Diseño de lineamientos estratégicos basados en la norma ISO 42001:2023 para mitigar el riesgo de exfiltración de datos mediante IA generativa en Acciones & Valores, Bogotá, 2026

David Alberto Manotas Ahumada

William Alberto Velásquez

Francisco Javier Buitrago Ortiz

Proyecto de investigación presentado como requisito para optar al título de:

Especialista en Gerencia de Ciberseguridad

Director (a):

Ricardo Andrés Villalba Rivera

Universidad EAN

Facultad de ingeniería

Gerencia en Ciberseguridad

Bogotá, Colombia

25/mayo/2026

1. El planteamiento del problema

1.1 Contexto Macro La Revolución de la IAG y el Fenómeno de la "Shadow AI" en el Sector Financiero Global

La llegada de la Inteligencia Artificial (IA) generativa cambió las reglas del juego en el sector financiero global. En Colombia, las firmas comisionistas de bolsa con una trayectoria sólida, como **Acciones & Valores**, han visto en herramientas como **Gemini, ChatGPT y Copilot (entre otras)** una oportunidad inmejorable para acelerar sus análisis de mercado y optimizar la redacción de informes. El problema de fondo es que la adopción tecnológica avanzó a un ritmo acelerado, dejando rezagados a los marcos tradicionales de gobernanza interna y de seguridad. Esto abrió una brecha de seguridad que expone información sensible de manera silenciosa pero constante.

Al no contar con una política clara ni con restricciones operativas automatizadas, los empleados de la firma interactúan de manera directa con estas herramientas de IA en sus versiones públicas. Esta práctica expone de forma latente datos financieros, estrategias de inversión corporativas y datos personales de clientes. El riesgo de fuga o exfiltración de datos; constituye una amenaza real y latente a la confidencialidad de la información en el sector bursátil y pone en jaque el cumplimiento de normativas estrictas de la Superintendencia Financiera de Colombia (SFC), específicamente la **Circular Externa 029 de 2019**, además de la legislación nacional de protección de datos (**Ley 1581 de 2012**).

Si dejamos que esta situación continúe de esta manera, y que la ausencia de herramientas perimetrales de Prevención de Pérdida de Datos (DLP) y el desconocimiento del personal sobre la huella digital que dejan sus consultas (*prompts*) en internet, generarán incidentes de seguridad de alto impacto. Las consecuencias para Acciones & Valores van desde costosas sanciones económicas impuestas por los entes de control hasta un quiebre reputacional en el mercado de capitales, donde la confianza de los inversionistas es el activo más difícil de recuperar.

1.2. Contexto Meso El Escenario Regulatorio y el Sector Bursátil en Colombia

En nuestro país, el sector bursátil opera bajo uno de los regímenes de vigilancia más estrictos de la región, liderado por la Superintendencia Financiera de Colombia (SFC) y el Autorregulador del Mercado de Valores (AMV). Las Sociedades Comisionistas de Bolsa (SCB) están sujetas a la **Circular Externa 029 de 2019** de la SFC (Sistema de Gestión de Seguridad de la Información y Ciberseguridad) y a la estricta observancia de la **Ley 1581 de 2012** (Régimen General de Protección de Datos Personales o Habeas Data).

La introducción de la inteligencia artificial generativa en este ecosistema genera una tensión regulatoria crítica. Mientras que la SFC exige una trazabilidad absoluta de las operaciones y la máxima protección de los activos de información de los inversionistas, el uso del canal público de herramientas como Gemini, ChatGPT y Copilot por parte de los empleados de la compañía para acelerar informes bursátiles, desarrollar aplicaciones y generar contenido audiovisual vulnera en la mayoría de los casos los principios de confidencialidad y segregación de funciones (Superintendencia Financiera de Colombia, 2023). A nivel nacional, encuestas gremiales estiman que el **65% de los profesionales del sector financiero** utilizan IA generativa de uso libre para optimizar sus tareas diarias sin el consentimiento ni el monitoreo de sus oficiales de cumplimiento ni lideres de ciberseguridad.

1.3 Contexto Micro La Problemática Específica en Acciones & Valores S.A.

Descendiendo a la realidad operativa local, la Sociedad Comisionista de Bolsa **Acciones & Valores S.A.** no es ajena a esta dinámica. En la firma se ha identificado una brecha crítica de seguridad derivada del uso no controlado y asimétrico de ChatGPT, Copilot y otros LLMs por parte de los equipos de análisis económico, mesas de dinero, asesores financieros y demás áreas operativas.

El problema radica en que, ante la presión operativa de los jefes directos por entregar análisis de mercado inmediatos, optimizar algoritmos de trading y automatizar tareas monótonas y de alta carga laboral, los empleados recurren a versiones públicas y gratuitas de estas IA. Al hacerlo, podrían ingresan variables financieras sensibles, estrategias de portafolio exclusivas de clientes y datos de identificación personal en las interfaces de cada una de las IA. Esto sumado que al carecer la firma de políticas corporativas explícitas para el uso de IAG, de estrategias de sensibilización normativa sobre los riesgos de los LLMs y de presupuesto para

establecer controles técnicos avanzados de Prevención de Pérdida de Datos (DLP) configurados para los equipos de los empleados y el tráfico web hacia estos entornos de IA, la información confidencial de Acciones & Valores S.A. podría quedar expuesta de manera directa a riesgos latentes de exfiltración, brechas de datos y accesos no autorizados por parte de terceros.

