Proyecto: Estrategias para incorporar Big Data e Inteligencia Artificial en la gestión de riesgos del sector de seguridad en Bogotá

Jimy Alexander Parra Fernández

Yuly Viviana Barreto Romero

Corporación Universitaria Minuto de Dios

Rectoría Virtual

Programa Especialización en Gerencia de Proyectos

junio de 2025

Proyecto: Estrategias para incorporar Big Data e Inteligencia Artificial en la gestión de riesgos del sector de seguridad en Bogotá

Jimy Alexander Parra Fernández
Yuly Viviana Barreto Romero

Trabajo de Grado presentado como requisito para optar al título de Especialista en Gerencia de Proyectos

Asesor(a)
Sergio Andrés Zabala Vargas
Doctor en Tecnología Educativa

Corporación Universitaria Minuto de Dios

Rectoría Virtual

Programa Especialización en Gerencia de Proyectos

junio de 2025

Contenido

Lista de tablas 5
Lista de figuras 6
Lista de anexos 7
Resumen 8
Abstract 10
Introducción 12
1 PLANTEAMIENTO DEL PROBLEMA 14
1.1 Descripción del problema 14
1.2 La pregunta de investigación 16
1.3 Los objetivos de investigación 16
1.3.1 Objetivo general 16
1.3.2 Objetivos específicos 17
1.4 Justificación de la investigación 17
2 MARCO DE REFERENCIA 20
2.1 Marco de Antecedentes 20
2.2 Marco Teórico 25
2.3 Marco normativo 28
3 METODOLOGÍA 31
3.1 Enfoque y alcance de la investigación 31
3.2 Población y muestra 32
3.2.1 Definición de la población 32
3.2.2 Cálculo y selección de la muestra 33
3.3 Instrumento(s) 34
3.3.1 Revisión sistemática de la literatura 34
3.3.2 Encuesta sobre nivel de madurez tecnológica 35
3.4 Descripción de procedimientos 37
3.4.1 Revisión de literatura 39
3.4.2 Encuesta de medición de nivel de madurez tecnológico 40

3.5 Análisis de información 42
3.5.1 Recolección de datos 43
3.5.2 Codificación de datos 44
3.6 Consideraciones éticas 45
3.6.1 Análisis de consideraciones éticas 45
3.6.2 Instrumentos de aceptación y autorización 46
4 HIPÓTESIS 48
4.1 Las variables 48
4.1.1 Variable(s) independiente(s) 48
4.1.2 Variable(s) dependiente(s) 49
5 RESULTADOS 51
5.1 Presentación de resultados 51
5.2 Propuesta al sector 68
5.3 Discusión 74
6 CONCLUSIONES 77
7 Referencias 80
Anexos 86

Lista de tablas

Tabla 1. MATRIZ DE ANÁLISIS BIBLIOGRÁFICO 51
Tabla 2. MODELO DE NEGOCIO Y PRODUCTO – Nivel estratégico. 56
Tabla 3. CLIENTES Y PROVEEDORES 60
Tabla 4. PROCESOS DE NIVEL TACTICO Y OPERATIVO 62
Tabla 5. INFRAESTRUCTURA Y SEGURIDAD 64
Tabla 6. ESTRATEGIA Y EXPERIENCIA EN INDUSTRIA 4.0 66

Lista de figuras

Figura 1. Cálculo de tamaño de muestra 33
Figura 2. Nivel de inversión durante 2 años 58

Lista de anexos

Anexo 1. Encuesta de identificación de la tecnología emergente en la gestión de riesgos en el sector de seguridad privada en Colombia.

Anexo 2. Declaración inicial e información sobre Encuesta de nivel de madurez tecnológico.

Resumen

En un entorno global marcado por la incertidumbre y la acelerada transformación digital, las organizaciones del sector de vigilancia y seguridad privada enfrentan crecientes desafíos para identificar, analizar y gestionar riesgos de manera eficiente. En Bogotá, muchas de estas empresas operan aún con metodologías manuales y desarticuladas, desaprovechando el potencial de datos generados por sensores, videovigilancia y sistemas GPS. Esta investigación plantea estrategias para incorporar tecnologías emergentes, como Big Data e Inteligencia Artificial (IA), en la gestión de riesgos del sector.

El estudio se desarrolló bajo un enfoque cuantitativo, estructurado en dos fases: una revisión sistemática de literatura (2018–2025) en la base de datos ScienceDirect y una encuesta aplicada a 30 empresas de seguridad privada en Bogotá. Esta permitió diagnosticar su nivel de madurez tecnológica y conocer el estado actual de uso y apropiación de tecnologías emergentes.

Los resultados muestran una adopción aún incipiente: solo el 10 % de las organizaciones ha iniciado acciones concretas de transformación digital, y el 33 % cuenta con estrategias formuladas, pero no implementadas. La interoperabilidad tecnológica solo está presente en el 17 %, la comunicación entre máquinas (M2M) en el 10 %, y apenas el 27 % de las empresas está en procesos activos de capacitación. No obstante, el 63 % valora el Big Data como altamente importante, y el 53 % reconoce el potencial de la IA.

La propuesta final incluye estrategias en tres fases: diagnóstico de madurez, adopción progresiva de herramientas tecnológicas y fortalecimiento del talento humano e infraestructura digital. Estas recomendaciones buscan cerrar brechas, fomentar la interoperabilidad, promover una cultura organizacional basada en datos y mejorar la capacidad de respuesta ante riesgos. Este

estudio aporta herramientas aplicables al fortalecimiento del sector y ofrece una base sólida para futuras investigaciones en contextos de transformación tecnológica similar.

Palabras clave: gestión de riesgos; inteligencia artificial; Big Data; seguridad privada; transformación digital; toma de decisiones

Abstract

In a global context marked by uncertainty and digital transformation, private security and surveillance organizations face growing challenges in efficiently identifying, analyzing, and managing risks. In Bogotá, many companies still rely on manual and fragmented methods, underutilizing data from sensors, video surveillance, and GPS systems. This study proposes strategies to incorporate emerging technologies such as Big Data and Artificial Intelligence (AI) into risk management processes within the sector.

A quantitative methodology was adopted, consisting of two phases: a systematic literature review (2018–2025) using the ScienceDirect database and a survey conducted among 30 private security companies in Bogotá to assess their level of technological maturity and adoption of emerging technologies.

Findings reveal limited implementation: only 10% of organizations have taken concrete steps toward digital transformation, while 33% have formulated strategies without effective execution. Technological interoperability is present in just 17% of cases, machine-to-machine communication in 10%, and only 27% of companies are actively engaged in digital training. However, 63% of respondents recognize Big Data as highly important, and 53% acknowledge the relevance of AI.

The final proposal is structured in three phases: diagnosis of digital maturity, gradual adoption of key technological tools, and strengthening of human talent and digital infrastructure. These strategies aim to close technological gaps, foster system interoperability, promote a data-driven organizational culture, and improve risk response capacity. This research contributes to strengthening the sector and provides a foundation for future studies in similar contexts of technological transformation.

Keywords: risk management; artificial intelligence; Big Data; private security; digital transformation; decision making

Introducción

En el actual escenario global, caracterizado por la complejidad, la velocidad del cambio y la creciente digitalización de procesos, la gestión de riesgos ha evolucionado hacia modelos más proactivos y basados en datos. Tecnologías emergentes como Big Data e Inteligencia Artificial (IA) han demostrado su capacidad para optimizar la identificación, análisis y evaluación de riesgos en diversos sectores, incluyendo la banca, la salud, la logística y la seguridad (Marr, 2021). Estas herramientas permiten no solo procesar grandes volúmenes de información en tiempo real, sino también generar modelos predictivos que anticipan amenazas y facilitan decisiones estratégicas informadas (Russom, 2011).

En América Latina, la integración de estas tecnologías avanza de manera desigual. Países como Brasil, México y Colombia han comenzado a adoptar soluciones basadas en IA y análisis de datos para mejorar la eficiencia y seguridad en sectores críticos. En Colombia, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) ha promovido desde 2019 una política nacional de transformación digital que incluye la adopción de IA en procesos públicos y privados, aunque su implementación en sectores como la seguridad privada aún presenta limitaciones estructurales (MinTIC, 2020). Esta situación se ve agravada por la baja inversión tecnológica, la escasa formación del talento humano y la resistencia cultural al cambio digital (González & Moreno, 2021).

Bogotá, como principal centro urbano y económico del país, concentra el mayor número de empresas de vigilancia privada, las cuales enfrentan entornos operativos complejos marcados por el aumento de la criminalidad, la movilidad urbana y la necesidad de respuesta rápida ante incidentes. No obstante, muchas de estas organizaciones aún gestionan los riesgos con metodologías manuales y fragmentadas, sin aprovechar los datos que ya generan a través de sensores, videovigilancia, bitácoras, GPS o registros electrónicos. Esta realidad evidencia una brecha tecnológica importante que limita su capacidad de anticipación, eficiencia operativa y competitividad (Vásquez & Beltrán, 2022).

En este contexto, el presente proyecto de investigación tiene como propósito desarrollar un conjunto de estrategias para incorporar tecnologías emergentes como Big Data e Inteligencia Artificial en la gestión de riesgos de organizaciones de vigilancia y seguridad privada en Bogotá. Esta propuesta busca fortalecer la capacidad analítica del sector, mejorar la toma de decisiones estratégicas, reducir los costos operativos y aumentar la eficiencia y resiliencia ante amenazas emergentes.

La estructura de este documento se organiza en siete capítulos. En el capítulo 1 se presenta el planteamiento del problema, la pregunta de investigación, los objetivos y la justificación del estudio. El capítulo 2 desarrolla el marco de referencia, que incluye los antecedentes investigativos, el marco teórico y el marco normativo. El capítulo 3 detalla la metodología, el enfoque investigativo, la muestra, los instrumentos y las consideraciones éticas. En el capítulo 4 se formula la hipótesis y se definen las variables del estudio. El capítulo 5 contiene los resultados obtenidos y la propuesta estratégica para el sector. En el capítulo 6 se exponen las conclusiones de la investigación, y el capítulo 7 presenta las referencias bibliográficas.

1 PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción del problema

En el entorno global, caracterizado por su alta volatilidad, complejidad e incertidumbre, las organizaciones enfrentan crecientes desafíos relacionados con la gestión de riesgos. En este contexto, tecnologías emergentes como el Big Data y la Inteligencia Artificial (IA) han demostrado su capacidad para transformar la manera en que las organizaciones identifican, analizan y evalúan riesgos, optimizando la toma de decisiones estratégicas. A nivel mundial, el uso de estas herramientas ha generado avances significativos en sectores como la banca, la salud, la logística y la seguridad, gracias a su capacidad para analizar grandes volúmenes de datos en tiempo real y generar modelos predictivos (MarketsandMarkets, 2022).

A nivel latinoamericano, países como Brasil, México y Colombia han comenzado a adoptar herramientas basadas en IA y análisis de datos para mejorar la eficiencia en sectores críticos como la seguridad, salud y transporte (CAF, 2021). En Colombia, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC, 2020) ha promovido el uso de tecnologías emergentes a través de su política nacional de transformación digital, incentivando la integración de IA en procesos operativos y estratégicos, incluso en el sector privado. Sin embargo, la implementación en sectores específicos como el de vigilancia y seguridad privada aún presenta desafíos significativos, especialmente en el análisis y gestión de riesgos asociados a los proyectos operativos y logísticos de estas organizaciones.

En Bogotá, ciudad con la mayor concentración de empresas de vigilancia del país, las organizaciones de seguridad privada enfrentan entornos urbanos cada vez más complejos, con altos niveles de criminalidad, movilidad intensa y riesgos operacionales diversos. La Cámara de Comercio de Bogotá (2023) identificó que más del 60 % de las empresas del sector reconocen dificultades para realizar una evaluación efectiva de riesgos, debido a la dependencia de metodologías manuales, la falta de herramientas tecnológicas y la baja capacidad para integrar fuentes de datos diversas.

En este contexto, las organizaciones del sector de vigilancia y seguridad privada en Bogotá enfrentan serias limitaciones en la identificación, análisis y evaluación sistemática de riesgos en sus operaciones. Las decisiones estratégicas que se toman actualmente dependen, en su mayoría, de reportes manuales y análisis retrospectivos, lo que limita la capacidad de anticiparse a eventos críticos o de optimizar los recursos frente a amenazas emergentes. A pesar de contar con grandes volúmenes de datos provenientes de sensores, registros de personal, bitácoras de incidentes, cámaras de videovigilancia y sistemas GPS, estos no son procesados de manera integrada ni se utilizan para alimentar modelos predictivos o algoritmos de IA.

Las causas de esta problemática pueden rastrearse hasta la falta de infraestructura tecnológica adecuada, el desconocimiento técnico por parte de los tomadores de decisiones y la resistencia organizacional al cambio digital. Según un estudio de la Universidad Nacional de Colombia (González & Moreno, 2021), muchas empresas del sector seguridad aún conciben las tecnologías como herramientas complementarias, y no como sistemas transformadores de su modelo de negocio. A esto se suma la falta de inversión en talento humano capacitado en analítica de datos y la ausencia de una cultura organizacional orientada hacia la innovación basada en datos (Vásquez & Beltrán, 2022).

Estas limitaciones generan consecuencias negativas tanto internas como externas para la organización. A nivel interno, se traduce en una toma de decisiones lenta y poco informada, con un alto grado de incertidumbre. Asimismo, se incrementan los costos operativos por ineficiencias en la asignación de recursos y se reduce la capacidad de respuesta frente a eventos adversos. A nivel externo, la empresa se vuelve menos competitiva, pierde contratos por fallas en el servicio y enfrenta sanciones por incumplimiento de estándares de gestión del riesgo. De hecho, la Superintendencia de Vigilancia y Seguridad Privada (2023) ha reportado un aumento en los procesos sancionatorios a empresas que no cumplen con protocolos mínimos de identificación y mitigación de riesgos. Por tanto, se plantea la necesidad de investigar cómo la implementación de herramientas de Big Data e Inteligencia Artificial puede facilitar la identificación, análisis y evaluación de riesgos en los proyectos de organizaciones de vigilancia y seguridad privada en Bogotá.

1.2 La pregunta de investigación

¿Cómo puede la implementación de Big Data e Inteligencia Artificial facilitar la identificación, análisis y evaluación de riesgos en proyectos de organizaciones de vigilancia y seguridad privada en Bogotá, Colombia; para mejorar la toma de decisiones estratégicas?

1.3 Los objetivos de investigación

1.3.1 Objetivo general

Presentar un conjunto de estrategias y recomendaciones para la incorporación de tecnologías emergentes, como Big Data e Inteligencia Artificial, que faciliten la identificación,

análisis y evaluación de riesgos en proyectos de organizaciones de vigilancia y seguridad privada en Bogotá, Colombia, con el propósito de mejorar la toma de decisiones estratégicas.

1.3.2 Objetivos específicos

Diagnosticar el estado actual de la implementación de tecnologías emergentes, específicamente Big Data e Inteligencia Artificial, en la gestión de riesgos en proyectos del sector de vigilancia y seguridad privada en Bogotá, Colombia, a partir de la revisión de literatura.

Establecer el estado de la incorporación de tecnologías emergentes y el interés de apropiación en la gestión de riesgos en proyectos del sector de vigilancia y seguridad privada en Bogotá, Colombia.

Desarrollar un conjunto de estrategias y recomendaciones para la incorporación de tecnologías emergentes, como Big Data e Inteligencia Artificial, en la gestión de riesgos de proyectos del sector de vigilancia y seguridad privada en Bogotá, Colombia; con el fin de contribuir a la modernización operativa y al fortalecimiento de la capacidad de respuesta del sector en la ciudad.

1.4 Justificación de la investigación

En un entorno global marcado por la incertidumbre, la creciente complejidad de los entornos urbanos y la evolución constante de las amenazas a la seguridad ciudadana, las organizaciones deben transformarse para responder de manera más eficiente y estratégica. La gestión de riesgos se ha convertido en un eje central para la sostenibilidad organizacional, particularmente en sectores como la vigilancia y seguridad privada, donde los riesgos son

dinámicos y multifactoriales. Ante esta realidad, tecnologías emergentes como el Big Data y la Inteligencia Artificial (IA) han demostrado su potencial para revolucionar los procesos de identificación, análisis y evaluación de riesgos, permitiendo a las organizaciones tomar decisiones basadas en datos, con mayor precisión, rapidez y capacidad predictiva (Marr, 2021).

Actualmente, muchas organizaciones de vigilancia en Colombia operan bajo esquemas tradicionales de análisis de riesgo, con metodologías manuales y desarticuladas que no permiten anticiparse con eficacia a amenazas emergentes ni adaptarse al dinamismo del entorno. Según el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC, 2020), la incorporación de IA y analítica avanzada en sectores estratégicos del país aún se encuentra en etapas iniciales, especialmente en pequeñas y medianas empresas, donde predominan la baja inversión tecnológica y la escasa capacitación del talento humano. Esta situación se replica en muchas empresas de seguridad privada, que pese a contar con grandes volúmenes de datos (videovigilancia, geolocalización, reportes de incidentes), no disponen de las herramientas ni del conocimiento necesario para transformarlos en insumos estratégicos.

Este proyecto se justifica por la necesidad urgente de cerrar esa brecha tecnológica. Al diagnosticar el estado actual de implementación de Big Data e IA en organizaciones de vigilancia en Bogotá, y desarrollar estrategias para su incorporación, se pretende contribuir a la modernización del sector, dotándolo de herramientas que optimicen su capacidad para anticipar amenazas, asignar recursos de manera más eficiente y tomar decisiones estratégicas fundamentadas. Como afirma Russom (2011), las organizaciones que adoptan enfoques analíticos avanzados logran una ventaja competitiva sostenible al transformar los datos en conocimiento accionable, especialmente en contextos donde el tiempo de respuesta es crucial.

Desde el punto de vista científico y académico, esta investigación representa una oportunidad para generar conocimiento nuevo y contextualizado en un área poco explorada en Colombia y América Latina. Aunque existen múltiples estudios sobre el impacto del Big Data en sectores como el financiero, la salud o la industria 4.0, el sector de la seguridad privada sigue siendo un campo con escasa documentación investigativa, pese a su impacto en la seguridad ciudadana y el orden público. Esta investigación, por tanto, responde a la necesidad de ampliar la base empírica y teórica sobre la aplicación de tecnologías emergentes en este campo específico, contribuyendo al desarrollo de modelos replicables en otros contextos similares (González & Moreno, 2021).

En cuanto a los estudiantes involucrados en el proyecto, esta investigación representa una oportunidad significativa para el desarrollo de competencias analíticas, investigativas y tecnológicas alineadas con las demandas del siglo XXI. Al abordar un problema real con herramientas metodológicas rigurosas y con un enfoque aplicado, los estudiantes desarrollarán habilidades valiosas para su ejercicio profesional en campos como la gestión de riesgos, la seguridad corporativa, el análisis de datos y la consultoría tecnológica.

En conclusión, esta investigación es pertinente, oportuna y necesaria. Aporta soluciones concretas a una problemática crítica del sector de vigilancia y seguridad privada en Bogotá, con impacto directo en la eficiencia operativa de las organizaciones, la seguridad de la ciudadanía y la generación de conocimiento científico.

2 MARCO DE REFERENCIA

2.1 Marco de Antecedentes

Para el desarrollo de esta investigación, se realizó una revisión del estado del arte correspondiente a los últimos siete años (junio 2018 – junio 2025). La búsqueda se llevó a cabo en la plataforma ScienceDirect, utilizando la siguiente ecuación de búsqueda: ("Big Data" OR "data analysis") AND ("Artificial Intelligence" OR "AI") AND ("risk management" OR "risk assessment" OR "risk analysis") AND ("private security" OR "security services").

