientas digitales depende significativamente de la capacidad del personal para utilizarlas de manera óptima y ética.

Conclusiones

La incorporación de herramientas digitales para el control de identidad en el Escuadrón Verde de Lima ha transformado las estrategias de prevención del delito, generando tanto oportunidades como desafíos que requieren atención continua.

Los sistemas biométricos integrados han demostrado ser un recurso efectivo en la modernización del control de identidad, con una aprobación del 88.5% entre los oficiales. La combinación de múltiples modalidades biométricas ha mejorado la precisión en la identificación de individuos, aunque persisten preocupaciones en torno a la protección de datos y la privacidad. Además, la capacidad de estos sistemas para adaptarse a distintos niveles de seguridad representa una ventaja operativa al permitir una respuesta proporcional según el nivel de riesgo.

Las bases de datos interconectadas han optimizado el uso de recursos y mejorado la eficiencia operativa al facilitar el intercambio de información en tiempo real y reducir duplicaciones. Esta mejora ha fortalecido la capacidad de respuesta del Escuadrón Verde; sin embargo, el 48.5% de los participantes identifica dificultades en la interoperabilidad y la seguridad, lo que evidencia la necesidad de una implementación que considere tanto aspectos técnicos como organizacionales.

El rastreo digital ha sido validado como una herramienta eficaz para la identificación y seguimiento de actividades delictivas, con un 86% de aprobación entre los entrevistados. La





incorporación de tecnologías de análisis predictivo ha permitido anticipar y prevenir delitos con mayor precisión. No obstante, las inquietudes sobre privacidad y ética evidencian la necesidad de establecer protocolos más estrictos que garanticen un equilibrio entre la eficacia operativa y la protección de derechos individuales.

La implementación integral de herramientas digitales en el control de identidad ha demostrado ser una estrategia efectiva para la prevención del delito, aunque requiere un equilibrio que contemple diversas dimensiones. La combinación de tecnologías, respaldada por más del 80% de aprobación general, indica que la efectividad en la prevención del delito no depende únicamente de la capacidad de cada herramienta por separado, sino de su integración en un sistema funcional y coherente.

Los hallazgos destacan la necesidad de armonizar la eficiencia operativa con la protección de derechos individuales, lo que exige un marco normativo flexible que se ajuste al desarrollo tecnológico. Además, la capacitación continua y el fortalecimiento de competencias resultan fundamentales para optimizar el uso de estas herramientas y reducir los riesgos asociados a su implementación.

Referencias

- Aguinaga, ME (2023). Nivel de aceptación de un sistema biométrico de control de acceso, basado en el reconocimiento facial para la identificación del personal docente [Tesis de maestría, Universidad de Ciencias Comerciales].
- Blanco, LG (2022). Intercepción, demora, identificación y solicitud de personas efectuadas por la Policía "sin orden judicial" previa. *Revista Pensamiento Penal*, 428, 1-58.
- Defensoría del Pueblo. (2019). Informe de Adjuntía N° 003-2019-DP/ADHPD Supervisión Nacional a los Departamentos de Investigación Criminal de la Policía Nacional del Perú. [https://www.defensoria.gob.pe/wp-content/uploads/2019/09/INFORME-DE-ADJUNTIA-N-003-2019-DP-ADHPD-Supervisión-Nacional-a-los-Departamentos-de - Investigación.pdf](https://www.defensoria.gob.pe/wp-content/uploads/2019/09/INFORME-DE-ADJUNTIA-N-003-2019-DP-ADHPD-Supervision-Nacional-a-los-Departamentos-de-Investigacion.pdf)
- Duce, M. y Lillo, R. (2020). Controles de identidad realizados por Carabineros: Una aproximación empírica y evaluativa sobre su uso en Chile. *Revista de Estudios de la Justicia*, 33, 167-203. <https://doi.org/10.5354/0718-4735.2020.57635>
- Leiva, MH (2020). Open Banking: Desafíos de las Entidades Financieras a la protección de Datos Personales [Tesis de grado, Universidad de San Andrés]. <https://repositorio.udesa.edu.ar/jspui/bitstream/10908/22839/1/%5BP%5D%5BW%5D%20T.%20Ab.%20Leiva%20Onetto%2C%20Mateo%20Hernán.pdf>
- Llerena, GC y Zelada, R. (2022). Aplicativo Seguridad 365 para la prevención e investigación del delito contra el patrimonio en el distrito de Santiago de Surco [Tesis de maestría, Pontificia Universidad Católica del Perú].





- Páez, JA (2023). Soluciones de Software en el Contexto de la Transformación Digital [Tesis de grado, Universidad Cooperativa de Colombia].
<https://repository.ucc.edu.co/server/api/core/bitstreams/573791e2-5c9f-4faa-9a86-f8822700336d/content>
- Policía Nacional del Perú. (2020). Anuario estadístico policial. PNP.
- Policía Nacional del Perú. (2021). Anuario estadístico policial. PNP.
- Policía Nacional del Perú. (2022). Anuario estadístico policial. PNP.
- Ruiz, ML (2021). Intervención policial por control de identidad como mecanismo de "detención por sospecha" ciudad de Yurimaguas Región San Martín año 2020 [Tesis de grado, Universidad Señor de Sipán].
- Torres, C., Vega, D. y Morales, E. (2023). Implementación de sistemas de control de identidad digital en América Latina: Un estudio comparativo. Revista Latinoamericana de Criminología, 16(2), 145-162.
- Villaplana, R. (2021). Recursos digitales de colaboración y de seguridad pública. QEPD: Revista de Investigaciones Políticas y Sociológicas, 20(2), 1-18.
<https://doi.org/10.15304/rips.20.2.7989>
- Vivas, E. (2022). Utilización de herramientas tecnológicas para el desarrollo de una política pública de seguridad pública - El caso de la Ciudad Autónoma de Buenos Aires [Tesis de maestría, Universidad Torcuato di Tella].
https://repositorio.utdt.edu/bitstream/handle/20.500.13098/12079/MPP_Vivas_2022.pdf?sequence=1