1.4. Estructuración Metodológica Árbol de Problemas

Para poder ver mejor la arquitectura de esta problemática, se podrían enumerar a continuación las causas raíz y los efectos directos de este fenómeno:

Efectos (Consecuencias)

Efecto Económico/Legal

Sanciones multimillonarias por parte de la SFC por incumplimiento de la Circular Externa 029 y multas de la Superintendencia de Industria y Comercio (SIC) por violación de la Ley 1581 de 2012.

Efecto Reputacional

Pérdida masiva de confianza por parte de los inversionistas y clientes de la comisionista ante una eventual filtración pública de datos.

Efecto Operacional

Pérdida de la propiedad intelectual de la firma y de ventajas competitivas en el mercado debido a la asimilación de algoritmos de trading propietarios por los modelos públicos de IA.

Problema Central

Uso sin control, sin normas e inseguro de herramientas de Inteligencia Artificial Generativa (IAG) en los procesos de análisis, trading y asesoría de la Sociedad Comisionista de Bolsa Acciones & Valores S.A., exponiendo activos de información

críticos y confidenciales a riesgos de exfiltración y brechas de seguridad sin que los empleados lo sepan o lo realicen con esa intención.

Causas Raíz

Nivel Gobernanza

Ausencia de políticas corporativas claras y comunicadas, lineamientos éticos y protocolos específicos que regulen el uso de la IAG dentro de la firma.

Nivel Cultura y Capacitación

Desconocimiento de los empleados sobre las implicaciones legales, regulatorias y de seguridad de datos al alimentar herramientas de IAG y LLMs públicos con información corporativa de carácter confidencial.

Nivel Tecnológico

Falta de presupuesto y herramientas técnicas de control, auditoría y sistemas DLP (Data Loss Prevention) adaptados para identificar y mitigar el flujo de datos hacia plataformas de IAG.

1.5. Justificación de la Investigación

Este problema se debe resolver de manera urgente y con todo el cuidado posible y por esto se justifica bajo cuatro dimensiones estratégicas fundamentales:

Práctica y Financiera

Proteger los activos de información críticos de Acciones & Valores S.A., disminuyendo así el riesgo de incidentes de ciberseguridad que puedan convertirse en pérdidas económicas directas o fugas de propiedad intelectual o información sensible de los clientes.

Legal y Normativa

Debemos asegurar el cumplimiento proactivo del marco normativo al cual estamos obligados y está estipulado por la SFC y la legislación de Habeas Data (SIC), evitando quejas y sanciones que afecten la licencia u operación de operación de la firma.

Teórica y Académica

Esta investigación busca aportar un precedente metodológico y un marco de gobernanza sobre el cual se alineen otras Sociedades Comisionistas de Bolsa en Colombia y empresas del sector financiero del país las cuales enfrentan el mismo problema: cómo innovar con IA sin comprometer la seguridad del mercado bursátil y de los clientes.

Sostenibilidad Corporativa y ESG

Esta investigación alinea la ciberseguridad con la triple línea de fondo de la compañia. En la dimensión ambiental, promueve la eficiencia computacional (Green AI) al centralizar el uso de los modelos de lenguaje en entornos empresariales estructurados, lo cual reduce las consultas redundantes y mitiga la huella de carbono digital de la firma. En el ámbito social, salvaguarda el derecho fundamental a la privacidad de los clientes bajo la Ley 1581 de 2012 y eleva la alfabetización ética y digital del talento humano, disminuyendo el estrés operativo por riesgos tecnológicos. Finalmente, en cuanto a la gobernanza y viabilidad económica, la adopción de la norma ISO 42001:2023 actúa como un pilar de resiliencia financiera que blinda el capital reputacional de Acciones & Valores ante incidentes de fuga de información, garantizando el cumplimiento estricto de la Circular Externa 029 de 2019 de la Superintendencia Financiera de Colombia y consolidando la confianza del mercado de capitales a largo plazo

2. Delimitación del problema

2.1 Delimitación de la investigación

Para garantizar la correcta viabilidad, pertinencia y enfoque del estudio, esta investigación se restringe bajo los siguientes criterios de distintas dimensiones:

2.2 Espacial y Geográfica

La investigación se desarrollará exclusivamente en la Sociedad Comisionista de Bolsa Acciones & Valores S.A., institución financiera con más de 65 años de trayectoria en el mercado bursátil colombiano. Se realizará principalmente en la sede principal ubicada en la ciudad de Bogotá, D.C., Colombia, la cual está bajo la jurisdicción regulatoria y legal de la Superintendencia Financiera de Colombia (SFC) y el Autorregulador del Mercado de Valores (AMV).

2.3 Temporal

Esta investigación tiene un horizonte temporal ubicado entre el primer semestre del año 2026 y el primer semestre de 2027. Este periodo estipulado comprende las distintas fases de diagnóstico del uso de la IA, evaluación de riesgos de fuga de información bajo el entorno normativo vigente y el diseño de la propuesta estratégica de gobernanza de la IA.