El trabajo de Galindo Caldés (2019) destaca la necesidad de transformar la gestión de recursos humanos en el sector público ante la nueva realidad tecnológica. La incorporación de la inteligencia artificial exige una redefinición de las tareas y funciones de los empleados públicos, lo que impulsa una transformación del modelo burocrático tradicional hacia una administración más moderna y eficiente. Este proceso implica la adopción de recursos humanos con competencias digitales, capaces de adaptarse a entornos dinámicos y automatizados. El estudio subraya que esta transición no es solo tecnológica, sino también organizacional y cultural, y requiere una visión estratégica en la formulación de políticas públicas. Además, plantea que la integración de tecnologías emergentes puede fortalecer la transparencia y la eficiencia en los servicios estatales.

Por su parte, Álvarez, Leguizamón-Páez y Londoño (2021) ofrecen una revisión integral sobre los riesgos de ciberseguridad que emergen de la interacción entre el Internet de las cosas (IoT) y Big Data. En su análisis, identifican amenazas críticas como la exposición de información sensible y la pérdida de integridad de los datos en infraestructuras distribuidas, especialmente en sectores estratégicos como la seguridad privada. Ante este panorama, los

autores proponen soluciones tecnológicas como el cifrado de datos en tránsito y en reposo, el uso de arquitecturas de red resilientes, y la implementación de análisis en el borde (edge analytics). Estas estrategias permiten reducir vulnerabilidades y fortalecer la defensa de sistemas que operan con grandes volúmenes de datos en tiempo real.

El estudio de Jauregi-Maza (2021) muestra cómo el uso de Big Data ha transformado significativamente la gestión pública en España, con efectos evidentes en sectores clave como la salud y la gestión urbana. La disponibilidad de información en tiempo real ha facilitado la toma de decisiones más ágiles y ha empoderado a los ciudadanos, quienes ahora pueden realizar trámites de forma más rápida y eficiente. Asimismo, el autor enfatiza que una gestión adecuada de los datos contribuye a optimizar las tareas administrativas cotidianas dentro de las instituciones públicas. Esta transformación no solo mejora la calidad del servicio, sino que también aumenta la capacidad de respuesta del Estado frente a las necesidades sociales.

En la misma línea, Cercos Rubio y Hermoso Traba (2022) analizan el impacto de la inteligencia artificial y Big Data en la gestión del talento humano dentro de las organizaciones. Los autores destacan que estas tecnologías pueden representar tanto ventajas como desafíos, especialmente en términos de adaptación del personal y gestión ética de los datos. Subrayan que la inteligencia artificial permite liberar a los profesionales del análisis manual de grandes volúmenes de información, enfocándose así en tareas estratégicas. Además, estas herramientas facilitan la reducción de costos, mejoran el conocimiento del comportamiento de los colaboradores y pueden aplicarse en diversas funciones del departamento de recursos humanos, optimizando sus procesos de manera integral.

Samaniego Piedrahita (2022) expone cómo las herramientas de Big Data pueden ser aprovechadas por organizaciones sociales para mejorar sus estrategias y aumentar el impacto de sus proyectos. En su investigación, se resalta que el análisis de grandes volúmenes de datos facilita la toma de decisiones más informadas y permite identificar oportunidades de crecimiento y fortalecimiento institucional. Asimismo, el autor recomienda el uso sistemático de estas tecnologías para gestionar eficazmente la información, lo cual se convierte en un elemento crucial para garantizar la sostenibilidad y eficacia de las iniciativas sociales. Este enfoque refuerza el papel de la analítica de datos como un motor para el desarrollo en contextos no empresariales.

Por otro lado, Satama y Terán (2023) examinan cómo la inteligencia artificial se convierte en un instrumento clave para maximizar beneficios y reducir costos en todos los niveles organizacionales. Su aplicación en áreas como finanzas, logística, producción y gestión de talento humano contribuye significativamente a la eficiencia empresarial. Además, la inteligencia artificial permite mejorar la toma de decisiones gracias a su capacidad para analizar patrones, prever escenarios y sugerir acciones estratégicas. Los autores recalcan que esta tecnología se posiciona como un pilar esencial en la modernización de la estructura empresarial, promoviendo una cultura organizacional basada en datos y resultados.

Montaudon-Tomas, Pinto-López y Amsler (2023) presentan un análisis sobre la implementación de inteligencia artificial en la gestión de proyectos, destacando su utilidad en la automatización de procesos y el seguimiento continuo de tareas. Las herramientas inteligentes permiten extender el análisis predictivo y prospectivo, lo que favorece la identificación temprana de riesgos y la optimización del cumplimiento de objetivos. Esta automatización también reduce la carga operativa, eliminando tareas repetitivas y mejorando la eficiencia del trabajo

colaborativo. El estudio concluye que la incorporación de IA en la gestión de proyectos no solo eleva la productividad, sino que también impulsa la innovación y la capacidad de adaptación ante cambios.

Smith (2023) explora la sinergia entre Big Data y modelos de inteligencia artificial, especialmente el aprendizaje automático, en el fortalecimiento de la ciberseguridad. Su investigación demuestra que estos sistemas permiten detectar amenazas en tiempo real mediante el análisis de patrones de comportamiento, lo que resulta especialmente útil en contextos de vigilancia que exigen respuestas rápidas y precisas. La anticipación de incidentes se convierte en un factor clave para reducir daños potenciales, garantizando una protección proactiva. Este enfoque demuestra cómo la inteligencia artificial, combinada con el análisis de datos masivos, puede revolucionar los sistemas de seguridad digital.

En el caso de Coronado (2024), se analiza la relevancia de la inteligencia artificial en las instituciones de seguridad social, destacando su papel en la modernización de procesos y el cumplimiento de objetivos institucionales. El autor señala que la gestión de datos maestros constituye un recurso esencial que debe integrarse con funciones tecnológicas, corporativas e institucionales. Además, resalta la necesidad de establecer marcos regulatorios específicos para garantizar que el uso de estas tecnologías respete los derechos y libertades de los ciudadanos. En este sentido, el trabajo de Coronado aporta una visión crítica sobre los desafíos éticos y normativos asociados al uso de IA y Big Data en entornos públicos.

Danish (2024) realiza un enfoque cuantitativo utilizando análisis predictivo aplicado a la ciberseguridad, basado en conjuntos de datos reales. A través del uso de algoritmos como la regresión logística y el clustering, demuestra que es posible prever amenazas con alta precisión

y, en consecuencia, reducir los tiempos de respuesta ante incidentes. Este modelo permite fortalecer los sistemas de gestión de riesgos en contextos operativos complejos, donde la velocidad y precisión en la toma de decisiones son fundamentales. El estudio confirma el valor de la analítica avanzada como una herramienta indispensable para construir entornos más seguros y resilientes.

El trabajo de Marwan (2024) se centra en las arquitecturas integradoras que combinan Big Data, inteligencia artificial y gobernanza de datos, orientadas a fortalecer la seguridad institucional. El autor argumenta que una implementación exitosa de estas tecnologías no solo requiere herramientas técnicas, sino también estructuras organizacionales que fomenten la colaboración entre humanos y sistemas inteligentes. Esta interacción se vuelve especialmente importante en organizaciones encargadas de manejar datos sensibles, como las del sector vigilancia, donde la confianza y la eficiencia son esenciales. El estudio destaca que la integración tecnológica debe ir acompañada de una gobernanza clara y ética.

Finalmente, Alevizos y Dekker (2024) proponen un modelo híbrido para incorporar inteligencia artificial en sistemas de inteligencia de amenazas, el cual automatiza desde la recolección hasta la generación de alertas. Este modelo incluye además principios de trazabilidad y consideraciones éticas, buscando asegurar un equilibrio entre automatización y supervisión humana. Los autores insisten en que la colaboración entre operadores humanos y sistemas inteligentes es clave para garantizar decisiones fundamentadas y evitar una dependencia excesiva de los procesos automatizados. Este enfoque refuerza la idea de que la tecnología debe complementar, y no reemplazar, la capacidad crítica del ser humano en la gestión de riesgos.

2.2 Marco Teórico

El avance de las tecnologías emergentes ha transformado significativamente la forma en que las organizaciones gestionan sus procesos críticos, incluyendo la identificación, análisis y evaluación de riesgos. En el contexto de las organizaciones de vigilancia y seguridad privada, estas tecnologías tienen el potencial de mejorar la capacidad de respuesta, reducir la incertidumbre operativa y fortalecer la toma de decisiones estratégicas. Para comprender mejor el enfoque de esta investigación, se profundiza en cinco conceptos fundamentales: gestión de riesgos en proyectos, Big Data, Inteligencia Artificial, toma de decisiones estratégicas y transformación digital en seguridad privada.

Gestión de riesgos en proyectos

La gestión de riesgos es un proceso sistemático que busca identificar, analizar y mitigar los efectos negativos de eventos inciertos que puedan afectar los objetivos de un proyecto. En proyectos del sector de vigilancia y seguridad privada, la gestión de riesgos adquiere un carácter prioritario debido a la alta exposición a amenazas físicas, tecnológicas, humanas y operativas.

De acuerdo con el Project Management Institute (2021), este proceso implica cinco pasos fundamentales: identificación de riesgos, análisis cualitativo y cuantitativo, planificación de respuestas, implementación de estrategias de mitigación y monitoreo constante. En el contexto de la seguridad privada, esto se traduce en el reconocimiento de amenazas como robos, intrusiones, fallas tecnológicas, ciberataques, entre otros, y en el desarrollo de planes para reducir su impacto.

Además, una gestión de riesgos eficaz permite asignar de forma más eficiente los recursos y priorizar acciones preventivas, lo que resulta en una operación más resiliente y adaptable ante incidentes imprevistos.

Big Data

Big Data se refiere al manejo y análisis de grandes volúmenes de datos que son generados de manera continua y a gran velocidad desde diversas fuentes: sensores, cámaras de vigilancia, sistemas de control de acceso, redes sociales, dispositivos móviles, entre otros. Esta tecnología permite descubrir patrones ocultos, correlaciones y tendencias que no serían perceptibles mediante métodos tradicionales de análisis.

En el ámbito de la seguridad privada, Big Data puede ser utilizado para crear modelos predictivos que anticipen riesgos, monitorear comportamientos inusuales en tiempo real y detectar zonas de alto riesgo mediante análisis geoespacial. Por ejemplo, al analizar datos históricos de incidentes, se puede identificar qué horarios o ubicaciones son más propensos a eventos delictivos y tomar decisiones preventivas con mayor precisión.

Mayer-Schönberger y Cukier (2013) sostienen que el valor de Big Data no solo está en la cantidad de información, sino en la capacidad de extraer conocimiento útil y accionable a partir de ella, lo que lo convierte en un recurso clave para la toma de decisiones estratégicas basadas en evidencia.

Inteligencia Artificial (IA)

La Inteligencia Artificial (IA) es un campo de la informática que busca desarrollar sistemas capaces de realizar tareas que requieren inteligencia humana, tales como el aprendizaje,

la percepción, la toma de decisiones y la resolución de problemas. Dentro de sus ramas se encuentran el aprendizaje automático (machine learning), el procesamiento de lenguaje natural y la visión por computador, entre otras.

En el sector de la seguridad privada, la IA se aplica, por ejemplo, en el reconocimiento facial para el control de acceso, la detección automática de comportamientos sospechosos mediante cámaras de vigilancia inteligentes, la predicción de patrones delictivos y la clasificación automática de incidentes según su nivel de riesgo.

Russell y Norvig (2020) argumentan que los agentes inteligentes pueden adaptar sus acciones según los datos recolectados del entorno, lo que les permite responder de manera proactiva ante amenazas emergentes. Esto representa una oportunidad para que las organizaciones de seguridad privada no solo reaccionen ante los riesgos, sino que los anticipen.

Toma de decisiones estratégicas

La toma de decisiones estratégicas consiste en seleccionar, de entre múltiples alternativas, aquella que permita alcanzar los objetivos organizacionales en el mediano y largo plazo. En entornos altamente volátiles como el de la seguridad privada, las decisiones estratégicas requieren de información precisa, actualizada y confiable.

Las tecnologías como Big Data e IA han transformado este proceso, al permitir simular escenarios futuros, analizar múltiples variables simultáneamente y generar recomendaciones basadas en modelos matemáticos y estadísticos. De esta forma, se incrementa la capacidad de las organizaciones para prever consecuencias, reducir incertidumbres y actuar con mayor agilidad frente a los cambios del entorno.

Mintzberg et al. (2005) afirman que la toma de decisiones estratégicas es un proceso no lineal que involucra intuición, análisis y aprendizaje organizacional. En este sentido, las tecnologías emergentes actúan como catalizadores que enriquecen la capacidad cognitiva de los líderes organizacionales.

Transformación digital en seguridad privada

La transformación digital se refiere a un proceso de cambio organizacional profundo, impulsado por la integración de tecnologías digitales en todos los niveles de la operación. No se trata únicamente de adoptar nuevas herramientas, sino de repensar procesos, modelos de negocio y estructuras operativas para adaptarse a las exigencias de la era digital.

En el sector de la seguridad privada, la transformación digital implica la implementación de tecnologías como drones, biometría, analítica de video, sensores inteligentes, sistemas integrados de gestión y plataformas basadas en la nube. Esto mejora la eficiencia operativa, reduce tiempos de respuesta y permite una gestión proactiva del riesgo.

Kane et al. (2015) argumentan que la transformación digital exitosa requiere una visión estratégica clara, liderazgo comprometido y una cultura organizacional abierta al cambio. En Bogotá, este proceso podría representar una oportunidad para modernizar las organizaciones de vigilancia y alinearlas con estándares internacionales de eficiencia y seguridad.

2.3 Marco normativo

La implementación de tecnologías emergentes como Big Data e Inteligencia Artificial en el sector de la vigilancia y seguridad privada debe enmarcarse en el cumplimiento de la normativa vigente en Colombia, la cual regula tanto la protección de datos personales como la

actividad de seguridad privada en sí misma. Este marco normativo establece los derechos fundamentales de los ciudadanos, las obligaciones de las empresas del sector y las condiciones para el uso de tecnologías digitales con fines estratégicos y operativos.

Constitución Política de Colombia 1991: Articulo 15 mediante el cual se establece el derecho que tienen las personas a conocer, actualizar y ratificar la información personal. (Constitución Política de Colombia, 1991, art. 15)

CONPES 3975 de 2019: Formula una política nacional para la transformación digital e inteligencia artificial. Esta política tiene como objetivo potenciar la generación de valor social y económico en el país a través del uso estratégico de tecnologías digitales en el sector público y el sector privado, para impulsar la productividad y favorecer el bienestar de los ciudadanos, así como generar los habilitadores transversales para la transformación digital sectorial, de manera que Colombia pueda aprovechar las oportunidades y enfrentar los retos relacionados con la Cuarta Revolución Industrial. (Departamento Nacional de Planeación, 2019)

Decreto 356 DE 1994: "Por el cual se expide el Estatuto de Vigilancia y Seguridad Privada" (Ministerio de Defensa Nacional, 1994)

Decreto 1979 de 2001: Por medio del cual se expide el manual de uniformes y equipos para el personal del servicio de vigilancia y seguridad privada. (Ministerio de Defensa Nacional, 2001)

Decreto 71 del 2002: Establece las normas y cuantías mínimas de patrimonio y Capital Social, que dicta que las empresas de vigilancia y seguridad privada deben mantener y acreditarse ante la Superintendencia de Vigilancia y Seguridad Privada. (Ministerio de Defensa Nacional, 2002)

Decreto 2355 de 2006: Por el cual se modifica la estructura de la Superintendencia de Vigilancia y Seguridad Privada, con el fin de mejorar los niveles de seguridad y confianza pública mediante la acción coordinada con las diferentes entidades y organismos estatales (Ministerio de Defensa Nacional, 2006)

Decreto 1377 de 2012: Reglamento aspectos relacionados con la titularidad del uso de la información para el tratamiento de sus datos personales. (Ministerio de Salud y Protección Social, 2012)

Ley 1266 de 2008: Por medio de la cual se dictan las disposiciones generales de habeas data. (Congreso de la República de Colombia, 2008)

Ley 1273 de 2009: Modifica el código penal y crea como bien jurídico tutelado la protección de la información y de los datos. (Congreso de Colombia, 2009)

Ley 1539 de 2012: "Por medio de la cual se implementa el certificado de aptitud psicofísica para el porte y tenencia de armas de fuego y se dictan otras disposiciones." (Congreso de Colombia, 2012)

Ley Estatutaria 1581 de 2012: "Por la cual se dictan disposiciones generales para la protección de datos personales." (Congreso de Colombia, 2012)

Ley 1801 de 2016: "Por la cual se expide el Código Nacional de Seguridad y Convivencia Ciudadana" (Ley 1801, 2016).

Ley 2197 de 2022: "Por medio de la cual se dictan normas tendientes al fortalecimiento de la seguridad ciudadana y se dictan otras disposiciones." (Congreso de Colombia, 2022).

Resolución 2852 de 2006: Por la cual se unifica el régimen de vigilancia y seguridad privada, estipulando que ambas entidades serán responsables de proporcionar o exigir al personal una capacitación y formación humana y técnica, de acuerdo con las modalidades del servicio y cargo que desempeñan, para así disminuir y prevenir las amenazas que afectan o puedan afectar la vida, la integridad personal o el tranquilo ejercicio de los legítimos derechos sobre los bienes de las personas que reciben su protección. (Superintendencia de Vigilancia y Seguridad Privada, 2006).

3 METODOLOGÍA

3.1 Enfoque y alcance de la investigación

La presente investigación se desarrolla bajo un enfoque cuantitativo, orientado a recolectar, analizar e interpretar datos numéricos que permitan describir la incidencia de los procesos de implementación de Big Data e Inteligencia Artificial en la gestión de riesgos en proyectos de organizaciones de vigilancia y seguridad privada. Este enfoque posibilita la identificación de patrones y tendencias que respalden la formulación de estrategias y recomendaciones prácticas para el sector.

En función de ello, el proceso metodológico se estructura en dos fases principales:

Análisis bibliométrico: Esta fase tiene como objetivo identificar las principales tendencias, autores, publicaciones y palabras clave asociadas a la implementación de Big Data e Inteligencia Artificial en la gestión de riesgos en el sector de vigilancia y seguridad privada. A través del uso de la base de datos ScienceDirect, se busca establecer el estado del arte, detectar

vacíos de investigación y reconocer oportunidades de desarrollo estratégico a nivel internacional que puedan ser aplicadas en el contexto colombiano.

Caracterización de empresas de vigilancia y seguridad privada en Bogotá, Colombia: En esta fase se pretende identificar cuántas empresas del sector, localizadas en la ciudad de Bogotá, han incorporado tecnologías como Big Data o Inteligencia Artificial en sus procesos de identificación, análisis y evaluación de riesgos. Para ello, se aplicará una encuesta estructurada que permitirá conocer el grado de adopción tecnológica y el uso específico de estas herramientas en sus proyectos actuales.

3.2 Población y muestra

3.2.1 Definición de la población

La población objeto de estudio está conformada por las empresas de vigilancia y seguridad privada legalmente constituidas y en operación en la ciudad de Bogotá, Colombia, que desarrollan o gestionan proyectos relacionados con la prestación de servicios de seguridad. Esta población incluye tanto empresas que ya han incorporado tecnologías emergentes como Big Data e Inteligencia Artificial en sus procesos de gestión de riesgos, como aquellas que aún no lo han hecho, pero tienen el potencial o el interés de hacerlo.