2.4 Temática y Conceptual

Este proyecto de investigación se alinea a las líneas de Seguridad de la Información, Ciberseguridad y de Tecnológia e Innovación. El núcleo principal de la investigación se centra en tres ejes normativos y técnicos como:

La norma ISO 42001:2023 (Sistema de Gestión de Inteligencia Artificial), donde se evalúan sus controles de gobernanza ética y gestión de riesgos.

La Circular Externa 029 de 2019 de la SFC y la Ley 1581 de 2012 (Protección de Datos Personales en Colombia).

La mitigación técnica del riesgo de exfiltración de activos de información confidencial hacia Modelos de Lenguaje Extensos (LLMs) de acceso público, tomando como objeto de estudio la herramienta Gemini.

2.5 Poblacional

El universo de estudio está constituido por la planta total de la firma en todo el país, la cual se estima es de 800 empleados los cuales están ubicados principalmente en la ciudad de Bogotá sobre los cuales se realizó un muestreo probabilístico (se explicará más a detalle en los

siguientes puntos) y se eligieron 169 empleados de diferentes áreas los cuales por sus funciones tienen acceso a información sensible y privilegiada de la compañía y de sus clientes. Para precisar la recolección de datos, se establecieron los siguientes criterios muestrales:

Criterios de Inclusión

Empleados de la compañía que se encuentran en las áreas de análisis económico, mesa de dinero (trading), asesoría financiera/comercial, gestión de riesgos y cumplimiento normativo.

Personal técnico o administrativo cuyo perfil operativo requiera el procesamiento o elaboración, de reportes financieros mediante herramientas de carácter digital.

Empleados que reconozcan o se evidencie que usen de manera autónomo herramientas de IA generativa para poder optimizar sus funciones diarias.

Criterios de Exclusión

Personal de áreas de mantenimiento físico, servicios generales o seguridad de física de las instalaciones y personal de mensajería.

Empleados que se encuentren en periodo de licencia, incapacidad o aislamiento laboral cuando se ejecute la fase de aplicación de los instrumentos de diagnóstico.

Personal externo o contratistas provisionales cuyas funciones no tengan relación directa con el manejo de activos de información confidencial ni de los clientes de la firma.

3. Pregunta de investigación

Para articular de manera concreta la brecha de seguridad identificada con los objetivos del estudio, se plantea la siguiente pregunta de investigación:

¿De qué manera el diseño de lineamientos estratégicos de gobernanza basados en la norma ISO:42001:2023 puede mitigar el riesgo de exfiltración de datos derivados del uso de

Inteligencia Artificial Generativa en los procesos operativos de Acciones & Valores S.A. durante el periodo 2026-2027?

3.1 Preguntas Subordinadas

¿Cuál es el estado actual del uso de herramientas de IAG y el nivel de exposición de datos confidenciales en los procesos operativos de la firma?

¿Qué controles y requisitos técnicos de la norma ISO 42001:2023 y la Circular Externa 029 de la SFC son aplicables a la mitigación del riesgo de Shadow AI?

¿Qué componentes estratégicos y tecnológicos deben integrar los lineamientos de gobernanza para garantizar un uso seguro de los LLMs en la comisionista de bolsa?

4. Variables técnicas y contextuales

4.1 Variables Técnicas

El uso de estas variables se centra básicamente en los sistemas, los datos, las herramientas tecnológicas y los controles de seguridad de la información.

4.1.2 Variable Técnica Independiente

Grado de alineación con los controles de la norma ISO 42001:2023

Definición Conceptual

Medida en que la firma cuenta con las respectivas directrices, políticas y controles técnicos específicos para la gobernanza de sistemas de Inteligencia Artificial.

Dimensiones

Políticas de IA

Existencia de lineamientos de uso aceptable de LLMs dentro de la firma.

Gestión de Riesgos de IA

Procesos internos establecidos para poder evaluar el impacto de los algoritmos y el flujo de datos que se realicen o se ejecuten con el uso de la IA.

Indicadores

Numero o porcentaje de controles de la norma ISO 42001:2023 implementados actualmente en la firma.

Existencia de un inventario corporativo de aplicaciones de IA utilizadas por los empleados de la firma.

4.1.3 Variable Técnica Dependiente

Vulnerabilidad a la exfiltración o fuga de activos de información

Definición Conceptual

El nivel de exposición y probabilidad de que los datos categorizados como confidenciales, secretos comerciales o datos personales sensibles de los clientes sean compartidos de forma no autorizada con LLMs de uso público.

Dimensiones

Nivel de Exposición de los Datos

Tipo de información corporativa que se introduce en las IA públicas (datos públicos vs. datos altamente confidenciales).

Controles Tecnológicos (DLP)

Capacidad técnica de los sistemas actuales con los que cuenta la compañía para poder bloquear o alertar oportunamente cuando se produzca una fuga de datos, o acceso no autorizado hacia URLs de IA públicas.

Indicadores

Frecuencia mensual de uso de versiones públicas de IA (Gemini, ChatGPT, Claude, Copilot) para tareas operativas y de soporte (Diario, Semanal, Nunca).