Según la Secretaría de Seguridad de Bogotá, “en la ciudad existen 472 empresas de vigilancia privada legalmente reconocidas, que emplean a más de 150.000 personas en esquemas de seguridad para propiedad horizontal, centros comerciales y establecimientos de comercio” (Alcaldía Mayor de Bogotá, 2023, párr. 2).

3.2.2 Cálculo y selección de la muestra

Mediante el uso de la herramienta virtual QuestionPro, se determinó el tamaño de la muestra, ya que esta plataforma cuenta con una calculadora integrada que aplica la fórmula estadística

Fórmula utilizada

Tamaño de la muestra: Z2 * (p) * (1-p) / c2

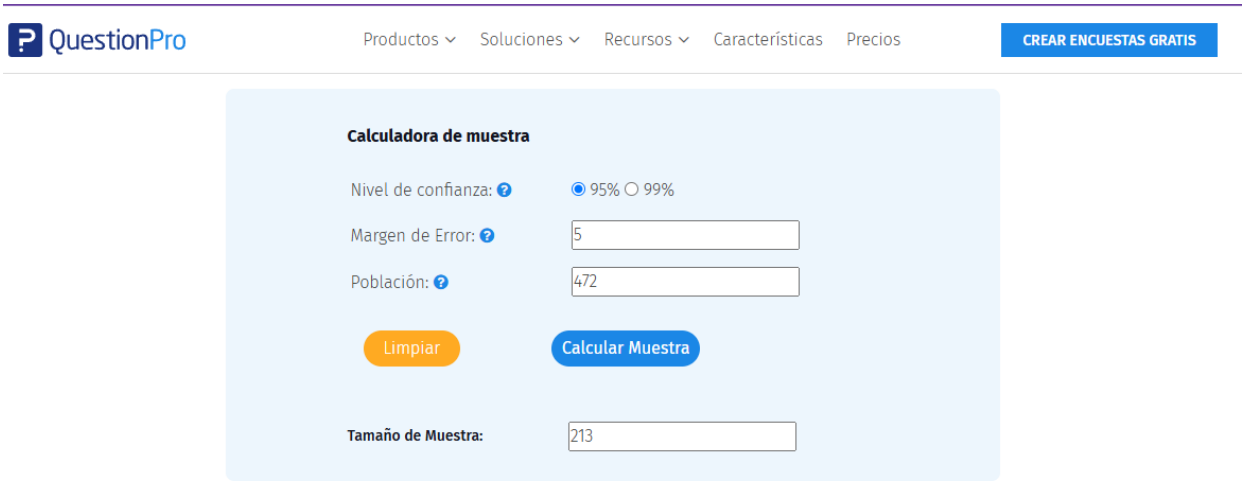
Donde:

Z = Nivel de confianza (1.96 para 95% o 2.5 para el 99%)

p = Proporción estimada (0.5)

c = Margen de error (0.4 = 4)

Figura 1. Cálculo de tamaño de muestra



Fuente: Software para encuestas Questionpro, 2025

De acuerdo con el análisis realizado mediante el software QuestionPro, se determinó que el tamaño de muestra estadísticamente adecuado es de 213 empresas. No obstante, considerando las condiciones del proyecto Nodo y el alcance específico de esta investigación, se llevará a cabo un análisis con una muestra de 30 empresas del sector de la vigilancia, seguridad privada y áreas afines. Esta selección tiene como propósito obtener información relevante y representativa que permita cumplir con los objetivos planteados, garantizando la viabilidad del estudio en términos de tiempo y recursos.

3.3 Instrumento(s)

Los instrumentos utilizados en esta investigación son, por un lado, una revisión sistemática de la literatura, que permite establecer el estado del arte sobre la implementación de Big Data e Inteligencia Artificial en la gestión de riesgos; y por otro, una encuesta aplicada a empresas del sector, orientada a identificar el nivel de madurez tecnológica en relación con el uso de estas herramientas en sus procesos de gestión de riesgos.

3.3.1 Revisión sistemática de la literatura

Consiste en el análisis de diversos documentos científicos, tales como revistas académicas, artículos y estudios especializados con la plataforma Sciencedirect, con el objetivo de elaborar una matriz de análisis bibliográfico que permita sistematizar la información recopilada. Esta matriz está estructurada en torno a las siguientes categorías:

Autores: Nombres de los autores.

Título del documento científico: Título del documento científico consultado.

Año de publicación del documento científico.

Tipo de documento: Artículo, revisión, artículo de conferencia, revistas, entre otros.

Objetivo del estudio: Propósito principal del documento.

Metodología utilizada: Tipo de enfoque utilizado.

Tecnologías abordadas: Mención específica a big data, inteligencia artificial u otras herramientas.

Principales hallazgos: Resultados o conclusiones relevantes del estudio.

Contribuciones al tema: Los aportes relevantes al proyecto.

3.3.2 Encuesta sobre nivel de madurez tecnológica

Para llevar a cabo la investigación, se aplicó una encuesta compuesta por 31 preguntas a una muestra de 30 empresas del sector de la vigilancia, seguridad privada y áreas afines. El instrumento fue diseñado con preguntas cerradas, empleando principalmente una escala tipo Likert de cinco niveles, con el propósito de medir las percepciones, el nivel de conocimiento y el grado de aplicación de tecnologías emergentes. El cuestionario se estructuró en cinco dimensiones temáticas, cada una orientada a abordar diferentes aspectos clave de la problemática investigada:

I. Modelo de negocio.

II. Clientes y proveedores.

III. Procesos de nivel táctico y operativo.

IV. Infraestructura y seguridad.

V. Estrategia y experiencia en industria 4.0

A continuación, se describen brevemente las dimensiones mencionadas:

Modelo de negocio: Examina el nivel de integración de la gestión de riesgos en el modelo de negocio, así como el conocimiento y uso de IA y Big Data en los procesos estratégicos.

Clientes y proveedores: Indaga sobre la relación con los stakeholders externos, su participación en la identificación de riesgos y la calidad de la información recabada durante las visitas técnicas.

Procesos de nivel táctico y operativo: Evalúa los procedimientos aplicados en campo para la recolección de datos y su efectividad para identificar y mitigar riesgos.

Infraestructura y seguridad: Analiza la disponibilidad de infraestructura tecnológica, el procesamiento de datos y las condiciones de ciberseguridad en el manejo de información sensible.

Estrategia y experiencia en Industria 4.0: Aborda la adopción de tecnologías emergentes y la implementación de soluciones basadas en IA y Big Data para la predicción y mitigación de riesgos en los proyectos.

Por otro lado, en el **Anexo 1** se presentan las preguntas incluidas en la encuesta aplicada para evaluar el nivel de madurez tecnológica de las empresas participantes en el marco de este proyecto.

3.4 Descripción de procedimientos

Con el objetivo de identificar los beneficios de la implementación de Big Data e Inteligencia Artificial en la gestión de riesgos en proyectos de organizaciones de vigilancia y seguridad privada en la ciudad de Bogotá, se diseñó un instrumento de encuesta estructurado. La muestra estuvo conformada por 30 empresas del sector, seleccionadas de manera estratégica con el fin de obtener información relevante, representativa y alineada con los objetivos del estudio.

Acercamiento: Se estableció contacto con las empresas del sector de vigilancia y seguridad privada previamente seleccionadas para conformar la muestra. Este acercamiento se realizó a través de correos electrónicos, llamadas telefónicas y redes institucionales, presentando brevemente los objetivos del estudio, la relevancia del tema y la importancia de su participación voluntaria. También se garantizó la confidencialidad de la información proporcionada.

Instrucciones y dinámica: Se enviaron instrucciones claras y precisas sobre la dinámica de la encuesta. Se explicó que el cuestionario sería autoadministrado, con una duración aproximada de 10 a 15 minutos, y que estaba compuesto por preguntas cerradas con escalas tipo Likert. Asimismo, se ofreció soporte técnico en caso de dudas durante su diligenciamiento.

Entrega de la encuesta: La encuesta fue distribuida de forma virtual a través de Microsoft forms mediante un enlace único enviado a cada empresa participante. Este formato facilitó el acceso desde diferentes dispositivos y permitió a los participantes responder a su ritmo, sin restricción horaria, dentro del plazo establecido.

Recolección de datos: Durante el período de recolección, se realizó un seguimiento activo mediante recordatorios periódicos, con el fin de incentivar la participación y lograr una tasa de respuesta adecuada. Una vez cerrado el formulario, se procedió a revisar las respuestas

recibidas, verificando la completitud y validez de los registros. Se eliminaron duplicados o formularios incompletos para asegurar la calidad de los datos.

Análisis de información: Una vez finalizada la recolección, los datos obtenidos fueron exportados a Microsoft Excel para su organización, depuración y análisis. Se utilizarán herramientas de análisis descriptivo para identificar patrones y tendencias clave en relación con el uso, conocimiento y beneficios de Big Data e Inteligencia Artificial en la gestión de riesgos para proyectos de organizaciones del sector de la seguridad privada.

Los resultados se presentarán en forma de estadísticas porcentuales, lo que permitirá interpretar de manera más comprensible la distribución de respuestas entre las distintas categorías evaluadas.

Para la visualización y análisis de la información se emplearán los siguientes elementos:

Tablas de frecuencia en porcentaje: cada tabla mostrará la distribución relativa de respuestas por ítem, destacando el valor más representativo o frecuente. Esto permitirá identificar con claridad las percepciones predominantes, el grado de conocimiento o uso de tecnologías emergentes, y las principales necesidades o barreras identificadas por las empresas participantes.

Gráficas de barras: se utilizarán para representar visualmente los porcentajes obtenidos en cada categoría. Estas gráficas facilitarán la comparación entre variables y ayudarán a interpretar tendencias clave en relación con la implementación de Big Data e Inteligencia Artificial en la gestión de riesgos.

3.4.1 Revisión de literatura

Para la revisión de la literatura, se utilizó la base de datos bibliográfica ScienceDirect con el objetivo de identificar las publicaciones más relevantes relacionadas con el tema de investigación. Este proceso se estructuró en tres etapas fundamentales: Formulación de las preguntas centrales de la investigación, búsqueda de información en la plataforma ScienceDirect y realización de un análisis bibliométrico.

3.4.1.1 Formulación de las preguntas centrales de la investigación.

Con el objetivo de lograr una mayor claridad sobre el tema y asegurar que la revisión de la literatura se mantenga alineada con el propósito del estudio, evitando la dispersión temática y garantizando un abordaje coherente y sistemático del problema de investigación, se formularon las siguientes preguntas:

¿Cuáles son las principales tecnologías emergentes, especialmente Big Data e Inteligencia Artificial, aplicadas actualmente en la gestión de riesgos en proyectos organizacionales?, ¿Qué beneficios y desafíos se han identificado en la incorporación de Big Data e Inteligencia Artificial en procesos de toma de decisiones estratégicas dentro del sector de vigilancia y seguridad privada?, ¿Qué modelos o enfoques teóricos existen para la identificación, análisis y evaluación de riesgos en proyectos, y cómo pueden integrarse con tecnologías emergentes?, ¿Cómo se ha implementado el uso de Big Data e Inteligencia Artificial en la gestión de riesgos en sectores similares al de la seguridad privada, y qué aprendizajes pueden aplicarse al contexto de organizaciones en Bogotá?, y ¿Qué recomendaciones han sido propuestas en la literatura científica para facilitar la adopción tecnológica en organizaciones con estructuras operativas tradicionales, como las de seguridad privada?

3.4.1.2 Búsqueda de información en la plataforma ScienceDirect

Mediante la siguiente ecuación de búsqueda: ("Big Data" OR "data analysis") AND ("Artificial Intelligence" OR "AI") AND ("risk management" OR "risk assessment" OR "risk analysis") AND ("private security" OR "security services")

Periodo: 2018 a 2025

Tipos documentos: Artículos científicos, ponencias en conferencias, revisiones, libros.

3.4.1.3 Análisis bibliométrico

Para el análisis bibliométrico se realizó una matriz en la que se clasificaron los siguientes aspectos: Autores, título del documento científico, año de publicación del documento científico, tipo de documento, objetivo del estudio, metodología utilizada, tecnologías abordadas, principales hallazgos y contribuciones al tema.

3.4.2 Encuesta de medición de nivel de madurez tecnológico

3.4.2.1 Preguntas de modelo de negocio y producto – Nivel estratégico

En esta sección, las preguntas están orientadas a identificar el nivel de transformación digital en el modelo de negocio, así como su implementación en los servicios ofrecidos por la organización. Por ejemplo:

- Cuenta con estrategia de transformación digital formulada desde la alta dirección.
- Alguno de sus productos integra tecnologías emergentes (inteligencia artificial, big data, o ciencia de datos).

- Cuenta con claridad en los procesos y protocolos para llevar a cabo proyectos con alta incorporación tecnológica.
- Reconoce los conceptos de tecnologías emergentes (inteligencia artificial, big data, y data science).

3.4.2.2 Preguntas de clientes y proveedores – Stakeholders

En esta sección se identificará el nivel de apropiación de las tecnologías habilitadoras de la transformación digital en su relación con clientes y proveedores. Por ejemplo:

- Implementa sistemas de información (herramientas software) para la gestión de proveedores.
- Implementa sistemas de información (herramientas software) para la gestión de clientes.
- Cuenta con la planificación y dirección de la cadena de suministros desde los clientes hasta los proveedores.

3.4.2.3 Preguntas de procesos – Nivel táctico y operativo.

En esta sección se identificará el nivel de apropiación de las tecnologías habilitadoras de la transformación digital en su proceso principal. Por ejemplo:

- ¿Cuál de las siguientes tecnologías utiliza en su organización?
- De acuerdo con las máquinas y equipos de su organización. ¿Cuál es el grado de implementación de las siguientes funcionalidades?

3.4.2.4 Preguntas de infraestructura y seguridad

En esta sección se identificará el nivel de apropiación de las tecnologías habilitadoras de la transformación digital en su infraestructura y gestión de la seguridad. Por ejemplo:

- ¿La organización, ya está utilizando servicios en la nube?

- ¿Cómo está organizada su gestión en tecnologías de la información – TI?

3.4.2.5 Preguntas de estrategia y experiencia en industria 4.0

En esta sección se identificará el nivel de conocimiento, adecuación y proyección de uso de las tecnologías habilitadoras de la industria 4.0. Por ejemplo:

- ¿Cómo realiza la organización el registro de la información generada por los procesos (producción, comercial, calidad, mantenimiento, administración, etc.)?
- ¿Dispone de alguna persona en la organización responsable de la transformación digital?
- ¿Cómo evalúa las capacidades de sus empleados en relación con los requisitos futuros de la industria 4?

3.5 Análisis de información

El análisis de la información se llevó a cabo en dos etapas. En la primera etapa, correspondiente a la recolección de los datos, se realizó un proceso de limpieza con el objetivo de eliminar duplicidades, inconsistencias y datos irrelevantes. Posteriormente, los datos fueron organizados para facilitar una comprensión estructurada y ordenada de la información, lo que permitió optimizar su análisis.

En la segunda etapa, se efectuó la codificación de los datos, con el propósito de identificar patrones, tendencias, relaciones conceptuales y elementos clave.

3.5.1 Recolección de datos

En la revisión de la literatura se consultaron diversos documentos científicos relevantes para el desarrollo de la investigación. A través de la base de datos ScienceDirect, se lograron recopilar 180 artículos publicados por distintos autores en el periodo comprendido entre 2018 y 2024. Durante el proceso de recopilación se incluyeron distintos tipos de fuentes, tales como ponencias, libros, revisiones y artículos científicos.

Posteriormente, se elaboró una matriz con el propósito de organizar la información, filtrar los contenidos irrelevantes y facilitar su análisis. Las categorías consideradas en dicha matriz fueron: nombre del autor o autores, título del documento, año de publicación, tipo de documento, objetivo del estudio, metodología empleada, tecnologías abordadas, principales hallazgos y contribución al tema de investigación.

Por otro lado, se aplicó una encuesta con el objetivo de evaluar el nivel de madurez tecnológica en la gestión de proyectos en distintos sectores de la economía. Se recopilaron aproximadamente 232 respuestas, de las cuales 30 correspondían específicamente al sector de vigilancia y seguridad, así como a sectores afines. La recolección de datos se llevó a cabo a través de la plataforma Microsoft Forms, y posteriormente la información fue descargada en formato Excel para su organización y sistematización.

Gracias a este proceso, fue posible realizar un análisis más preciso, orientado a comprender los niveles de adopción tecnológica presentes en las organizaciones de este sector, e identificar tendencias y oportunidades de mejora en la gestión de sus proyectos.

3.5.2 Codificación de datos

Debido al manejo de grandes volúmenes de datos y la necesidad de un acceso ágil y eficiente a los mismos, se utilizó la plataforma JASP para analizar la información obtenida en la encuesta sobre el nivel de madurez tecnológica en la gestión de proyectos.

JASP fue seleccionada por su interfaz intuitiva, que facilita el análisis estadístico incluso para usuarios con poca experiencia en software estadístico. Además, ofrece una amplia gama de pruebas estadísticas tanto descriptivas como inferenciales, permite visualizar los resultados mediante gráficos claros y personalizables, y proporciona informes automáticos con interpretación de los datos. Gracias a estas características, JASP permitió realizar un análisis riguroso, eficiente y visualmente comprensible de los resultados, contribuyendo así a obtener conclusiones más precisas y fundamentadas.

Importación de los datos: Una vez que la matriz de datos (respuestas) de la encuesta sobre el nivel de madurez tecnológica en la gestión de proyectos estuvo debidamente organizada en Excel, se procedió a importar la información a la plataforma JASP para su análisis. Este software permite una integración sencilla con archivos en formato Excel, reconociendo automáticamente las variables y facilitando su tratamiento estadístico. La importación se realizó de manera rápida y eficiente, permitiendo visualizar los datos dentro de la interfaz de JASP y verificar que las variables fueran interpretadas correctamente.

Transformación y codificación: Se asignaron códigos numéricos a las respuestas seleccionables de la encuesta con el fin de facilitar su análisis cuantitativo. Por ejemplo, las opciones de respuesta fueron: “Nulo”, “Existe iniciativa”, “En desarrollo”, “En implementación” y “En acción”. Estas fueron categorizadas de la siguiente manera: “Nulo” = 1, “Existe iniciativa” = 2, “En desarrollo” = 3, “En implementación” = 4 y “En acción” = 5.

Esta codificación permitió transformar las respuestas cualitativas en datos cuantitativos, lo cual facilitó su procesamiento estadístico y permitió realizar un análisis alineado con el enfoque de la investigación.

Validación de los datos: Las respuestas codificadas serán validadas a través de la plataforma JASP, con el objetivo de garantizar que la estructura de los datos sea correcta y esté adecuadamente relacionada con las variables correspondientes. Además, la plataforma permite identificar y corregir posibles inconsistencias, lo que contribuye a evitar errores en el análisis y asegura la fiabilidad de los resultados obtenidos.

3.6 Consideraciones éticas

3.6.1 Análisis de consideraciones éticas

La presente investigación se rige por principios éticos fundamentales que garantizan el respeto, la integridad y la confidencialidad de la información obtenida durante su desarrollo. Dado que el estudio involucra la recopilación y análisis de datos provenientes de organizaciones de vigilancia y seguridad privada en Bogotá, Colombia, se adoptarán medidas éticas rigurosas en cada etapa del proceso investigativo.

En primer lugar, toda participación de personas u organizaciones será voluntaria, mediada por un consentimiento informado claro, en el cual se explicará el propósito del estudio, la naturaleza de la información que se recolectará, el uso previsto de los datos y el derecho a retirarse en cualquier momento sin consecuencia alguna. Este consentimiento será otorgado por escrito, en formato digital (formulario de microsoft forms), antes de iniciar el diligenciamiento de la encuesta.

Se garantizará la confidencialidad de los datos personales e institucionales, asegurando que la información recopilada no será utilizada para fines distintos a los de esta investigación y será tratada de forma anónima en los resultados y publicaciones, evitando la identificación de personas u organizaciones específicas. Asimismo, los datos serán almacenados de manera segura, protegidos mediante mecanismos de cifrado y acceso restringido únicamente al equipo investigador. Además, se evitará cualquier tipo de conflicto de interés y se promoverá una relación de respeto y transparencia con todas las partes involucradas. El estudio no buscará generar juicios de valor sobre el estado actual de implementación tecnológica en las organizaciones, sino identificar oportunidades de mejora a partir de un análisis objetivo y propositivo. Finalmente, esta investigación se acoge a las normativas éticas nacionales e internacionales vigentes, como la Ley 1581 de 2012 sobre Protección de Datos Personales en Colombia.

3.6.2 Instrumentos de aceptación y autorización

La encuesta se aplicará a través de la plataforma Microsoft Forms, la cual incluirá una declaración inicial de consentimiento informado. Esta declaración aparecerá al comienzo del

formulario e incluirá la siguiente pregunta:

"¿Está de acuerdo con la declaración inicial y desea continuar con la encuesta?"

Los participantes podrán elegir entre dos opciones de respuesta:

1. Sí, autorizo y deseo continuar con la encuesta.
2. No autorizo y no deseo participar.

Solo quienes seleccionen la primera opción podrán acceder al contenido de la encuesta, garantizando así que la participación sea voluntaria y esté mediada por un consentimiento informado claro. Para más información puede dirigirse al **Anexo 2.**

4 HIPÓTESIS

La incorporación de tecnologías emergentes, específicamente Big Data e Inteligencia Artificial, en los procesos de gestión de riesgos en proyectos del sector de vigilancia y seguridad privada en Bogotá, permite una identificación más oportuna de amenazas, un análisis predictivo más preciso y una evaluación más integral de los riesgos operativos, estratégicos y tecnológicos. Esta implementación tecnológica contribuye a fortalecer la capacidad analítica de las organizaciones, optimizando la toma de decisiones estratégicas mediante el uso de datos en tiempo real, patrones de comportamiento y modelos de simulación, lo cual se traduce en una mayor eficiencia operativa, capacidad de respuesta y anticipación frente a eventos críticos.

4.1 Las variables

4.1.1 Variable(s) independiente(s)

La variable independiente en esta investigación es la implementación de tecnologías emergentes, específicamente Inteligencia Artificial y Big Data, en la gestión de riesgos en proyectos del sector de vigilancia y seguridad privada. Estas tecnologías tienen el potencial de fortalecer la capacidad analítica de las organizaciones, facilitando una identificación más precisa de riesgos, así como la optimización de los procesos de análisis y evaluación. En consecuencia, su adecuada implementación contribuye a mejorar la toma de decisiones estratégicas dentro del sector.

4.1.2 Variable(s) dependiente(s)

Las variables dependientes de esta investigación se enfocan en dos aspectos clave derivados de la hipótesis planteada:

Gestión de riesgos: A través del uso de tecnologías emergentes como la Inteligencia Artificial y el Big Data, se busca mejorar la identificación, clasificación y evaluación de los riesgos operativos y tecnológicos. Estas tecnologías permiten una gestión más precisa, proactiva y predictiva, al facilitar el análisis de grandes volúmenes de datos y la detección temprana de posibles amenazas.

Toma de decisiones estratégicas: La integración de Inteligencia Artificial y Big Data aporta una mayor capacidad analítica para la toma de decisiones estratégicas, al permitir el acceso a datos en tiempo real, el reconocimiento de patrones de comportamiento y la utilización de modelos de simulación. Esto contribuye a mejorar la capacidad de respuesta, anticipar incidentes críticos y optimizar la eficiencia operativa dentro de los proyectos de vigilancia y seguridad privada.

Capacidad analítica organizacional: El uso de Big Data e Inteligencia Artificial fortalece la capacidad analítica de las organizaciones, permitiéndoles procesar grandes volúmenes de información, identificar patrones relevantes y generar conocimiento accionable. Esta capacidad es fundamental para traducir los datos en decisiones informadas. Medir esta variable permite verificar si las empresas no solo adoptan tecnologías, sino que además desarrollan las competencias necesarias para aprovechar su potencial analítico, lo cual es determinante para lograr una gestión de riesgos eficiente y una toma de decisiones estratégicas basada en evidencia.

Eficiencia operativa: Las tecnologías emergentes no solo mejoran la identificación de riesgos, sino que también optimizan la ejecución operativa al reducir tiempos, minimizar errores y mejorar el uso de los recursos. Además, esta variable permite identificar si la transformación digital tiene efectos tangibles en el rendimiento de las actividades diarias, más allá de la toma de decisiones estratégicas. Por tanto, constituye una medida clave de éxito organizacional desde la perspectiva funcional y productiva.

Capacidad de respuesta y anticipación frente a eventos críticos: la incorporación de Big Data e Inteligencia Artificial permite detectar amenazas de manera temprana y reaccionar de forma más eficaz, reduciendo así la exposición a eventos disruptivos. Esta variable se orienta a medir no solo la velocidad con la que se responde ante un incidente, sino también la capacidad preventiva de las herramientas tecnológicas implementadas. Evaluarla permite comprobar si efectivamente se ha logrado fortalecer la resiliencia operativa del sector de vigilancia y seguridad privada frente a incidentes críticos.

5 RESULTADOS

5.1 Presentación de resultados

Tabla 1. MATRIZ DE ANÁLISIS BIBLIOGRÁFICO

Autores	Título	Año	Tipo de documento	Objetivo	Metodología	Tecnología abordada	Principales hallazgos	Contribución al proyecto
Ullah & Babar	Architectural Tactics for Big Data Cybersecurity Analytic Systems	2018	Revisión sistemática (arXiv)	Identificar tácticas arquitectónicas en sistemas analíticos de ciberseguridad con Big Data	Revisión SLR de 74 estudios	Big Data analytics	Define 17 tácticas clave (performance, seguridad, usabilidad)	Sirve como guía para diseñar infraestructuras robustas en vigilancia.
Zolanvari et al.	Machine Learning Based Network Vulnerability Analysis of IIoT	2019	Estudio de caso (arXiv)	Analizar vulnerabilidades en IIoT mediante ML	Implementación en testbed + ML	Machine Learning, Big Data	Detecta ataques (SQLi, backdoors) con alta efectividad	Evidencia práctica de detección automática de riesgos en redes industriales.
Salo, Injadat et al.	Data Mining with Big Data in Intrusion Detection Systems	2020	Revisión SLR	Explorar técnicas de data mining en IDS en entorno Big Data	Revisión sistemática	Big Data, data mining, IDS	Identifica 17 técnicas dominantes en detección en tiempo real	Guía soporte para selección de herramientas tecnológicas en vigilancia.
González, Pérez & Martínez	Big Data y gestión del riesgo en pymes de seguridad	2020	Artículo académico	Medir el impacto de Big Data en riesgos operativos de pymes	Cuantitativo: encuesta	Big Data	68 % de mejora en identificación de riesgos operacionales	Evidencia positiva sobre adopción gradual en empresas pequeñas.
Radanliev et al.	Design of a dynamic … predictive cyber risk analytics … IoT edge	2020	Estudio teórico (arXiv)	Diseñar sistema de IA/ML para riesgo cibernético en entornos extremos como IoT en el borde (arxiv.org)	Revisión y diseño conceptual	IA, ML, edge computing, IoT	Propone motor cognitivo en el borde para auto-detección de anomalías.	Sienta base para arquitecturas de riesgo en redes de seguridad basadas en IA.
Aguilar Rivera	Vigilancia con IA y Big Data: retos y oportunidades …	2021	Académico	Evaluar límites éticos y normativos de IA/Big Data en vigilancia	Revisión documental & normativo	IA, Big Data	Identifica tensiones entre eficacia y privacidad	Ayuda a diseñar recomendaciones ético-legales en vigilancia privada.

Silva, Gómez & Torres	Aplicación de IA en vigilancia urbana: un estudio latinoamericano	2021	Estudio de campo	Explorar adopción de IA en seguridad urbana en Latinoamérica	Entrevistas + análisis cuali.	IA, visión por computador	Percepción positiva hacia modelado predictivo	Proporciona evidencias contextuales aplicables a Bogotá.
Ullah & Babar	On the Scalability of Big Data Cyber Security Analytics Systems	2021	Artículo técnico (arXiv)	Evaluar escalabilidad de sistemas Big Data para ciberseguridad	Experimental con Spark sobre clusters	Big Data analytics, Apache Spark	SCALER mejora escalabilidad en un 20.8 % respecto al ajuste estándar	Aporta directrices para implementación eficaz y escalable de análisis en tiempo real en seguridad.
Leenen & Meyer	Artificial Intelligence and Big Data Analytics in Support of Cyber Defense	2021	Capítulo de libro (IGI)	Revisar cómo IA y Big Data apoyan la defensa cibernética	Revisión de literatura	IA, Big Data analytics, defense	Documenta casos de uso e identifica ventajas/desafíos operativos	Marco conceptual para integrar tecnología emergente en estrategias defensivas.
Kaur, Sharma & Mittal	Artificial intelligence approaches and mechanisms for big data analytics: a systematic study	2021	Artículo (PMC)	Evaluar modelos IA para reducir carga de datos y optimizar redes de video	Estudio sistémico y comparativo	IA, Big Data, ML	Modelo eficiente reduce carga y mantiene calidad	Aplica a optimización del procesamiento de video en vigilancia.
Zhang, Chan, Yan et al.	Towards risk-aware AI and ML systems: An overview	2022	Revisión	Sistematizar riesgos en sistemas de IA/ML	Revisión sistemática	IA, ML	Clasifica riesgos (datos, modelos, seguridad); propone marco proactivo	Marco útil para incorporar gestión de riesgos en proyectos de seguridad con IA.
Lee, Kim et al.	Big Data analytics in security risk evaluation	2022	Artículo académico	Evaluar uso de Big Data para anuencias de riesgo estratégico	Cuantitativo experimental	Big Data, análisis predictivo	Mejora del 25 % en precisión de clasificación de riesgo	Apllicable para mejorar sistemas de alertas tempranas.
Richards, Young	Ethical implications of AI surveillance	2022	Revisión documental	Explorar implicaciones éticas y legales del uso de IA en vigilancia	Revisión documental	IA	Señala riesgo de sesgos y la necesidad de transparencia	Resalta recomendaciones que deben tenerse en cuenta en Bogotá.
Sarker et al.	Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity	2022	Artículo académico	Analizar técnicas ML (clustering, outliers) en ciberseguridad	Revisión técnica	Machine Learning, clustering	Clustering detecta anomalías, ofrece rutas futuras	Muestra cómo estructurar detección automatizada basada en patrones en vigilancia.

Smith, Johnson	AI-based Risk Modeling in Private Security Projects	2023	Estudio de caso	Modelar riesgos operativos mediante IA en empresas de seguridad privada	Estudio de caso + análisis ML	IA, Machine Learning	Reducción de 30 % en eventos inesperados	Demuestra resultados operativos claros en contexto similar al de Bogotá.
Patel, Shah	Real-time video analytics for threat detection	2023	Artículo de conferencia	Analizar desempeño de algoritmos de video en detección de amenazas	Experimental + métricas de rendimiento	IA, Deep Learning	Detecta amenazas con precisión de 92 % en tiempo real	Útil para diseñar modelos en entornos reales de videovigilancia.
van Noordt et al.	The Role of AI Technology in Predictive Risk Assessment for Business Continuity (Grecia)	2023	Estudio de caso (MDPI)	Estudiar uso de NLP en evaluación predictiva de riesgos para continuidad empresarial	Cuantitativo (encuesta + regresión)	IA (NLP), Big Data	> 80 % reconoce beneficio del NLP para acelerar y mejorar exactitud del riesgo.	Ilustra cómo manejar grandes datos no estructurados en procesos de riesgo.
Danish, et al.	Enhancing Cyber Security through Predictive Analytics…	2024	Cuantitativo	Evaluar el impacto del analytics predictivo en detección de amenazas	Cuantitativo (regresión)	Big Data, analytics predictivo	Mejora en tiempos de respuesta frente a métodos tradicionales	Evidencia empírica aplicable para gestión operativa de riesgos.
Celis	AI-Driven Predictive Analytics for Cybersecurity	2024	Artículo web informe	Explorar uso de IA predictiva en ciberseguridad	Análisis descriptivo	IA predictivo, Big Data analytics	Destaca anticipación de amenazas y priorización de recursos	Respalda el uso de IA para priorizar riesgos y recursos en proyectos de seguridad.
Bhargava & Maddiredy	Real-Time Data Analytics with AI: Improving Security Event…	2024	Artículo académico (sitio)	Explorar framework de IA para monitoreo de eventos de seguridad en tiempo real	Análisis de logs y tráfico de red	IA, Big Data, ML	Implementa detección de anomalías en red y responde automáticamente a incidentes.	Presenta aplicación directa de IA en monitoreo continuo de eventos de seguridad.

Fuente: Elaboración propia (2025). Basada en consulta bibliográfica en la plataforma Sciencedirect.

En el marco de la presente investigación, se llevó a cabo un análisis bibliográfico exhaustivo con el propósito de identificar y sistematizar conocimientos relevantes sobre la implementación de tecnologías emergentes, particularmente Big Data e Inteligencia Artificial, en

la gestión de riesgos. La matriz se construyó a partir de la revisión de veinte documentos científicos publicados entre 2018 y 2025, consultados principalmente en la base de datos ScienceDirect.

A partir del análisis, se identificaron tres ejes temáticos predominantes. El primero corresponde a los estudios centrados en la gestión de riesgos y la ciberseguridad, en los que se examina cómo las tecnologías emergentes permiten identificar y mitigar vulnerabilidades en tiempo real (Ullah & Babar, 2018; Radanliev et al., 2020; Sarker et al., 2022; Bhargava & Maddireddy, 2024). El segundo eje temático abarca las aplicaciones específicas en entornos de seguridad física y vigilancia urbana, especialmente en lo relacionado con videovigilancia, análisis de patrones y sistemas de monitoreo predictivo (Silva, Gómez & Torres, 2021; Smith & Johnson, 2023; Patel & Shah, 2023). Finalmente, el tercer eje aborda los aspectos éticos, legales y normativos del uso de IA y Big Data, destacando las tensiones entre eficacia operativa y protección de la privacidad (Aguilar Rivera, 2021; Richards & Young, 2022).

En cuanto a las metodologías utilizadas en los estudios, se observa un equilibrio entre enfoques teóricos y aplicados. Las revisiones sistemáticas y documentales (por ejemplo, las de Ullah & Babar, 2018; Salo et al., 2020; Zhang et al., 2022) ofrecen una visión estructurada del estado del arte, mientras que los estudios de caso y los diseños cuantitativos (Smith & Johnson, 2023; Danish et al., 2024; van Noordt et al., 2023) proporcionan evidencia empírica sobre los beneficios de estas tecnologías en entornos reales. Asimismo, investigaciones experimentales como la de Patel & Shah (2023) permiten evaluar métricas de rendimiento y precisión en la detección de amenazas, lo cual es clave para validar el potencial operativo de las soluciones tecnológicas.

En lo que respecta a las tecnologías abordadas, todas las investigaciones analizadas coinciden en el uso estratégico de Big Data e Inteligencia Artificial, siendo estas las herramientas centrales para el análisis predictivo, la automatización de procesos y la toma de decisiones basadas en datos. En particular, técnicas como Machine Learning, Deep Learning, procesamiento de lenguaje natural (NLP) y clustering permiten desarrollar modelos avanzados para la detección de amenazas, la clasificación de riesgos y la predicción de eventos críticos. Además, se destacan tecnologías complementarias como la computación en el borde (edge computing), sistemas de detección de intrusos (IDS), y arquitecturas cognitivas que fortalecen la eficiencia, escalabilidad y adaptabilidad de las soluciones.

Los hallazgos principales de la matriz bibliográfica refuerzan la hipótesis central del proyecto. Se evidencian mejoras significativas en la identificación temprana de amenazas, la evaluación integral de riesgos y la optimización de la toma de decisiones estratégicas mediante el uso de tecnologías emergentes. Por ejemplo, estudios como los de Danish et al. (2024) y Salo et al. (2020) muestran incrementos en la precisión de detección y reducción de tiempos de respuesta. Otros, como los de Ullah & Babar (2021) y Leenen & Meyer (2021), ofrecen directrices arquitectónicas para garantizar la escalabilidad y robustez de las soluciones tecnológicas. En el plano ético y normativo, los estudios de Aguilar Rivera (2021) y Richards & Young (2022) hacen hincapié en la importancia de considerar la transparencia algorítmica, el consentimiento informado y la protección de datos personales en la aplicación de estas tecnologías en el sector de la seguridad.

Asimismo, algunos trabajos (Silva, Gómez & Torres, 2021; Smith & Johnson, 2023) presentan experiencias contextualizadas en países de América Latina, lo que fortalece la validez externa del análisis y su aplicabilidad al caso específico de Bogotá. Estos estudios permiten

comprender cómo las organizaciones del sector pueden adoptar tecnologías emergentes de manera progresiva, considerando tanto las limitaciones de infraestructura como los retos normativos y sociales del entorno local.

Por otro lado, los resultados obtenidos en la encuesta, se llevó a cabo un análisis de los datos correspondientes a 30 empresas del sector de la vigilancia, la seguridad privada y áreas afines, con el propósito de recopilar información significativa que aporte al desarrollo de la presente investigación. Dicho análisis tiene como objetivo evaluar el nivel actual de madurez tecnológica en la adopción de soluciones basadas en inteligencia artificial y big data para la gestión de riesgos en los proyectos de estas organizaciones.

Tabla 2. MODELO DE NEGOCIO Y PRODUCTO – Nivel estratégico.

I. MODELO DE NEGOCIO					
Preguntas	**Nulo**	**En desarrollo**	**En acción**	**Existe la iniciativa**	**En implementación**
Cuenta con estrategia de transformación digital formulada desde la alta dirección.	10%	33%	33%	13%	10%
Cuenta con indicadores para medir nivel de la transformación digital.	13%	17%	37%	20%	13%
Tiene interés en la capacitación del talento humano en transformación digital.	7%	23%	27%	23%	20%
Alguno de sus productos integra tecnologías emergentes (Inteligencia artificial, big data o ciencia de datos).	17%	13%	30%	17%	23%
Reconoce importancia que tiene el uso y análisis de información.	0%	13%	53%	17%	17%
Identifica que el desarrollo y la innovación tecnológica juega un papel importante.	3%	30%	40%	10%	17%
Cuenta con claridad en los procesos y protocolos para llevar a cabo proyectos con alta incorporación tecnológica.	10%	20%	33%	13%	23%
Reconoce los conceptos de tecnologías emergentes (Inteligencia artificial, Big-Data y Data Science).	7%	7%	43%	20%	23%

Fuente: Elaboración propia (2025). Basada en preguntas de encuesta nivel de madurez (apropiación) en la gestión de proyectos.