Número de políticas DLP (Data Loss Prevention) activas y configuradas específicamente para los equipos de cómputo corporativos orientadas a plataformas de IAG de acceso libre.

4.2 Variables Contextuales

Con estas variables se describe el entorno del sector bursátil y financiero colombiano, donde podemos ver la cultura interna de la firma y el marco regulatorio actual que ayuda a condicionar el problema.

4.2.1 Comportamiento operativo de "Shadow AI" (Cultura Organizacional)

Definición Conceptual

El nivel de adopción de forma autónoma y no controlada ni regulada de las herramientas de IA por los empleados de la firma para solucionar necesidades productivas de forma inmediata y ágil.

Dimensiones

Percepción de Necesidad

Presión por parte de los altos directivos hacia los empleados de optimizar el tiempo en procesos como la creación de informes o códigos de trading, agilizar tareas operativas o cumplir con tareas o reportes a entes de control. Y estar a la vanguardia en innovación en el sector.

Concienciación

Nivel de conocimiento actual de los empleados acerca de los riesgos legales de alimentar a una IA publica con datos de clientes y de la compañía.

Indicadores:

Porcentaje de los 169 empleados que se realizó la muestra que usan IA sin el conocimiento o consentimiento del área de riesgos no financieros y el líder de seguridad informática de la firma.

Número de capacitaciones recibidas por el personal sobre el uso seguro de IA en el último año.

4.2.2 Nivel de cumplimiento normativo en el sector (SFC y Ley 1581)

Definición Conceptual

El estado de cumplimiento de las operaciones bursátiles y de remesas de la firma con las políticas establecidas por la Superintendencia Financiera de Colombia (Circular Externa 029) y el régimen de protección de datos Ley 1581 de la SIC.

Dimensiones

Cumplimiento Superfinanciera

Alineación de los procedimientos de trading y deber de asesoría automatizada bajo los estándares de ciberseguridad exigidos a las entidades financiera.

Habeas Data Ley 1581

Garantizar que ningún dato personal privado o sensible de los clientes sea indexado en modelos gratuitos del mercado.

Indicadores

Existencia de auditorías internas que califiquen y monitoreen el impacto de las nuevas tecnologías y herramientas de cara a la Circular 029.

Cláusulas de confidencialidad firmadas y actualizadas en todos los contratos de los empleados respecto al uso de herramientas web de terceros, así como a los proveedores y aliados los respectivos NDA.

Matriz

Tipo de Variable	Variable	Dimensión Clave	Instrumento de Medición Sugerido
Técnica	Controles ISO 42001:2023	Políticas y Gestión de Riesgos	Lista de chequeo / Entrevista al Gerente de TI y Gerente de riesgos NO financieros.
Técnica	Exfiltración o fuga de datos	Controles DLP y categorización de la criticidad del dato	Análisis de los logs de la red (tráfico web) y matriz de criticidad y clasificación de datos.
Contextual	*Shadow AI*	Concienciación a los actores y frecuencia de uso de las herramientas	Encuesta diagnóstica anónima a los empleados y terceros.
Contextual	Cumplimiento Regulatorio	Cumplimiento con SFC y Ley 1581	Revisión de la documentación legal y normativa interna que aplique según la actividad.

4.3 Operacionalización de las Variables

A nivel metodológico, esta investigación toma un enfoque correlacional-causal, donde se busca establecer cómo la implementación de una estructura de gobernanza específica influye sobre el nivel de riesgo informático y operativo de la firma.

Variable Independiente

Lineamientos estratégicos basados en la norma ISO 42001:2023.

Definición Conceptual

Conjunto de lineamientos, políticas de la organización y controles a nivel de ingeniería social y tecnológica basados en el estándar internacional ISO 42001:2023. El propósito es llevar a cabo el uso responsable, seguro y ético de la Inteligencia Artificial, poniendo en equilibrio la innovación operativa que sucede en el sector y la mitigación de vulnerabilidades dentro de la firma.

Variable Dependiente

Nivel de riesgo de exfiltración o fuga de datos.

Definición Conceptual

Flujo, extracción o exposición accidental o malintencionada de activos de información catalogada como confidencial, propiedad intelectual o datos personales privados y sensibles protegidos legalmente por la normatividad, que se encuentre fuera de los límites de control de la firma hacia ambientes de LLMs de carácter público.

4.4 Tabla de Operacionalización de las Variables

Variable	Tipo	Definición Conceptual	Definición Operacional	Dimensión	Indicador	Ítem del Instrumento
Lineamientos estratégicos basados en ISO 42001:2023	**Independiente**	Estándar internacional para el establecimiento y mejora continua de un Sistema de Gestión de Inteligencia Artificial (SGIA) (ISO, 2023).	Evaluación técnica del nivel actual de madurez y la brecha regulatoria mediante una lista de chequeo institucional.	**Gobernanza de IA**	Nivel de formalización de las políticas coporativas sobre el uso de IAG.	*Matriz de Análisis Normativo: Ítems M1 - M4*
				Controles Técnicos	Existencia y uso de sistemas DLP y filtros de red hacia IA no permitidas.	*Matriz de Análisis Normativo: Ítems M5 - M8*

				Capacitación	Frecuencia y alcance de los planes de formación en ciberseguridad para la IA.	*Matriz de Análisis Normativo: Ítems M9 - M10*
Nivel de riesgo de exfiltración o fuga de datos	**Dependiente**	Propiedad o característica de vulnerabilidad en la fuga de información privada y sensible hacia ambientes externos y no autorizados de IA.	Puntuación cuantitativa resultado de la aplicación del cuestionario usando la escala de Likert CDR-IA.	**Cultura de Seguridad**	Nivel de concienciación de los empleados sobre los riesgos de los LLMs públicos. Percepción de criticidad de los datos compartidos en las plataformas externas.	**P4: Conocimiento de riesgos de IA públicas.** **P5: Percepción de confidencialidad.** **P6: Reporte activo de incidentes de Shadow AI.** **P7: Confianza de los clientes en la seguridad de la firma.** **P8: Responsabilidad a nivel individual del dato.**
				Prácticas de Uso	Frecuencia de uso autónomo de la IA (Shadow AI). Nivel de	**P9: Frecuencia de uso diario de IA públicas.** **P10: Tipo de información cargada (ej. códigos de trading).**

		criticidad de la información introducida en modelos de IA.	**P11: Resumen de reportes con datos privados de los clientes.** **P12: Copia de textos corporativos en la IA.** **P13: Uso de equipos propios para acceso a LLMs públicos y privados.**
	Cumplimiento Normativo	Nivel de adherencia a la Ley 1581 (Habeas Data). Alineación con la Circular Externa 029 de la SFC.	**P14: Conocimiento y aplicación de la Ley 1581 en entornos IA.** **P15: Identificación de lineamientos de la SFC.** **P16: Cumplimiento de las políticas de accesos de la firma.** **P17: Consentimiento expreso del cliente para uso de IA.** **P18:**

			Adherencia al código de ética corporativo.

4.4.1 Justificación del Mapeo de Ítems

La distribución de los ítems P4 a P18 en el instrumento CDR-IA obedece a una lógica factorial que responde directamente a las subvariables del problema de investigación:

Dimensión Cultura de Seguridad (P4 - P8)

Evalúa el componente de conocimiento interno del empleado. Este a su vez mide si el personal de Acciones & Valores S.A. realmente entiende y asimila que ingresar información a modelos públicos de IA con datos corporativos privados quiebra el principio de confidencialidad, o si actúan por un sesgo de optimización de tiempo y actividades.

Dimensión Prácticas de Uso (P9 - P13)

Mide la variable conductual y técnica real. abarcando el saber y el hacer. Identificando así de manera anónima qué tan constante es la práctica de Shadow AI al interior de la firma, rastreando qué tipos de activos de información específicos (algoritmos de trading, análisis bursátiles, base de datos de clientes) están migrando a los servidores de las plataformas de IA públicos.

Dimensión Cumplimiento Normativo (P14 - P18)

Compara el comportamiento del empleado de cara al entorno legal colombiano. Permite saber si el uso de la IAG en la firma está generando un riesgo inminente o muy alto de sanción legal por parte de la Superintendencia Financiera o de la Superintendencia de Industria y Comercio (SIC) teniendo en cuenta la clasificación de los riesgos en la compañía.

5. Naturaleza del problema

5.1 Clasificación y Justificación de la Naturaleza del Problema

El fenómeno que se identificó en la Sociedad Comisionista de Bolsa Acciones & Valores S.A. no es solamente una causa aislada; al contrario, este posee una **naturaleza de tipo mixta** que integra tres dimensiones interdependientes dentro del ecosistema institucional:

Dimensión Tecnológica

Se caracteriza por la ausencia o falta de validación de controles técnicos especializados en los perímetros de la red y en los dispositivos finales de usuario. Actualmente, la firma dispone de algunas reglas de Prevención de Pérdida de Datos (DLP) configuradas para interceptar, auditar o bloquear el flujo de cadenas de texto con datos financieros estructurados en dispositivos USB, discos, unidades ópticas, pero se queda muy corta cuando se enfoca hacia las API o interfaces públicas de Inteligencia Artificial Generativa (como Gemini, ChatGPT, Claude, Copilot entre otros).Sumando el fenómeno del teletrabajo o esquemas híbridos donde el empleado usa el internet de su hogar el cual no tiene unos controles robustos al respecto.

Dimensión de los Procesos

Hay un vacío a nivel procedimental en el flujo de las operaciones diarias. Los analistas de mercado, *traders* y asesores financieros no tienen un protocolo estandarizado de acceso, uso e interacción segura con LLMs. Donde las tareas operativas de análisis de reportes macroeconómicos y optimización de código de trading tienen pocos puntos de control de seguridad de la información previos a su procesamiento en entornos web externos.

Dimensión Organizacional y Cultural

Se puede evidenciar una brecha respecto a la cultura de seguridad y cumplimiento normativo. Los empleados trabajan bajo una alta presión por la eficiencia del tiempo y resultados, lo que promueve el fenómeno de *Shadow AI*. Existe una falta de conocimiento a nivel general sobre cómo el uso autónomo de herramientas de IA gratuitas y no controladas vulnera las directrices expuestas por la Circular Externa 029 de la SFC y los principios de confidencialidad de la Ley 1581 de 2012.