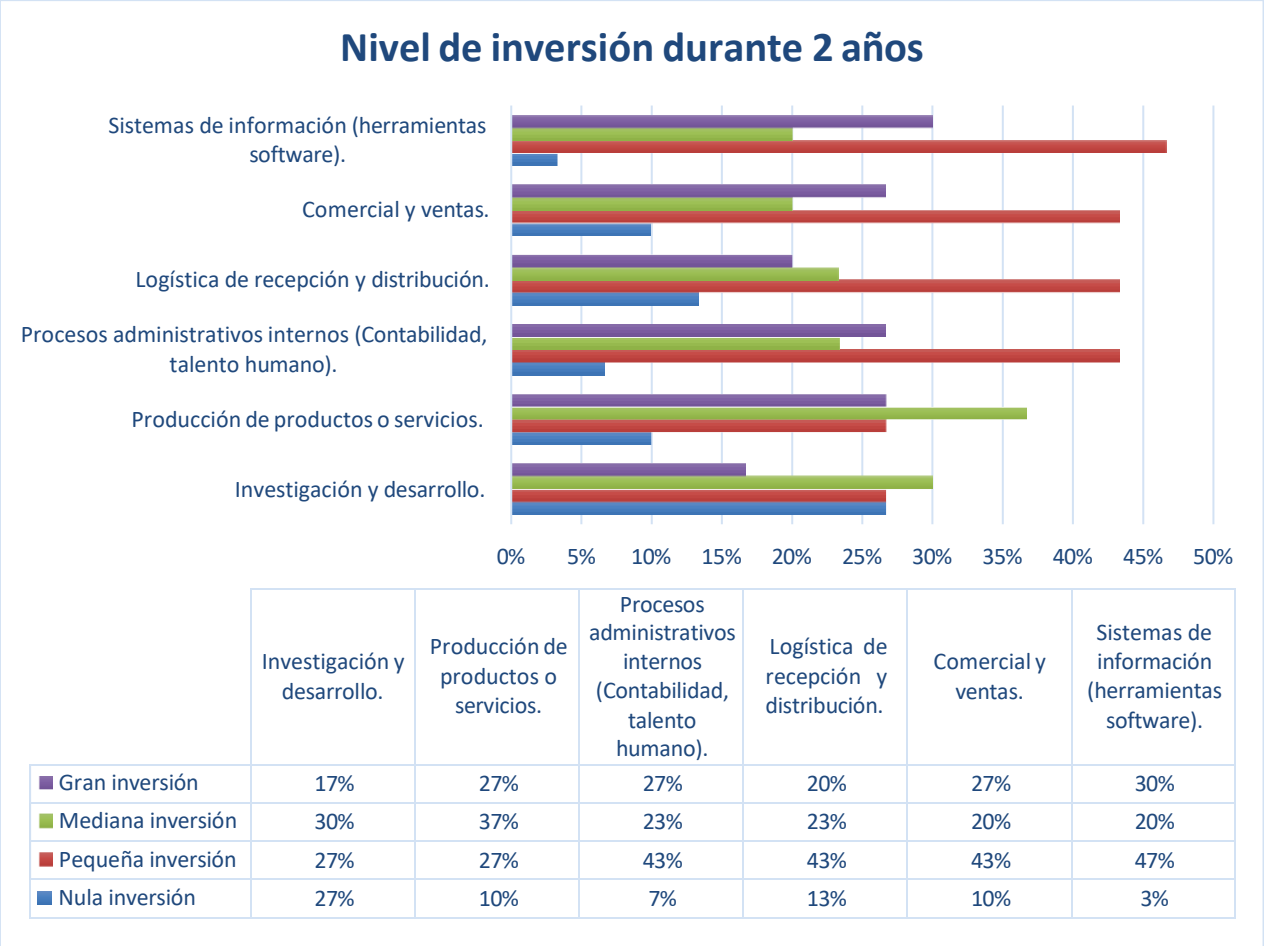
Los resultados muestran que el 33% de las organizaciones cuenta con una estrategia de transformación digital formulada desde la alta dirección, lo cual evidencia una intención clara desde los niveles estratégicos. No obstante, solo el 10% se encuentra en etapa de implementación, lo que sugiere una brecha significativa entre la planificación y la ejecución de dichas estrategias. En la misma línea, el 37% de las empresas ha definido indicadores para medir el nivel de transformación digital, lo que indica un interés por monitorear el avance, aunque este esfuerzo no siempre se refleja en acciones concretas.

Respecto al talento humano, un 27% de las organizaciones ha manifestado estar en acción en cuanto a la capacitación en temas de transformación digital. Este porcentaje, aunque positivo, indica que aún existe una necesidad considerable de fortalecer las competencias internas para facilitar la apropiación de tecnologías emergentes. En relación con la oferta de productos, el 30% de las empresas señala que alguno de sus servicios integra tecnologías como inteligencia artificial, big data o ciencia de datos, lo que revela una baja penetración de estas herramientas en su portafolio actual, limitando así su aplicación efectiva en procesos de gestión de riesgos.

Uno de los hallazgos más relevantes del análisis es que el 53% de las organizaciones reconoce la importancia del uso y análisis de la información, reflejando una comprensión sólida sobre el valor estratégico de los datos en la toma de decisiones. Esta percepción favorable también se refleja en el hecho de que el 40% de las organizaciones reconoce el papel fundamental del desarrollo y la innovación tecnológica, lo que demuestra una actitud abierta hacia la transformación digital. Sin embargo, solo un 33% indica tener claridad en los procesos y protocolos para ejecutar proyectos con alta incorporación tecnológica, y un 23% se encuentra en etapa de implementación, lo que evidencia la necesidad de fortalecer las capacidades operativas

del sector. Finalmente, el 43% de los encuestados afirma reconocer los conceptos asociados a tecnologías emergentes como inteligencia artificial, Big Data y ciencia de datos, lo cual representa un punto de partida importante para avanzar en procesos de formación y apropiación tecnológica dentro de las organizaciones.

Figura 2. Nivel de inversión durante 2 años



	Investigación y desarrollo.	Producción de productos o servicios.	Procesos administrativos internos (Contabilidad, talento humano).	Logística de recepción y distribución.	Comercial y ventas.	Sistemas de información (herramientas software).
Gran inversión	17%	27%	27%	20%	27%	30%
Mediana inversión	30%	37%	23%	23%	20%	20%
Pequeña inversión	27%	27%	43%	43%	43%	47%
Nula inversión	27%	10%	7%	13%	10%	3%

Fuente: Elaboración propia (2025). Basada en preguntas de encuesta nivel de madurez (apropiación) en la gestión de proyectos.

En relación con el análisis de la inversión tecnológica realizada por las organizaciones encuestadas durante los últimos dos años, se observa una clara tendencia hacia la priorización de recursos en áreas estratégicas operativas, principalmente en sistemas de información, comercial y ventas, logística, y procesos administrativos. Estos datos son clave para comprender el nivel de

compromiso con la incorporación de tecnologías emergentes como Big Data e Inteligencia Artificial en la gestión organizacional y, específicamente, en la identificación, análisis y evaluación de riesgos.

El área con mayor nivel de inversión reportada es la de sistemas de información (herramientas software), donde el 47% de las organizaciones manifiestan haber realizado una pequeña inversión, el 20% una mediana inversión y el 30% una gran inversión, dejando únicamente un 3% con nula inversión. Este resultado evidencia un interés creciente por fortalecer la infraestructura tecnológica, lo cual es esencial para la implementación de soluciones basadas en datos y automatización de procesos.

De forma paralela, áreas como comercial y ventas y logística de recepción y distribución también presentan un 43% de pequeñas inversiones, lo cual indica que las organizaciones han comenzado a destinar recursos para mejorar la eficiencia operativa y la gestión de relaciones con clientes. En ambos casos, la inversión mediana y alta aún es limitada, lo que sugiere que los avances en estas áreas están en fases preliminares de desarrollo.

En cuanto a los procesos administrativos internos (como contabilidad y talento humano), el 43% de las organizaciones indica haber hecho una pequeña inversión, mientras que el 23% realizó una inversión mediana y el 27% una inversión significativa. Esto refleja un reconocimiento por parte de las empresas sobre la importancia de modernizar los procesos internos, que son fundamentales para una adecuada toma de decisiones estratégicas basadas en datos.

Por otro lado, el área de producción de productos o servicios muestra una distribución más equilibrada: el 37% reporta una inversión media, el 27% una pequeña inversión y otro 27% una gran inversión. Este patrón indica que, aunque existe interés por aplicar tecnologías

emergentes en el núcleo productivo, las estrategias no han sido uniformes entre las distintas organizaciones.

Finalmente, el área con menor nivel de inversión es la de investigación y desarrollo (I+D). Un 27% de las organizaciones declara no haber realizado ninguna inversión en esta área, otro 27% realizó una pequeña inversión, el 30% una inversión mediana y apenas el 17% una gran inversión. Esta baja prioridad otorgada a la I+D representa una limitante significativa para la generación de soluciones innovadoras en la gestión de riesgos y evidencia una oportunidad de mejora importante en el sector.

Tabla 3. CLIENTES Y PROVEEDORES

II. CLIENTES Y PROVEEDORES				
Preguntas	**No se realiza**	**En algunos casos**	**En la mayoría de los casos**	**Se realiza permanentemente**
Implementa sistemas de información (herramientas software) para la gestión de proveedores.	10%	37%	23%	30%
Implementa sistemas de información (herramientas software) para la gestión de clientes.	13%	30%	30%	27%
Analiza información de sus clientes para generar o mejorar productos o servicios.	3%	30%	37%	30%
Integra múltiples canales de comunicación en las interacciones con sus clientes.	0%	33%	37%	30%
Integra múltiples canales de comunicación en las interacciones con sus proveedores.	10%	23%	43%	23%
Cuenta con la planificación y dirección de la cadena de suministros desde los clientes hasta los proveedores.	10%	40%	17%	33%

Fuente: Elaboración propia (2025). Basada en preguntas de encuesta nivel de madurez (apropiación) en la gestión de proyectos.

El análisis relacionado con clientes y proveedores permite evidenciar el nivel de adopción tecnológica y de prácticas integradas en la gestión de relaciones externas por parte de las

organizaciones del sector de vigilancia y seguridad privada en Bogotá. En general, los resultados muestran un avance importante en el uso de herramientas digitales y en la integración de procesos clave con impacto directo en la cadena de suministro y en la atención al cliente, aunque persisten áreas donde el desarrollo aún es parcial o incipiente.

En primer lugar, el uso de sistemas de información (herramientas software) para la gestión de proveedores se reporta como una práctica permanente en el 30% de las organizaciones, y en un 23% adicional se aplica en la mayoría de los casos. Estos datos indican un progreso notable en la automatización y sistematización de procesos logísticos y de abastecimiento, fundamentales para la trazabilidad y la eficiencia operativa en un entorno de riesgos cambiantes. De forma similar, la implementación de sistemas de información para la gestión de clientes se realiza de manera permanente en el 27% de los casos y con frecuencia en otro 30%, lo cual refleja una apropiación moderada de soluciones digitales para fortalecer las relaciones comerciales, aunque con un margen de mejora respecto a la consolidación total de dichas herramientas.

Uno de los aspectos más relevantes identificados es el uso de la información de los clientes para generar o mejorar productos y servicios. El 37% de las organizaciones lo realiza en la mayoría de los casos, mientras que un 30% lo hace de forma permanente. Este hallazgo sugiere una evolución hacia enfoques centrados en el cliente y orientados por datos, que son fundamentales para aplicar herramientas de inteligencia artificial en procesos de análisis predictivo o segmentación avanzada de usuarios. Este comportamiento también se ve reflejado en la gestión de la comunicación con los clientes: un 37% integra múltiples canales de interacción en la mayoría de los casos y un 30% lo hace permanentemente, lo que representa un

paso significativo hacia modelos de atención omnicanal, potenciando el conocimiento del cliente y la personalización de servicios.

En cuanto a la relación con proveedores, el 43% de las organizaciones señala que integra múltiples canales de comunicación en la mayoría de los casos, seguido de un 23% que lo hace de manera permanente. Este enfoque mejora la coordinación con aliados estratégicos y la capacidad de respuesta ante eventos disruptivos, contribuyendo así a una gestión más robusta de riesgos. Finalmente, el 33% de las empresas afirma contar con planificación y dirección de la cadena de suministros de manera permanente, mientras que un 40% lo hace en algunos casos. Esta última cifra, aunque mayoritaria, señala que en muchas organizaciones aún no se ha consolidado una visión integral de la cadena de valor, lo cual representa una oportunidad de fortalecimiento importante para garantizar continuidad operativa y gestión anticipada de riesgos.

Tabla 4. PROCESOS DE NIVEL TACTICO Y OPERATIVO

III. PROCESOS DE NIVEL TACTICO Y OPERATIVO			
Preguntas	**Nulo**	**Parcialmente**	**Implementado**
Las máquinas y sistemas se pueden controlar a través de tecnologías.	23%	50%	27%
Comunicación entre maquinas / sistemas - M2M	43%	47%	10%
Capacidad de integrarse y colaborar con otras maquinas / sistemas - INTEROPERABILIDAD	40%	43%	17%

Fuente: Elaboración propia (2025). Basada en preguntas de encuesta nivel de madurez (apropiación) en la gestión de proyectos

El análisis de los procesos de nivel táctico y operativo evidencia un panorama en el que la incorporación de tecnologías emergentes aún se encuentra en fases iniciales, con una implementación parcial predominante y escasos casos de adopción plena. Este componente, fundamental para lograr la transformación digital integral de las operaciones, muestra señales de

avance, pero también importantes retos en términos de automatización, interoperabilidad y comunicación entre sistemas.

En cuanto a la posibilidad de controlar máquinas y sistemas mediante tecnologías, el 50% de las organizaciones reporta una implementación parcial, lo cual indica que, si bien existe un reconocimiento del valor de la automatización, su adopción no ha sido homogénea ni completamente integrada en los procesos operativos. Solo el 27% señala tener esta funcionalidad implementada, lo que sugiere que una parte significativa del sector aún depende de sistemas manuales, limitando la eficiencia y la capacidad de respuesta ágil ante riesgos operativos.

Por otro lado, la comunicación entre máquinas o sistemas (Machine to Machine – M2M), que representa una capacidad clave dentro del paradigma de la Industria 4.0 y es fundamental para la toma de decisiones en tiempo real, presenta uno de los indicadores más bajos: apenas el 10% de las organizaciones afirma tener esta funcionalidad implementada, mientras que un preocupante 43% manifiesta no contar con ella en absoluto. Este dato revela una brecha significativa en cuanto al uso de tecnologías avanzadas de conectividad operativa, lo que podría obstaculizar la implementación eficaz de herramientas de Big Data e Inteligencia Artificial en los niveles más cercanos a la ejecución táctica de los proyectos.

De manera similar, la capacidad de integración y colaboración entre máquinas o sistemas (interoperabilidad) tampoco muestra un nivel de madurez alto. Un 43% indica que esta capacidad se encuentra parcialmente implementada y un 40% señala que no se ha implementado en absoluto. Solamente un 17% de las organizaciones cuenta con interoperabilidad efectiva. Este dato es especialmente relevante, ya que la interoperabilidad es un habilitador crítico para la consolidación de entornos digitales interconectados, que permiten recopilar, procesar y analizar grandes volúmenes de datos en tiempo real para la gestión proactiva del riesgo.

Tabla 5. INFRAESTRUCTURA Y SEGURIDAD

IV. INFRAESTRUCTURA Y SEGURIDAD					
Preguntas	**Totalmente en desacuerdo**	**Parcialmente en desacuerdo**	**Ni de acuerdo, ni en desacuerdo**	**Parcialmente de acuerdo**	**Totalmente de acuerdo**
La información de su organización se encuentra segura en el contexto de la transformación digital.	0%	20%	17%	33%	30%
Realiza evaluaciones y auditorías de seguridad de la información en su organización como parte de la estrategia de transformación digital.	7%	20%	10%	33%	30%
Promueve la conciencia y la capacitación en seguridad de la información entre los empleados de acuerdo a la transformación digital.	0%	17%	13%	43%	27%
Las medidas de respuesta ante incidentes de seguridad de la información en su organización son efectivas	0%	17%	17%	37%	30%

Fuente: Elaboración propia (2025). Basada en preguntas de encuesta nivel de madurez (apropiación) en la gestión de proyectos

Los resultados obtenidos en la dimensión de infraestructura y seguridad reflejan un panorama alentador en la protección de la información en el marco de la transformación digital. Se observa una tendencia mayoritaria hacia el acuerdo con las afirmaciones relacionadas con la seguridad digital, lo que sugiere un grado de madurez aceptable en la adopción de medidas de protección de datos.

En cuanto a la realización de evaluaciones y auditorías de seguridad de la información como parte de la estrategia de transformación digital, el 63% de los encuestados manifestó estar

de acuerdo (33% parcialmente de acuerdo y 30% totalmente de acuerdo). Este resultado sugiere que una parte significativa de las organizaciones ha comenzado a implementar mecanismos formales para evaluar su seguridad informática. Sin embargo, aún persiste un 37% que no las realiza de forma regular o que no tiene una postura clara al respecto, lo cual representa una posible debilidad que podría comprometer la integridad de la información y la eficiencia de los sistemas tecnológicos en caso de incidentes o vulnerabilidades.

Respecto a las evaluaciones y auditorías de seguridad como parte de la estrategia de transformación digital, también se evidencia una respuesta favorable: un 33% está parcialmente de acuerdo y un 30% totalmente de acuerdo con que estas se realizan, sumando un 63% que valida esta práctica. Esto demuestra que, si bien existen organizaciones que han adoptado una postura activa en la gestión de la ciberseguridad, aún un 37% reporta ausencia total, parcial o ambigüedad en esta labor, lo que representa un riesgo potencial en la protección de datos sensibles y operativos.

La promoción de la conciencia y la capacitación en seguridad de la información entre los empleados se posiciona como el aspecto con mayor nivel de aceptación. Un 43% de los encuestados está parcialmente de acuerdo con esta afirmación y un 27% totalmente de acuerdo, lo que da un total del 70%. Este resultado resalta la importancia que las organizaciones del sector otorgan al capital humano como parte de su estrategia de seguridad, entendiendo que la formación y sensibilización son pilares fundamentales para prevenir brechas internas.

Por último, las medidas de respuesta ante incidentes de seguridad también reflejan un nivel de implementación considerable: el 37% está parcialmente de acuerdo y el 30% totalmente de acuerdo, lo que equivale al 67% de las organizaciones que afirman contar con mecanismos efectivos para responder ante eventos de seguridad informática. No obstante, un 17% se

mantiene en posición neutral y otro 17% manifiesta desacuerdo parcial, lo cual sugiere que aún existen espacios para mejorar la preparación ante contingencias y fortalecer los protocolos de acción inmediata.

Tabla 6. ESTRATEGIA Y EXPERIENCIA EN INDUSTRIA 4.0

V. ESTRATEGIA Y EXPERIENCIA EN INDUSTRIA 4.0					
Preguntas	**Sin importancia**	**Importancia baja**	**Importancia media**	**Importancia alta**	**Importancia muy alta**
Inteligencia artificial.	10%	10%	27%	30%	23%
Fabricación aditiva.	27%	3%	47%	20%	3%
Internet de las cosas.	10%	7%	30%	27%	27%
Big data y análisis de datos.	7%	13%	17%	23%	40%
Realidad virtual y aumentada.	13%	7%	47%	17%	17%
Plataformas y comunicaciones.	7%	3%	33%	30%	27%
Tecnologías en la nube (Cloud).	7%	7%	27%	33%	27%
Ciberseguridad.	7%	3%	27%	30%	33%
Marketing digital.	7%	7%	33%	27%	27%
Formación y personas.	7%	3%	33%	30%	27%
Robótica y automatización.	7%	13%	33%	33%	13%

Fuente: Elaboración propia (2025). Basada en preguntas de encuesta nivel de madurez (apropiación) en la gestión de proyectos

El análisis de los resultados revela que algunas herramientas son ampliamente valoradas, mientras que otras muestran una menor integración o comprensión de su aplicabilidad al sector. En primer lugar, Big Data y análisis de datos es la tecnología que recibe la mayor valoración en términos de importancia estratégica. Un 40% de los encuestados la considera de importancia muy alta y un 23% de importancia alta, lo que totaliza un 63%. Este resultado sugiere que las organizaciones están reconociendo el valor de la analítica avanzada como una herramienta fundamental para la gestión del riesgo, la predicción de amenazas y la optimización de recursos.

Su aplicación permite, por ejemplo, identificar patrones delictivos, anticipar eventos y mejorar la toma de decisiones operativas y administrativas.

Le sigue la ciberseguridad, con un 63% de respuestas entre importancia alta (30%) y muy alta (33%). Este dato indica una conciencia sólida sobre la necesidad de proteger los datos sensibles de clientes, operaciones y vigilancia digital, lo cual es especialmente relevante en un contexto donde las amenazas cibernéticas se incrementan paralelamente al avance digital. Además, la creciente implementación de tecnologías conectadas obliga al sector a priorizar medidas de seguridad informática, protocolos de respaldo y entrenamiento en ciberhigiene.

Otro aspecto relevante es la percepción sobre las tecnologías en la nube (Cloud), que acumulan un 60% de valoración alta o muy alta. Este resultado refleja una clara tendencia hacia la digitalización de procesos y almacenamiento de información en entornos virtuales, lo cual mejora el acceso remoto, la continuidad del negocio y la interoperabilidad entre dispositivos o sedes operativas. Sin embargo, este porcentaje también sugiere que hay margen de mejora para una adopción más robusta e integral de la nube.

La inteligencia artificial (IA) obtiene también una puntuación significativa: 30% la percibe como de importancia alta y 23% como muy alta, alcanzando un total del 53%. Aunque esta cifra es positiva, muestra que aún hay organizaciones que no han interiorizado completamente el potencial transformador de la IA en aplicaciones como videovigilancia inteligente, análisis predictivo, automatización de procesos de monitoreo y sistemas de toma de decisiones en tiempo real. Un 20% adicional la considera de importancia baja o sin importancia, lo cual indica que aún existen barreras como desconocimiento, falta de formación técnica o resistencia al cambio.

En cuanto al Internet de las cosas (IoT), el 54% de las organizaciones lo sitúa entre las categorías alta (27%) y muy alta (27%). Esto refleja un avance moderado en la adopción de sensores, dispositivos conectados y sistemas que interactúan con el entorno en tiempo real, lo que es clave para monitoreo de instalaciones, control de accesos y operaciones descentralizadas.

Por otro lado, tecnologías como la fabricación aditiva (impresión 3D) y la realidad virtual y aumentada presentan menores niveles de valoración. En el caso de la fabricación aditiva, un 27% la considera sin importancia y solo el 3% muy importante, lo cual es comprensible dado que su uso es más frecuente en sectores industriales o de producción de objetos físicos, y su aplicación directa al sector de vigilancia aún es limitada o poco conocida. La realidad virtual, aunque con un 47% de respuestas en la categoría de importancia media, aún no alcanza niveles altos de adopción; sin embargo, podría tener un alto potencial en el futuro, por ejemplo, en simulación de entrenamientos y formación del personal operativo.

En cuanto a plataformas y comunicaciones, marketing digital, formación y personas, y robótica y automatización, los datos muestran una distribución intermedia, con porcentajes que oscilan entre el 30% y 60% de reconocimiento en los niveles medio a muy alto. Estos resultados revelan que hay un proceso de apropiación gradual, en el que las empresas están explorando e implementando estas tecnologías, aunque de forma desigual y aún sin consolidación generalizada.

5.2 Propuesta al sector

Con base en los resultados obtenidos y en estudios previos sobre la aplicación de la inteligencia artificial y el big data en la gestión de proyectos, se proponen lo siguiente:

5.2.1 Estrategias para fortalecer la adopción tecnológica

A partir del análisis realizado, se propone una estrategia integral compuesta por cuatro líneas de acción fundamentales para fortalecer la adopción de tecnologías emergentes como Big Data e Inteligencia Artificial en la gestión de riesgos del sector de vigilancia y seguridad privada en Bogotá. Estas estrategias han sido construidas con base en los resultados de la encuesta aplicada a 30 organizaciones del sector, los cuales evidencian el nivel actual de madurez tecnológica y las oportunidades de mejora.

La primera línea de acción se enfoca en fomentar la automatización de los procesos operativos mediante la implementación de tecnologías que faciliten la comunicación y el control entre máquinas y sistemas. Los resultados muestran que solo el 27% de las organizaciones ha implementado mecanismos de control tecnológico sobre sus sistemas, y apenas un 10% cuenta con comunicación máquina a máquina (M2M), mientras que la interoperabilidad entre sistemas alcanza únicamente un 17%. Estos datos reflejan una baja incorporación de capacidades clave para avanzar hacia entornos digitalizados y conectados. En este sentido, Porter y Heppelmann (2015) afirman que los productos y sistemas inteligentes conectados no solo permiten una operación más eficiente, sino también una gestión más precisa, contribuyendo directamente a la identificación y mitigación de riesgos.

La segunda estrategia propone consolidar una cultura organizacional orientada al uso estratégico de los datos. Según la encuesta, el 53% de las organizaciones reconoce la importancia del análisis de información, y el 63% valora el Big Data y el análisis de datos como tecnologías de alta o muy alta relevancia. Esto indica un reconocimiento incipiente, pero significativo, del papel de la analítica avanzada como herramienta para mejorar la toma de decisiones. Davenport

y Harris (2007) sostienen que las organizaciones que adoptan una cultura basada en datos tienen mayor capacidad para anticiparse a los riesgos y tomar decisiones informadas, aspecto especialmente crítico en sectores donde la prevención y la respuesta oportuna son fundamentales.

La tercera línea de acción se centra en el fortalecimiento de la ciberseguridad como componente transversal de la transformación digital. De acuerdo con los resultados, un 63% de las organizaciones realiza auditorías de seguridad, un 67% afirma contar con medidas de respuesta ante incidentes, y un 70% promueve activamente la capacitación del personal en temas e seguridad de la información. Estas cifras reflejan una base favorable para la construcción de una cultura de protección digital. Como lo plantean Von Solms y Van Niekerk (2013), una estrategia de ciberseguridad efectiva no solo depende de tecnologías robustas, sino también del desarrollo continuo de competencias en los equipos humanos que las gestionan.

Por último, se recomienda fortalecer la experiencia del cliente a través de herramientas digitales que permitan una interacción más fluida y personalizada. El 30% de las organizaciones analizan permanentemente los datos de sus clientes para mejorar sus servicios, y otro 30% ha incorporado múltiples canales de comunicación tanto con clientes como con proveedores. Este comportamiento evidencia una evolución hacia modelos centrados en el usuario y basados en datos, lo cual contribuye a mejorar la trazabilidad de la información, optimizar la prestación de servicios y responder de manera más eficiente ante posibles riesgos. En concordancia, Kane et al. (2015) afirman que una transformación digital efectiva se alcanza cuando la estrategia orienta la adopción tecnológica, priorizando el rediseño de procesos y la preparación del talento humano.

En conjunto, estas cuatro estrategias, automatización operativa, cultura de datos, ciberseguridad y experiencia digital del cliente ofrecen una ruta clara y fundamentada para avanzar hacia una transformación digital sólida, capaz de mejorar significativamente la identificación, análisis y evaluación de riesgos en el sector de vigilancia y seguridad privada.

5.2.2 Importancia de la transformación digital en el sector

La transformación digital implica un cambio profundo en la manera en que las organizaciones operan, se comunican y toman decisiones estratégicas. En el sector de vigilancia y seguridad privada en Bogotá, los datos analizados evidencian un nivel medio-bajo de madurez digital, con una adopción parcial de tecnologías emergentes como la inteligencia artificial, el Big Data y herramientas de interoperabilidad entre sistemas. Esta situación revela tanto avances iniciales como desafíos significativos en el camino hacia una digitalización más robusta.

De acuerdo con Westerman, Bonnet y McAfee (2014), una empresa digitalmente madura no se limita a incorporar nuevas tecnologías, sino que transforma su cultura, su estructura organizativa y su estilo de liderazgo para adaptarse a los cambios del entorno. En la misma línea, Schwab (2016) sostiene que la Cuarta Revolución Industrial exige a las organizaciones responder con agilidad a los acelerados avances tecnológicos, especialmente en sectores con alta responsabilidad operativa como la seguridad privada.

Los resultados de la encuesta aplicada a 30 organizaciones del sector muestran que, si bien el 33% cuenta con una estrategia de transformación digital formulada desde la alta dirección, solo un 10% la ha llevado a la fase de implementación. Esta brecha entre planificación e implementación evidencia la necesidad de mayor acompañamiento técnico, claridad en las

rutas de acción y compromiso institucional para lograr una adopción tecnológica efectiva y sostenida.

Asimismo, un 30% de las organizaciones indica haber integrado tecnologías como inteligencia artificial, Big Data o ciencia de datos en sus productos o servicios. Si bien esto representa un avance, también refleja una apropiación aún incipiente, considerando el gran potencial de estas herramientas para fortalecer la identificación, análisis y evaluación de riesgos. La baja automatización de procesos, la escasa interoperabilidad entre sistemas y la limitada comunicación entre máquinas (M2M) refuerzan la urgencia de consolidar una infraestructura digital capaz de soportar una gestión del riesgo más ágil, predictiva y basada en datos.

En este contexto, la transformación digital debe concebirse no solo como la incorporación de tecnología, sino como un proceso integral que exige el rediseño de procesos, la capacitación continua del talento humano, el fortalecimiento del liderazgo organizacional y la consolidación de una cultura de innovación. No se trata únicamente de modernizar sistemas, sino de reconfigurar la organización para responder de forma proactiva a las nuevas dinámicas del entorno.

En conclusión, la transformación digital representa una oportunidad estratégica para modernizar las operaciones, optimizar la gestión de riesgos y mejorar la toma de decisiones en las organizaciones del sector de seguridad privada. Sin embargo, para que este proceso sea efectivo, es indispensable superar la fase declarativa y avanzar hacia una implementación estructurada, progresiva y sostenida, que involucre activamente a todos los niveles de la organización.

5.2.3 Implementación progresiva y sostenida del cambio digital

La transformación digital en el sector de vigilancia y seguridad privada debe asumirse como un proceso progresivo, planificado y adaptado a las capacidades de cada organización. No se trata de una transición inmediata ni uniforme, sino de un cambio estructural que requiere etapas definidas, una visión estratégica de largo plazo y una integración equilibrada entre tecnología, liderazgo y cultura organizacional.

La propuesta contempla una implementación gradual compuesta por tres fases principales. La primera fase consiste en la realización de un diagnóstico interno riguroso del nivel de madurez tecnológica. Este paso es esencial para identificar brechas, reconocer fortalezas y establecer prioridades de acción realistas. Los resultados del diagnóstico aplicado a 30 organizaciones del sector evidencian una alta heterogeneidad en la adopción de tecnologías emergentes. Por ejemplo, solo el 17% ha alcanzado una interoperabilidad efectiva entre sistemas, y apenas el 10% ha implementado comunicación entre máquinas (M2M). Estos indicadores reflejan la necesidad urgente de evaluar con objetividad las condiciones actuales antes de emprender cualquier proceso de transformación.

La segunda fase debe enfocarse en la adopción escalonada de tecnologías clave que fortalezcan la eficiencia operativa y la toma de decisiones basada en datos. Según la encuesta, un 30% de las organizaciones ya ha realizado inversiones significativas en sistemas de información, lo cual representa una base tecnológica importante. Sobre esta infraestructura se puede avanzar hacia la implementación de plataformas de análisis de datos, tecnologías en la nube e incluso soluciones de inteligencia artificial aplicadas a la gestión de riesgos. La clave de esta fase es

alinear las decisiones tecnológicas con los objetivos estratégicos de cada organización y su capacidad operativa.

En una tercera etapa, la prioridad debe ser el fortalecimiento de las capacidades humanas y organizacionales. La formación del talento humano en competencias digitales, la promoción de una cultura orientada a la innovación y la implementación de políticas de ciberseguridad sólidas son elementos imprescindibles para garantizar el éxito sostenido de la transformación digital. En este sentido, Westerman, Bonnet y McAfee (2014) enfatizan que el éxito de este tipo de procesos no depende únicamente de la tecnología, sino de su integración efectiva con la estrategia, el liderazgo y la cultura organizacional. Resulta preocupante, por ejemplo, que solo el 27% de las organizaciones se encuentre en fase activa de capacitación en transformación digital, lo que evidencia una debilidad crítica que debe ser abordada de forma prioritaria.

5.3 Discusión

Los resultados obtenidos en esta investigación revelan matices importantes que enriquecen el análisis sobre la implementación de Big Data e Inteligencia Artificial (IA) en la gestión de riesgos en las organizaciones de vigilancia y seguridad privada en Bogotá.

Uno de los hallazgos más destacados es que la mayoría de estas organizaciones aún se encuentra en fases iniciales de apropiación tecnológica. Por ejemplo, solo el 30% ha integrado tecnologías emergentes (IA, Big Data o ciencia de datos) en alguno de sus productos o servicios, y apenas un 33% cuenta con una estrategia de transformación digital formulada desde la alta dirección, de las cuales solo el 10% está en fase de implementación efectiva. Este dato respalda lo planteado por Galindo Caldés (2019), quien sostiene que la transformación digital no es un simple proceso técnico, sino también cultural y organizacional, que requiere liderazgo, visión

estratégica y adaptación institucional. En consecuencia, los resultados obtenidos refuerzan la idea de que la digitalización del sector seguridad debe entenderse como parte de un proceso más amplio de maduración organizacional, más que como la simple adopción de herramientas tecnológicas.

En cuanto a Big Data, los participantes reconocen su potencial para mejorar la identificación y evaluación de riesgos. El 63% de las organizaciones encuestadas valora el análisis de datos como una herramienta de alta o muy alta importancia estratégica, y el 53% afirma comprender la relevancia del análisis de información para la toma de decisiones. Esta percepción coincide con lo señalado por Mayer-Schönberger y Cukier (2013), quienes argumentan que el valor del Big Data radica en su capacidad para generar conocimiento útil. Igualmente, se alinea con las afirmaciones de Jauregi-Maza (2021) y Samaniego Piedrahita (2022), quienes destacan que el uso de datos masivos incrementa la eficiencia decisional. No obstante, en el caso específico de las organizaciones de vigilancia en Bogotá, persisten barreras significativas para una implementación plena, entre ellas la baja capacitación del talento humano (solo un 27% está en acción en este aspecto), lo cual contrasta con los sectores analizados por los autores mencionados, generalmente más digitalmente avanzados, como el sector público o el social.

Respecto a la Inteligencia Artificial, su adopción aún se limita a funciones operativas básicas como el reconocimiento facial o la analítica de video. Aunque el 53% de las organizaciones la considera importante, su aplicación estratégica sigue siendo restringida. Esto concuerda parcialmente con Satama y Terán (2023), quienes afirman que la IA ya se utiliza ampliamente en múltiples áreas para la predicción de escenarios y la toma de decisiones estratégicas. Sin embargo, el sector de vigilancia aún no alcanza este nivel de sofisticación. De

hecho, solo el 17% de las organizaciones reporta interoperabilidad efectiva entre sistemas, y un escaso 10% ha implementado comunicación entre máquinas (M2M), lo cual limita las posibilidades de automatización avanzada. Estos hallazgos son coherentes con lo planteado por Alevizos y Dekker (2024), quienes defienden la necesidad de modelos híbridos donde la supervisión humana continúe siendo esencial para evitar una dependencia excesiva de la automatización.

La transformación digital, como se confirma tanto en los datos como en la teoría, es un facilitador clave del cambio organizacional. Kane et al. (2015) destacan que dicha transformación requiere una cultura abierta al cambio, liderazgo comprometido y una visión estratégica clara. Sin embargo, los resultados evidencian que estos elementos aún están poco consolidados: aunque el 33% de las organizaciones ha formulado estrategias digitales, el bajo nivel de implementación (10%) y la escasa capacitación interna sugieren que muchos procesos aún se desarrollan sin una guía estratégica clara. Esta realidad explica por qué, pese al reconocimiento de los beneficios de Big Data e IA, su adopción permanece limitada. Este fenómeno también es coherente con lo que advierte Coronado (2024) respecto a las barreras estructurales, regulatorias y éticas que enfrentan los sectores sensibles.

Desde la perspectiva de la gestión de riesgos, los resultados validan lo planteado por el Project Management Institute (2021), que señala que las tecnologías emergentes permiten una identificación más proactiva de amenazas, pero solo si se integran dentro de un enfoque sistémico. La evidencia muestra que muchas organizaciones aplican herramientas digitales de manera aislada, sin articularlas con una estrategia de análisis, mitigación y monitoreo de riesgos. Esta situación contrasta con lo afirmado por Montaudon-Tomas, Pinto-López y Amsler (2023), quienes sostienen que la incorporación de IA en la gestión de proyectos está ampliamente

extendida. En el contexto del sector de vigilancia y seguridad privada en Bogotá, este proceso sigue siendo incipiente y fragmentado.

Finalmente, el estudio aporta evidencia empírica que confirma la sinergia entre Big Data y la Inteligencia Artificial en el fortalecimiento de los sistemas de seguridad, tal como exponen Smith (2023) y Danish (2024). Estas tecnologías ofrecen capacidades notables para anticipar riesgos y mejorar la capacidad de respuesta ante incidentes. Sin embargo, los resultados muestran que la madurez digital del sector aún es limitada, lo que impide una explotación completa de estas capacidades predictivas. Esto representa no solo una brecha, sino también una valiosa oportunidad para impulsar la innovación, fortalecer las capacidades institucionales y avanzar hacia un modelo de gestión de riesgos más inteligente y estratégico.

6 CONCLUSIONES

A partir del análisis de los resultados obtenidos y de la revisión sistemática de la literatura especializada, se pueden extraer conclusiones relevantes que responden tanto a los objetivos específicos como a la pregunta de investigación de este estudio.

En primer lugar, respecto al diagnóstico del estado actual de implementación de Big Data e Inteligencia Artificial (IA) en las organizaciones de vigilancia y seguridad privada en Bogotá, los hallazgos revelan una adopción limitada, desigual y todavía incipiente. Si bien se evidencia una creciente conciencia sobre el valor estratégico de estas tecnologías, su integración práctica sigue siendo reducida. Solo el 10 % de las organizaciones ha puesto en marcha acciones concretas orientadas a la transformación digital, mientras que el 33 % cuenta con estrategias formuladas desde la alta dirección, pero sin ejecución efectiva. Esta situación refleja una clara

brecha entre la planificación estratégica y la capacidad operativa para llevar a cabo dichas iniciativas, lo que representa uno de los principales obstáculos para avanzar en procesos de digitalización profunda.