5.2 Mecanismo de Intervención: Relación Causal

Para poder solucionar esta problemática multidimensional, la investigación expone un modelo de ejecución directa que se basa en las variables expuestas del estudio:

Factor de Intervención (Variable Independiente - VI)

La elaboración de **lineamientos estratégicos basados en la norma ISO 42001:2023** . Esta variable actúa como el estímulo o causa, y aporta un marco de gobernanza integro que incluye las tres dimensiones del problema mediante políticas de bueno uso ético, diseño de controles de ingeniería de datos y estrategias corporativas de concienciación para los empleados.

Efecto Esperado

La disminución del **Nivel de riesgo de exfiltración o fuga de datos**, el cual se medirá de manera empírica por medio de la **Puntuación Global del instrumento CDR-IA** y los indicadores establecidos en la Matriz Normativa. La intervención de la variable independiente busca mover estadísticamente esta puntuación desde un nivel de alta vulnerabilidad hacia un nivel donde el riesgo sea administrable, seguro y aprobado por la junta directiva.

5.3 Análisis de la Brecha Organizacional

La meta metodológica de este proyecto de investigación consiste en poder cerrar la brecha existente entre el panorama actual de desregularización y el escenario ideal seguro y confiable bajo el estándar internacional.

Dimensión	Estado Actual (AS-IS)	Estado Deseado (TO-BE)
Gobernanza e IA (Organizacional)	Uso de IA de forma autónoma (*Shadow AI*). Ausencia de lineamientos éticos o políticas de	Adopción controlada y regularizada de la IAG. Políticas corporativas formalizadas y

	uso aceptable de IAG en la comisionista.	alineadas con la norma internacional ISO 42001:2023 y los objetivos estratégicos de la firma.
Operación y Flujos (Procesos)	Procesamiento y análisis de informes bursátiles y códigos de trading directamente en LLMs públicos sin validación previa del área de seguridad informática.	Protocolo obligatorio de anonimización de los datos y flujos de trabajo con puntos de control de seguridad antes de cual interacción con IA.
Ciberseguridad y Red (Tecnológica)	Baja implementación o carencia de políticas DLP específicas para entornos de IA. Tráfico web hacia plataformas de IA des monitoreado en los dispositivos finales de usuario.	Reglas DLP activas y afinadas en la red corporativa y a nivel externo. Filtrado automático de cargas de datos confidenciales y monitoreo constante de APIs de IA.
Cumplimiento Legal (Normativo)	Riesgo inminente de sanción por parte de la SFC (Circular 029) e incidentes de violación de la Ley 1581 de 2012.	Blindaje a nivel legal y regulatorio. Cumplimiento auditable ante los requerimientos de la SFC y la SIC.

5.4 Efectos de la No Intervención

Si se mantiene el estado actual en Acciones & Valores S.A. frente al avance acelerado de la adopción de la IA generativa esto podría causar graves consecuencias a corto y mediano plazo:

Materialización de Brechas de Datos

La posibilidad de que un secreto comercial (un algoritmo propio de trading o una estrategia de portafolio de un cliente de alto patrimonio) sea absorbido por el

modelo de aprendizaje de IA públicas, quedando indexado y potencialmente expuesto a competidores del sector.

Riesgo Económico

El descubrimiento de estas prácticas por parte de una auditoría de la Superintendencia Financiera de Colombia podría acarrear amonestaciones públicas y multas muy altas por la falta de debida diligencia en la custodia de los activos de información financiera (Circular Externa 029).

Riesgo Reputacional

En el sector comisionista de bolsa, la reputación es el activo más importante; un incidente de exfiltración o fuga de datos personales de inversionistas (Habeas Data) podría provocar una migración masiva de clientes hacia firmas competidoras, afectando la viabilidad financiera e histórica de la entidad.

6. Objetivo General

Diseñar lineamientos estratégicos de gobernanza y protocolos técnicos basados en la norma ISO 42001:2023, para mitigar el riesgo de exfiltración o fuga de datos derivado del uso de Inteligencia Artificial Generativa pública (Gemini, ChatGPT, Claude, Copilot entre otras) en los procesos operativos de Acciones & Valores S.A. durante el periodo 2026-2027.

7. Objetivos Específicos

Elaborar un diagnóstico técnico-operativo de las brechas de seguridad y puntos críticos de fuga de información en el uso actual de IA por parte de los empleados.

Evaluar los requisitos de gobernanza de la norma ISO 42001:2023 y la Circular 029 de la SFC para su integración en la política de ciberseguridad corporativa.

Establecer una matriz de clasificación de activos de información y protocolos técnicos de anonimización para interacciones seguras con la IA..

Desarrollar un esquema de capacitación y sensibilización que minimice el riesgo operativo por error humano en el manejo de herramientas disruptivas.

8. Diseño metodológico

Para asegurar que la coherencia epistemológica y operativa de la investigación, se estableció una cadena de derivación metodológica que alinea cada una de las fases del estudio con la problemática planteada

Pregunta Problema → Enfoque (Mixto) → Tipo/Alcance (Descriptivo-Propositivo) → Diseño (No Experimental, Transversal, con componente de Estudio de Caso).