En cuanto al nivel de madurez tecnológica, se observan avances moderados en áreas como los sistemas de información, donde el 30 % de las organizaciones ha realizado inversiones significativas, así como en procesos administrativos y logísticos. Sin embargo, tecnologías esenciales para una transformación digital integral, como la interoperabilidad (solo implementada en el 17 % de las organizaciones), la comunicación máquina a máquina (M2M), presente apenas en el 10 %, y la automatización avanzada, presentan niveles de apropiación considerablemente bajos. Aunque herramientas como Big Data, la ciberseguridad y la computación en la nube son ampliamente reconocidas como prioritarias, el 63 % de las organizaciones considera el Big Data de alta o muy alta importancia, la inteligencia artificial aún no ha sido plenamente comprendida ni valorada: solo el 53 % le otorga la misma valoración. Estos datos evidencian la necesidad urgente de promover programas de formación especializada, procesos de sensibilización tecnológica y esquemas de acompañamiento técnico que permitan reducir las brechas actuales en capacidades digitales y de gestión del cambio.

En respuesta a la pregunta de investigación, se concluye que la integración de Big Data e IA tiene un alto potencial para optimizar la identificación, el análisis y la evaluación de riesgos en proyectos del sector. Estas tecnologías ofrecen ventajas significativas, como la posibilidad de anticiparse a amenazas mediante análisis predictivos más precisos, la reducción de tiempos de respuesta y la mejora en la toma de decisiones estratégicas en contextos operativos cada vez más complejos. Sin embargo, su efectividad depende de una implementación estructurada, sostenida en el tiempo y enmarcada en una estrategia de transformación digital sólida. Esta debe

contemplar tanto los aspectos técnicos como organizacionales y culturales que permitan que la tecnología se traduzca en verdaderas capacidades institucionales.

Finalmente, la propuesta desarrollada en este estudio, basada en tres fases: diagnóstico del nivel de madurez tecnológica, adopción progresiva de herramientas clave, y fortalecimiento del talento humano e infraestructura digital, constituye una hoja de ruta viable para el sector. Esta propuesta responde directamente a las principales debilidades identificadas, como la limitada ejecución de estrategias digitales, la baja interoperabilidad tecnológica y la escasa inversión en formación del personal (solo el 27 % de las organizaciones está en acción respecto a la capacitación en transformación digital). Su implementación permitiría avanzar hacia un modelo de gestión de riesgos más inteligente, proactivo y sostenible, que alinee la innovación tecnológica con los objetivos estratégicos del sector de vigilancia y seguridad privada en Bogotá, y que potencie su capacidad de respuesta frente a los desafíos actuales del entorno operativo.

7 Referencias

Acevedo Argüello, C., Zabala Vargas, S., Rojas Mesa, J., & Guayán Perdomo, O. (2020). Análisis de Redes Sociales como estrategia para estudiar los Sistemas de Innovación. Revisión sistemática de la literatura. Revista Interamericana de Investigación, Educación y Pedagogía, 13(2), 369-402. https://doi.org/10.15332/s1657-107X

Aguilar, L. J. (2016). Big Data, Análisis de grandes volúmenes de datos en organizaciones. Alfaomega Grupo Editor.

Aguilar Rivera, A. (2021). Vigilancia con IA y Big Data: retos y oportunidades. Revista Iberoamericana de Ciencia, Tecnología y Sociedad, 16(47), 45–62.

Alcaldía Mayor de Bogotá. (2023, agosto 30). El Distrito trabaja de la mano con las empresas de seguridad. https://bogota.gov.co/mi-ciudad/seguridad/el-distrito-trabaja-de-la-mano- con-las-empresas-de-seguridad

Alevizos, A., & Dekker, R. (2024). Integrating AI into threat intelligence: A hybrid model approach. Journal of Cybersecurity and Artificial Intelligence, 7(2), 88–105. https://doi.org/10.1016/j.jcai.2024.02.008

Alevizos, E., & Dekker, A. (2024). Hybrid intelligence for threat detection systems: Balancing automation and human oversight.

Álvarez, Y., Leguizamón-Páez, D., & Londoño, L. (2021). Cybersecurity risks in Big Data and IoT convergence: A literature review. IEEE Access, 9, 122371–122390. https://doi.org/10.1109/ACCESS.2021.3109972

Bhargava, R., & Maddireddy, S. (2024). Real-time data analytics with AI: Improving security event monitoring. Journal of Artificial Intelligence Applications, 9(1), 21–35.

Blanco, J. M., & Cohen, J. (2018). Inteligencia artificial y poder. Real Instituto Elcano, ARI, 93.

Cámara de Comercio de Bogotá. (2023). Informe sectorial de vigilancia y seguridad privada. https://www.ccb.org.co

CAF – Banco de Desarrollo de América Latina. (2021). Estado de la digitalización en América Latina: Avances y desafíos. https://www.caf.com

Celis, D. (2024). AI-driven predictive analytics for cybersecurity. Cybersecurity Intelligence Report, 6(2), 8–17.

Cercos Rubio, L., & Hermoso Traba, R. (2022). Inteligencia Artificial en la Gestión de RRHH: Big Data y People Analytics.

Congreso de la República de Colombia. (2008, 31 de diciembre). Ley 1266 de 2008: Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial y de servicios. Diario Oficial.

Congreso de Colombia. (2009, 5 de enero). Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones (Diario Oficial No. 47.223).

Congreso de Colombia. (2012). Ley 1539 de 2012: Por medio de la cual se implementa el certificado de aptitud psicofísica para el porte y tenencia de armas de fuego y se dictan otras disposiciones. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=48017

Congreso de Colombia. (2012, 17 de octubre). Ley Estatutaria 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales (Diario Oficial
No. 48 587, 18 de octubre de 2012)

Congreso de Colombia. (2016, 29 de julio). Ley 1801 de 2016: Por la cual se expide el

Código Nacional de Policía y Convivencia Ciudadana (Diario Oficial No. 49 949).

Congreso de Colombia. (2022, 25 de enero). Ley 2197 de 2022: Por medio de la cual se dictan normas tendientes al fortalecimiento de la seguridad ciudadana y se dictan otras disposiciones (Diario Oficial No. 51 928).

Constitución Política de Colombia. (1991). Artículo 15. https://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15

Coronado, J. R. (2024). Impacto del Big Data y la Inteligencia Artificial en la gestión de la Seguridad Social. Revista de Derecho de la Seguridad Social, Laborum, (Extraordinario 6), 49-70.

Danish, M., Qureshi, M. A., & Tariq, U. (2024). Enhancing cybersecurity through predictive analytics. Journal of Cybersecurity Research, 5(1), 14–29.

Danish, T. (2024). Enhancing cyber security through predictive analytics: A machine learning approach. Computers & Security, 130, 103201. ttps://doi.org/10.1016/j.cose.2024.103201

Davenport, T. H., & Harris, J. G. (2007). Competing on analytics: The new science of winning. Harvard Business Press.

Departamento Nacional de Planeación. (2019, 8 de noviembre). Documento CONPES 3975: Política nacional para la transformación digital e inteligencia artificial. Bogotá: Autor. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3975.pdf es.wikipedia.org+11repository.agrosavia.co+11colaboracion.dnp.gov.co+11

Fernández, A. L. F. O. N. S. O. (2020). El papel del Big Data en el reporting y la toma de decisiones. Revista de Contabilidad y Dirección, 31, 21-36.

Galindo Caldés, R. (2019). Big data e inteligencia artificial en la gestión de los recursos humanos del sector público. Revista catalana de dret públic, 2019,(58).

González, C., Pérez, R., & Martínez, L. (2020). Big Data y gestión del riesgo en pymes de seguridad. Revista de Ciencias Empresariales, 14(2), 120–134.

González, J., & Moreno, D. (2021). Barreras para la implementación de Inteligencia Artificial en empresas colombianas de seguridad privada. Universidad Nacional de Colombia.

Hernández Sampieri, R. y Mendoza Torres, C. P. (2018). Definición del alcance de la investigación en la ruta cuantitativa: exploratorio, descriptivo, correlacional o explicativo. En Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta (pp. 104-121). McGraw-Hill.

Jaimes-Quintanilla, M. A., & Zabala-Vargas, S. (2024). Inteligencia artificial en la gestión de proyectos: Caso construcción y obra civil. European Public & Social Innovation Review, 9, 1-21. https://doi.org/10.31637/epsir-2024-1615

Jauregi-Maza, L. (2021). Big Data: la revolución de los datos masivos en la Administración Pública. Inguruak. Revista Vasca de Sociología y Ciencia Política, (71).

Kane, G. C., Palmer, D., Phillips, A. N., Kiron, D., & Buckley, N. (2015). Strategy, not technology, drives digital transformation. MIT Sloan Management Review and Deloitte University Press.

Kaur, P., Sharma, M., & Mittal, M. (2021). Artificial intelligence approaches and mechanisms for big data analytics: A systematic study. PeerJ Computer Science, 7, e407. https://doi.org/10.7717/peerj-cs.407

Lee, H., Kim, S., & Choi, M. (2022). Big data analytics in security risk evaluation.

Journal of Risk Analysis and Crisis Response, 12(2), 75–90.

Leenen, L., & Meyer, T. (2021). Artificial intelligence and big data analytics in support of cyber defense. En R. Leal-Arcas (Ed.), Cybersecurity and Resilience in the Arctic (pp. 90– 108). IGI Global.

Marr, B. (2021). Data strategy: How to profit from a world of big data, analytics and the internet of things (2nd ed.). Kogan Page.

MarketsandMarkets. (2022). Big data security market by component – Global forecast to 2026. https://www.marketsandmarkets.com

Marwan, A. (2024). Integrative approaches in cybersecurity and AI for enterprise resilience. Information Systems Frontiers, 26(1), 121–138. https://doi.org/10.1007/s10796-023- 10253-6

Mayer-Schönberger, V., & Cukier, K. (2013). Big data: A revolution that will transform how we live, work, and think. Houghton Mifflin Harcourt.

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2020). Política nacional de transformación digital e inteligencia artificial. https://www.mintic.gov.co

Ministerio de Defensa Nacional. (1994, 11 de febrero). Decreto 356 de 1994: Por el cual se expide el Estatuto de vigilancia y seguridad privada. Diario Oficial, (11 de febrero de 1994). Consultado el 8 de junio de 2025, en Biblioteca Digital de Bogotá.

Ministerio de Defensa Nacional. (2001, 17 de septiembre). Decreto 1979 de 2001: Por el cual se expide el Manual de Uniformes y Equipos para el personal de los servicios de Vigilancia y Seguridad Privada (Diario Oficial No. 44558). Recuperado de la página de la Presidencia de la República de Colombia

Ministerio de Defensa Nacional. (2002, 18 de enero). Decreto 71 de 2002: Por el cual se dictan normas sobre cuantías mínimas de patrimonio que deberán mantener y acreditar los servicios de vigilancia y seguridad privada (Diario Oficial No. 44686). Recuperado de la página de la Presidencia de la República de Colombia

Ministerio de Defensa Nacional. (2006, 17 de julio). Decreto 2355 de 2006: Por el cual se modifica la estructura de la Superintendencia de Vigilancia y Seguridad Privada y se dictan otras disposiciones (Diario Oficial No. 46332). Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=66726

Ministerio de Salud y Protección Social. (2012, 26 de junio). Decreto 1377 de 2012: Por el cual se reglamenta el parágrafo 1.º del artículo 13 del Decreto-Ley 1281 de 2002, adicionado por el artículo 111 del Decreto-Ley 19 de 2012 (Diario Oficial). Recuperado de la base normativa de la Función Pública

Mintzberg, H., Ahlstrand, B., & Lampel, J. (2005). Strategy safari: A guided tour through the wilds of strategic management. Simon and Schuster.

Montaudon-Tomas, C. M., Pinto-López, I. N., & Amsler, A. (2023). Inteligencia artificial en gestión de proyectos: usos y aplicaciones.

Patel, V., & Shah, D. (2023). Real-time video analytics for threat detection. Proceedings of the International Conference on AI Applications, 65–72.

Porter, M. E., & Heppelmann, J. E. (2015). How smart, connected products are transforming companies. Harvard Business Review, 93(10), 96–114.

Pressman, R.S. (2020). Software Engineering: A practitioner’s approach (9ª Ed.). Mc Graw Hill.

Project Management Institute, I. (2021). Guía de los Fundamentos para la Dirección de Proyectos (Guía del PMBOK) – Séptima edición. Pennsylvania:

NISO (National Information Standards Organization).

Project Management Institute. (2010). Guía de los Fundamentos para la Dirección de Proyectos (P. Publications Ed. 4ta ed.). Pelsylvania, USA.

Project Management Institute. (2021). A guide to the project management body of knowledge (PMBOK® Guide) (7th ed.). Project Management Institute.

Radanliev, P., et al. (2020). Design of a dynamic, predictive cyber risk analytics framework for IoT edge computing. arXiv. https://arxiv.org/abs/2003.03839

Richards, D., & Young, M. (2022). Ethical implications of AI surveillance. Journal of Ethics and Information Technology, 24(3), 189–204.

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

Russom, P. (2011). Big data analytics. TDWI Best Practices Report. https://tdwi.org/research/2011/09/best-practices-report-q4-big-data-analytics.aspx

Salo, F., Injadat, M., Nassif, A. B., & Essex, A. (2020). Data mining techniques in intrusion detection systems: A systematic literature review. IEEE Access, 8, 13546–13661. https://doi.org/10.1109/ACCESS.2020.2965753

Samaniego Piedrahita, O. E. (2022). La analítica con Big Data para procesar datos relacionados con proyectos sociales en la provincia de Los Ríos (Bachelor's thesis, Babahoyo: UTB-FAFI. 2022).

Sarker, I. H., et al. (2022). Machine learning for intelligent data analysis and automation in cybersecurity. Computers & Security, 112, 102499. https://doi.org/10.1016/j.cose.2021.102499

Satama, F. L. V., & Terán, G. A. F. (2023). Inteligencia Artificial: El reto contemporáneo de la gestión empresarial. Revista ComHumanitas, 14(1), 94-111.

Schwab, K. (2016). The fourth industrial revolution. World Economic Forum.

Silva, M., Gómez, F., & Torres, L. (2021). Aplicación de IA en

vigilancia urbana: un estudio latinoamericano. Revista Latinoamericana de Seguridad, 8(3), 67–83.

Smith, A., & Johnson, B. (2023). AI-based risk modeling in private security projects. Journal of Security Science and Technology, 11(1), 55–70.

Smith, J. L. (2023). AI-driven cybersecurity: Leveraging Big Data for real-time risk mitigation. International Journal of Cybersecurity Intelligence and Cybercrime, 6(4), 115–132. https://doi.org/10.1016/j.ijcic.2023.12.004

Superintendencia de Vigilancia y Seguridad Privada. (2006, 8 de agosto). Resolución 2852 de 2006: Por la cual se unifica el régimen de vigilancia y seguridad privada (Diario Oficial No. 46 382, 5 de septiembre de 2006).

Superintendencia de Vigilancia y Seguridad Privada. (2023). Informe de cumplimiento normativo en empresas de vigilancia. https://www.supervigilancia.gov.co

Tayo, R., & Leidy, P. (2017). Modelo de gestión de riesgos para proyectos de desarrollo tecnológico. Santiago de Queretaro: CIATEQ.

Ullah, I., & Babar, M. A. (2018). Architectural tactics for big data cybersecurity analytic systems. arXiv. https://arxiv.org/abs/1807.06605

Ullah, I., & Babar, M. A. (2021). On the scalability of big data cybersecurity analytics systems. arXiv. https://arxiv.org/abs/2103.08564

van Noordt, C., Lima, M., & Stamatis, D. (2023). The role of AI technology in predictive risk assessment for business continuity. Sustainability, 15(4), 2211. https://doi.org/10.3390/su15042211

Vásquez, L., & Beltrán, M. (2022). Transformación digital en organizaciones medianas del sector privado en Colombia. Revista Colombiana de Tecnología y Sociedad, 18(2), 45–60.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security.

Computers & Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Westerman, G., Bonnet, D., & McAfee, A. (2014). Leading digital:

Turning technology into business transformation. Harvard Business Review Press.

Zabala-Vargas, S., Álvarez-Pizarro, Y., Sánchez-Galvis, I., & Rubio-Vásquez, K. (2024). Blockchain-Based Strategy to Optimize Certified Notifications from Government Entities. Administrative Sciences, 14(9). https://doi.org/10.3390/admsci14090195

Zabala-Vargas, S., & Jaimes-Quintanilla, M. (2025). Tecnologías 4.0 (IOT y ciencia de datos) orientada a optimizar la gestión de proyectos de construcción. European Public & Social Innovation Review, 10, 1-21. https://epsir.net/index.php/epsir/article/view/1621

Zabala-Vargas, S., Jaimes-Quintanilla, M., & Ramírez-Martínez, D. (2024). Project- based learning and emerging technologies. A strategy to improve academic performance in the training of project managers. 18th International Technology, Education and Development Conference, 5642-5646. https://doi.org/10.21125/inted.2024.1469

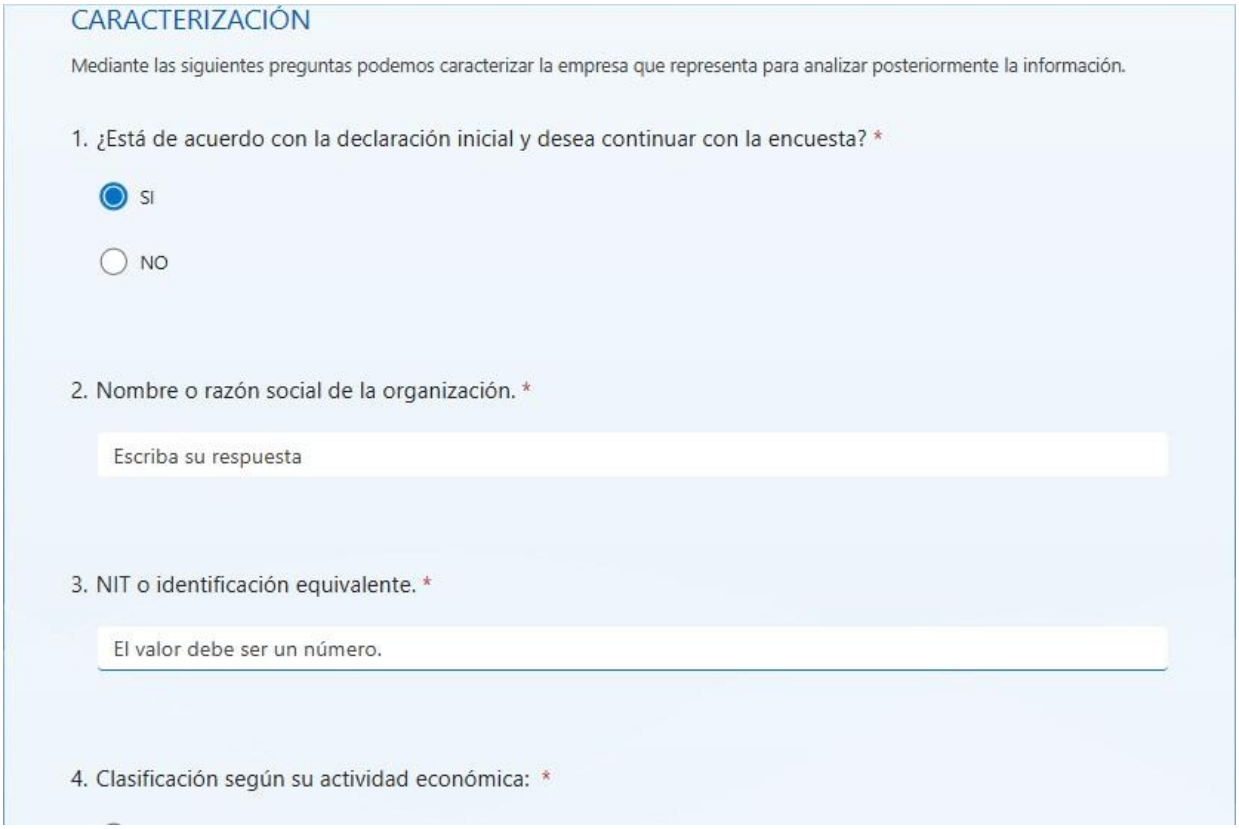
Zhang, X., Chan, J., Yan, H., & Wu, T. (2022). Towards risk-aware AI and ML systems: An overview. Journal of Artificial Intelligence Research, 75, 1–24. https://doi.org/10.1613/jair.1.12152

Zolanvari, M., Teixeira, M. A., Gupta, K., Khan, K., & Jain, R. (2019). Machine learning-based network vulnerability analysis of industrial Internet of Things. arXiv. https://arxiv.org/abs/1904.05500

Anexos

Anexo 1.