8.1. Enfoque de la Investigación

La investigación establece un **enfoque mixto**, implementando un **diseño convergente u de triangulación simultánea** (Hernández-Sampieri y Mendoza, 2018). Esta decisión metodológica se ajusta a la naturaleza multifactorial del problema de investigación, el cual integra dimensiones técnicas (controles de seguridad), normativas (estándares regulatorios) y humanas (comportamiento de los usuarios) las cuales no se pueden abordar de manera suficiente desde un único paradigma.

Componente Cuantitativo

Permite medir las brechas de seguridad, los rangos de exposición de la información y el nivel de cumplimiento normativo frente a los requisitos de la norma ISO 42001:2023, la ISO 27001:2022 y la Circular Externa 029 de 2019 de la Superintendencia Financiera de Colombia (SFC).

Componente Cualitativo

Ayuda a la comprensión de las prácticas reales del grupo poblacional estudiado, sus factores de comportamiento y los diferentes contextos operativos del día a día que influyen en el uso informal de las herramientas de inteligencia artificial generativa públicas.

De acuerdo con Hernández-Sampieri y Mendoza (2018), la convergencia de estos enfoques en el mismo estudio permite obtener una visión integral y holística del riesgo de exfiltración o fuga de datos, lo que fortalece el diagnóstico y asegura la efectividad de la propuesta final.

8.2. Tipo y Alcance de la Investigación

Según la taxonomía de alcances de la investigación (Hernández-Sampieri y Mendoza, 2018), este estudio tiene un **alcance combinado de carácter Descriptivo-Propositivo**:

Alcance Descriptivo

Se enfoca en caracterizar de manera puntual el estado actual (*AS-IS*) de la firma Acciones & Valores respecto a la gestión del riesgo tecnológico, indicando las propiedades, perfiles y vulnerabilidades de los empleados al interactuar con modelos de lenguaje masivos (LLMs) de carácter público.

Alcance Propositivo

A partir de estos descubrimientos descriptivos y el diagnóstico de las brechas, la investigación avanza de una fase propositiva orientada al diseño y formulación de una solución estratégica estructurada (el marco de lineamientos técnicos y de gobierno bajo la norma ISO 42001:2023) para transformar el estado de vulnerabilidad hacia un estado seguro (*TO-BE*).

8.3. Diseño de la Investigación

Para la respectiva recolección y el procesamiento de la información, la investigación se articula de manera diferenciada según la naturaleza de sus componentes:

Diseño Cuantitativo (No Experimental y Transversal)

El estudio es *no experimental* ya que no existe una manipulación deliberada e intencional de las variables; se observan los fenómenos de seguridad y fugas de información en su entorno real para posteriormente analizarlos (Hernández-Sampieri y Mendoza, 2018). Así mismo, es *transversal (o transeccional)* ya que la recolección de los datos masivos (encuestas a empleados y la auditoría técnica de logs de red) se ejecuta en punto único o momento del tiempo en el año 2026.

Diseño Cualitativo (Estudio de Caso)

Se adopto el *estudio de caso* como un diseño cualitativo idóneo para examinar de manera intensiva y profundidad una unidad social u organizacional específica: la cual es la firma comisionista de bolsa Acciones & Valores. Este diseño permite evaluar las diferentes dinámicas de la interacción informal con la IA, los vacíos actuales en las políticas internas y la resistencia cultural dentro del sector bursátil supervisado.

8.4. Estrategia de Integración y Fases del Estudio

Los datos cuantitativos y cualitativos se recolectan de manera paralela y se analizan de forma independiente para, luego de esto, realizar una **triangulación de datos** en la fase de discusión. Este cruce metodológico permite comparar las autopercepciones de los empleados (cualitativo) respecto a las métricas reales del tráfico en la red y los niveles de cumplimiento normativo (cuantitativo).

Para materializar esta estrategia, el estudio se implementa de manera lógica y secuencial a través de las siguientes **cinco fases metodológicas**:

Fase de Diagnóstico

Ejecución de encuestas analíticas y fichas de observación técnica de logs para poder medir el nivel actual de madurez y los puntos críticos de fuga actuales.

Fase Normativa

Revisión interna de la documentación y cumplimiento sistemático de los requisitos de gobernanza expuestos en la norma ISO 42001:2023 y las circulares de la SFC.

Fase de Clasificación

Diseño técnico de la matriz de activos de información para categorizar los datos institucionales aptos y no aptos para entornos de IA.

Fase de Diseño de Protocolos

Formulación de lineamientos iniciales de uso e interacción segura de IA, tales como reglas de prevención DLP y técnicas de anonimización de *prompts*.

Fase de Propuesta Pedagógica

Elaboración junto con el equipo de formación de la compañía del esquema de capacitación y sensibilización para poder mitigar los riesgos operativos derivados del error humano en el uso indebido de IA Publicas.