Encuesta de identificación de la tecnología emergente en la gestión de riesgos en el sector de seguridad privada en Colombia.



CARACTERIZACIÓN

Mediante las siguientes preguntas podemos caracterizar la empresa que representa para analizar posteriormente la información.

1. ¿Está de acuerdo con la declaración inicial y desea continuar con la encuesta? *

- (●) SI
- ( ) NO

2. Nombre o razón social de la organización. *

Escriba su respuesta

3. NIT o identificación equivalente. *

El valor debe ser un número.

4. Clasificación según su actividad económica: *

Encuesta nivel de madurez tecnológica (apropiación) en la gestión de proyectos

* Obligatorio

Parte 1 de 5: MODELO DE NEGOCIO Y PRODUCTO - Nivel estratégico

Mediante las siguientes preguntas se identificará el nivel de transformación digital de su modelo de negocio y la implementación de la misma en sus productos.

Nota: Al hablar de producto se hace referencia a tangibles o intangibles y al hablar de producción es el proceso de creación de cada uno de ellos.

11. De acuerdo a la afirmación seleccione cuál nivel representa mejor la organización. *

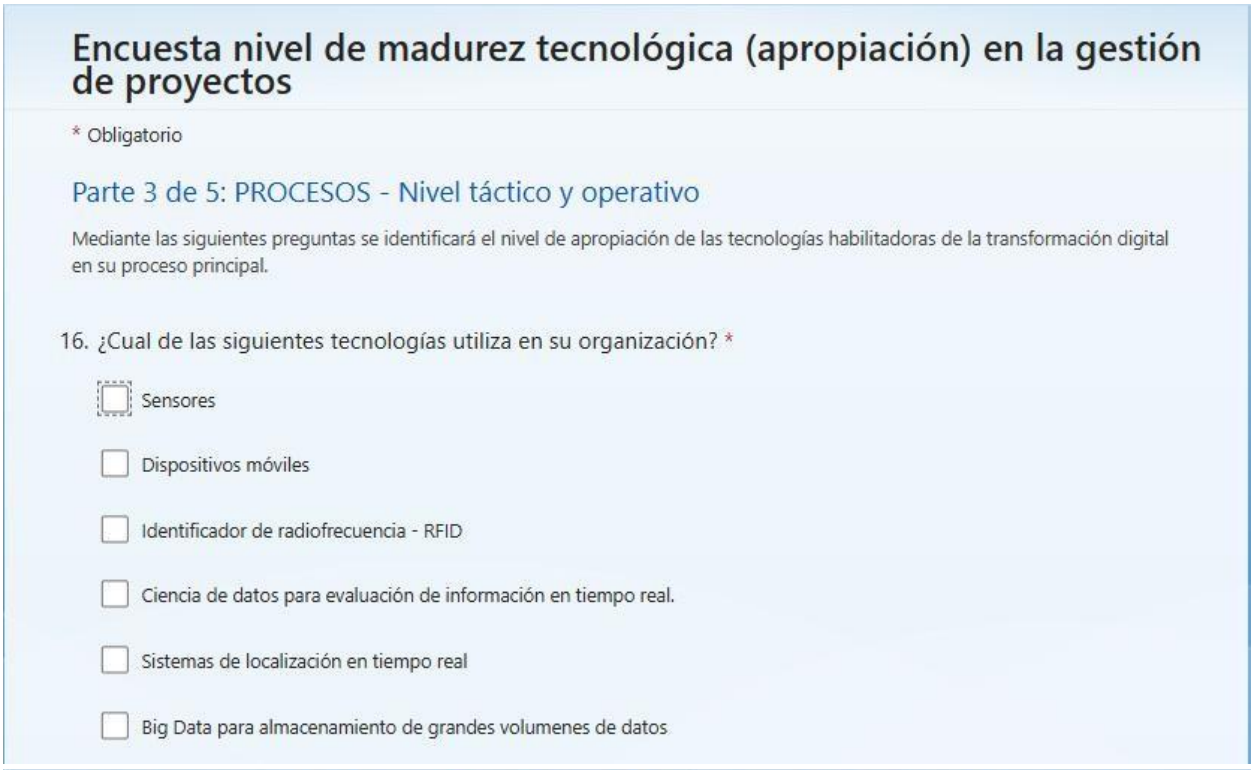
	Nulo	Existe la iniciativa	En desarrollo	En implementación	En acción
Cuenta con estrategia de transformación digital formulada desde la alta dirección.	◯	◯	◯	◯	◯
Cuenta con indicadores para medir nivel del transformación digital.	◯	◯	◯	◯	◯
Tiene interés en la capacitación del talento	◯	◯	◯	◯	◯

Parte 2 de 5: CLIENTES Y PROVEEDORES

Mediante las siguientes preguntas se identificará el nivel de apropiación de las tecnologías habilitadoras de la transformación digital en su relación con clientes y proveedores.

14. De acuerdo a las siguientes afirmaciones seleccione cuál nivel representa mejor su organización.

	No se realiza	En algunos casos	En la mayoria de los casos	Se realiza permanentemente
Implementa sistemas de información (herramientas software) para la gestión de proveedores.	◯	◯	◯	◯
Implementa sistemas de información (herramientas software) para la gestión de clientes.	◯	◯	◯	◯
Analiza información de sus clientes para generar o mejorar productos o servicios.	◯	◯	◯	◯



Encuesta nivel de madurez tecnológica (apropiación) en la gestión de proyectos

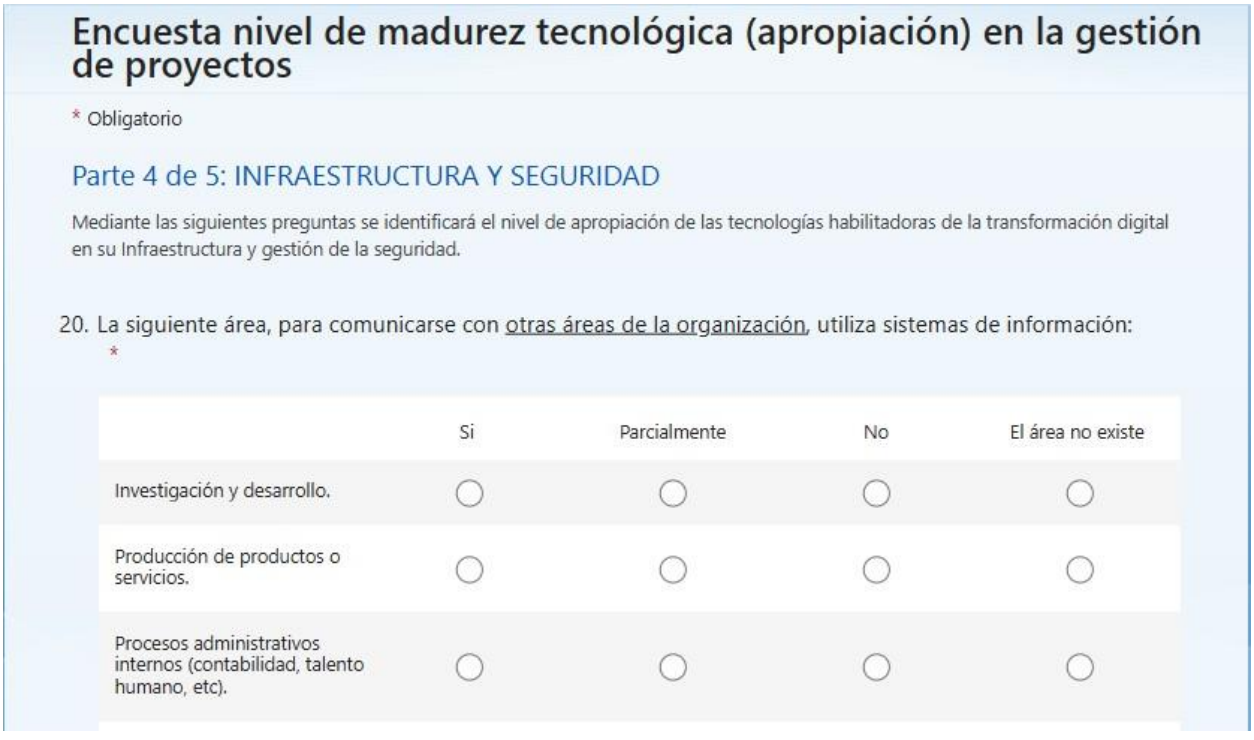
* Obligatorio

Parte 3 de 5: PROCESOS - Nivel táctico y operativo

Mediante las siguientes preguntas se identificará el nivel de apropiación de las tecnologías habilitadoras de la transformación digital en su proceso principal.

16. ¿Cual de las siguientes tecnologías utiliza en su organización? *

- [ ] Sensores
- [ ] Dispositivos móviles
- [ ] Identificador de radiofrecuencia - RFID
- [ ] Ciencia de datos para evaluación de información en tiempo real.
- [ ] Sistemas de localización en tiempo real
- [ ] Big Data para almacenamiento de grandes volumenes de datos



Encuesta nivel de madurez tecnológica (apropiación) en la gestión de proyectos

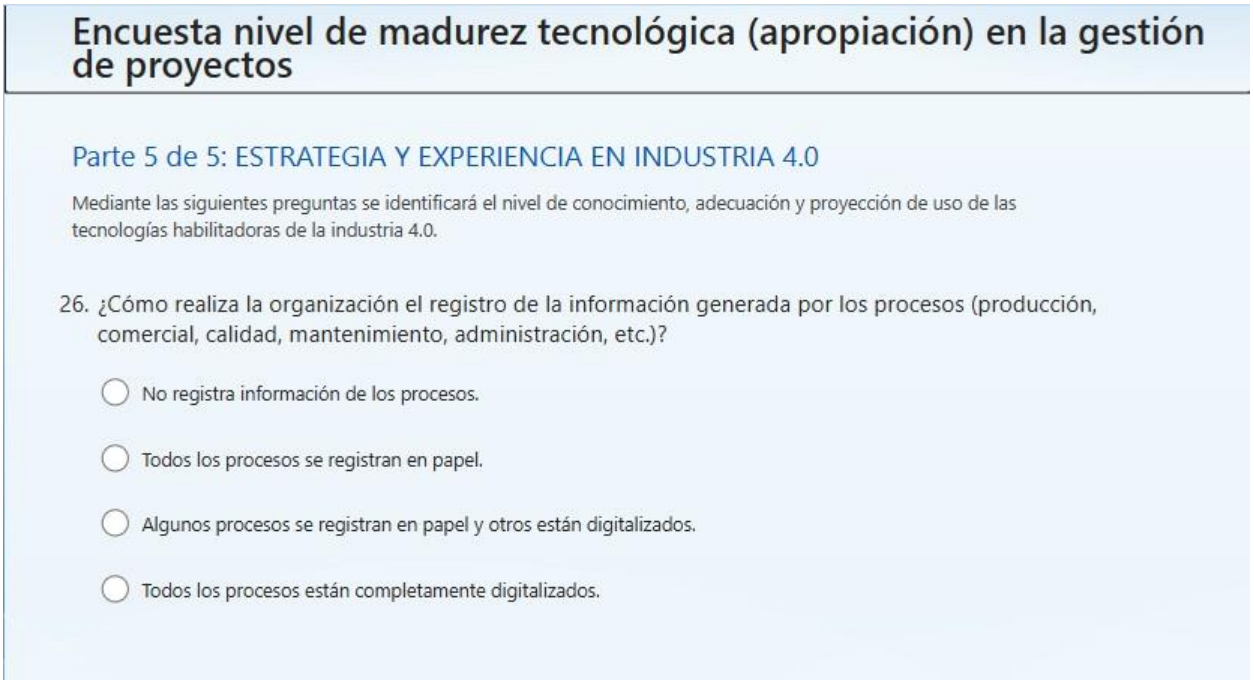
* Obligatorio

Parte 4 de 5: INFRAESTRUCTURA Y SEGURIDAD

Mediante las siguientes preguntas se identificará el nivel de apropiación de las tecnologías habilitadoras de la transformación digital en su Infraestructura y gestión de la seguridad.

20. La siguiente área, para comunicarse con otras áreas de la organización, utiliza sistemas de información: *

	Si	Parcialmente	No	El área no existe
Investigación y desarrollo.	○	○	○	○
Producción de productos o servicios.	○	○	○	○
Procesos administrativos internos (contabilidad, talento humano, etc).	○	○	○	○



Encuesta nivel de madurez tecnológica (apropiación) en la gestión de proyectos

Parte 5 de 5: ESTRATEGIA Y EXPERIENCIA EN INDUSTRIA 4.0

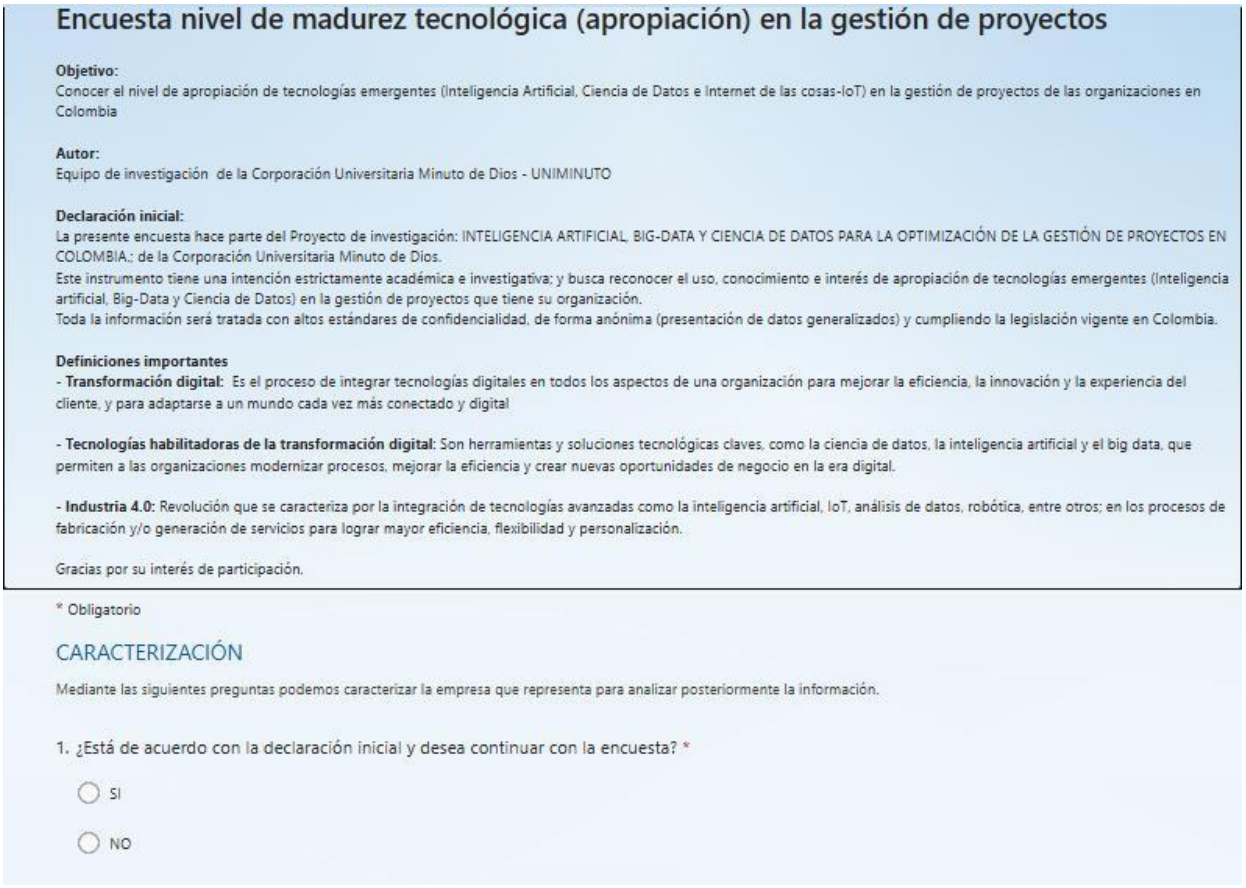
Mediante las siguientes preguntas se identificará el nivel de conocimiento, adecuación y proyección de uso de las tecnologías habilitadoras de la industria 4.0.

26. ¿Cómo realiza la organización el registro de la información generada por los procesos (producción, comercial, calidad, mantenimiento, administración, etc.)?

- ○ No registra información de los procesos.
- ○ Todos los procesos se registran en papel.
- ○ Algunos procesos se registran en papel y otros están digitalizados.
- ○ Todos los procesos están completamente digitalizados.

Anexo 2.

Declaración inicial e información sobre Encuesta de nivel de madurez tecnológico.



Encuesta nivel de madurez tecnológica (apropiación) en la gestión de proyectos

Objetivo:
Conocer el nivel de apropiación de tecnologías emergentes (Inteligencia Artificial, Ciencia de Datos e Internet de las cosas-IoT) en la gestión de proyectos de las organizaciones en Colombia

Autor:
Equipo de investigación de la Corporación Universitaria Minuto de Dios - UNIMINUTO

Declaración inicial:
La presente encuesta hace parte del Proyecto de investigación: INTELIGENCIA ARTIFICIAL, BIG-DATA Y CIENCIA DE DATOS PARA LA OPTIMIZACIÓN DE LA GESTIÓN DE PROYECTOS EN COLOMBIA.: de la Corporación Universitaria Minuto de Dios.
Este instrumento tiene una intención estrictamente académica e investigativa; y busca reconocer el uso, conocimiento e interés de apropiación de tecnologías emergentes (Inteligencia artificial, Big-Data y Ciencia de Datos) en la gestión de proyectos que tiene su organización.
Toda la información será tratada con altos estándares de confidencialidad, de forma anónima (presentación de datos generalizados) y cumpliendo la legislación vigente en Colombia.

Definiciones importantes
- **Transformación digital:** Es el proceso de integrar tecnologías digitales en todos los aspectos de una organización para mejorar la eficiencia, la innovación y la experiencia del cliente, y para adaptarse a un mundo cada vez más conectado y digital

- **Tecnologías habilitadoras de la transformación digital:** Son herramientas y soluciones tecnológicas claves, como la ciencia de datos, la inteligencia artificial y el big data, que permiten a las organizaciones modernizar procesos, mejorar la eficiencia y crear nuevas oportunidades de negocio en la era digital.

- **Industria 4.0:** Revolución que se caracteriza por la integración de tecnologías avanzadas como la inteligencia artificial, IoT, análisis de datos, robótica, entre otros; en los procesos de fabricación y/o generación de servicios para lograr mayor eficiencia, flexibilidad y personalización.

Gracias por su interés de participación.

* Obligatorio

CARACTERIZACIÓN

Mediante las siguientes preguntas podemos caracterizar la empresa que representa para analizar posteriormente la información.

1. ¿Está de acuerdo con la declaración inicial y desea continuar con la encuesta? *

- ◯ SI
- ◯ NO