9. Técnicas e instrumentos de recolección de datos

9.1. Técnicas de recolección de datos

Adoptando un enfoque mixto, esta investigación utiliza un **diseño convergente.** Bajo este modelo, los datos cuantitativos y cualitativos se recopilan de forma paralela en el tiempo, se procesan de manera independiente y luego, se someten a un proceso de **triangulación de datos**. Esta estrategia metodológica nos permite comparar, correlacionar y complementar las diferentes perspectivas de los empleados frente a las evidencias empíricas arrojadas por la infraestructura tecnológica actual que sería (lo que dicen los usuarios vs. lo que muestran los datos de la red).

Para el despliegue del estudio se han elegido de manera analítica las siguientes técnicas estructuradas:

9.1.1. Técnicas Cuantitativas

Encuesta por Cuestionario

Enfocada a tipificar y medir de manera masiva cada una de las variables de estudio en el personal analista de la firma. El propósito es poder cuantificar la frecuencia de interacción con la IA, clasificar la tipología de los datos suministrados en los *prompts*

y después evaluar el nivel de conocimiento técnico en seguridad de la información de los empleados.

Observación Tecnológica por Listas de Verificación (*Checklists*)

Técnica de revisión estructurada que se basa en los dominios de control de los estándares internacionales ISO 27001:2022 e ISO 42001:2023, diseñada para poder medir matemáticamente el grado de madurez corporativa en términos de gobernanza de IA.

9.1.2. Técnicas Cualitativas

Entrevista Semiestructurada

Aplicada de forma directa hacia grupos focalizados y empleados tomadores de decisiones dentro de la firma. Esta permite capturar las narrativas profundas sobre cada una de las prácticas operativas que se realizan de manera informal, poder identificar los riesgos emergentes que no están visibilizados ni documentados y así diagnosticar los diferentes vacíos normativos en las políticas corporativas vigentes y la regulación del mercado.

Observación Directa de Procesos Operativos

Realizada por un grupo evaluador dedicado el cual examina el flujo de trabajo en las estaciones de trabajo, con el fin de poder mapear visual y operativamente cada uno de los puntos críticos propensos a la fuga de información.

Revisión Documental

Análisis crítico y exhaustivo de los manuales internos de seguridad de la información, lineamientos de cumplimiento vigentes y procedimientos normativos institucionales.

9.1.2. Población y Muestra

Para brindar validez interna a la investigación dentro del sector bursátil, se establece una distinción metodológica entre el universo total de la firma y el segmento objetivo que será evaluado.

9.1.2.1. Definición del Universo y la Población

Universo / Población (N)

Está confirmado por la totalidad de empleados vinculados a la firma comisionista de bolsa Acciones & Valores, la cual cuenta con una planta global aproximada de **800 empleados**.

Muestra (n): El subconjunto representativo se obtuvo mediante muestreo probabilístico, lo que nos dios un valor de **169 analistas y empleados**, a quienes se les realizara de manera formal el Cuestionario de Diagnóstico de Riesgo (CDR-IA).

9.1.2.2 Tipo de Muestreo

Se determina aplicar un Muestreo Probabilístico Aleatorio Simple. Este método asegura que cada uno de los 800 empleados de la firma posea exactamente la misma probabilidad matemática de ser escogido para conformar la muestra de 169 individuos, eliminando así los sesgos de selección y permitiendo generalizar los resultados del riesgo de exfiltración de datos a toda la organización.

9.1.2.2.1 Cálculo Matemático de la Muestra (Población Finita)

Para justificar matemáticamente la obtención de la muestra de 169 colaboradores se parte de la base actual de 800 empleados, se parametriza la fórmula estándar para poblaciones finitas con un nivel de confianza del 95% (Z = 1.96), una variabilidad del 50% (p = q = 0.5) y un margen de error establecido en 6.7% (e = 0.067):

$$n = \frac{N \cdot Z^2 \cdot p \cdot q}{e^2 \cdot (N-1) + Z^2 \cdot p \cdot q}$$

Donde los parámetros estadísticos se definen y operacionalizan de la siguiente manera:

N (Tamaño de la población): 800 empleados.

Z (Nivel de confianza): 1.96 (valor crítico estandarizado para un nivel de confianza del 95%).

e (Margen de error): 0.067 (6.7% de error admisible).

p (Probabilidad de ocurrencia del evento): 0.50 (grado de variabilidad estimado al 50% ante la ausencia de antecedentes previos).

q (Probabilidad de no ocurrencia del evento): 0.50 (definido como 1 - p, equivalente al 50%).

Desarrollo paso a paso de la ecuación:

Sustitución de los valores en la fórmula

$$n = \frac{800 \cdot (1.96)^2 \cdot 0.5 \cdot 0.5}{(0.067)^2 \cdot (800 - 1) + (1.96)^2 \cdot 0.5 \cdot 0.5}$$

Resolución de potencias y productos intermedios

$$n = \frac{800 \cdot 3.8416 \cdot 0.25}{0.004489 \cdot 799 + 3.8416 \cdot 0.25}$$

Simplificación de términos (numerador y denominador)

$$n = \frac{768.32}{3.586711 + 0.9604}$$

$$n = \frac{768.32}{4.547111}$$

Resultado matemático final

n = 168.969 - 169 (redondeado)

A través de esta demostración formal, se justifica que el tamaño de la muestra es representativa y óptima para poder evaluar el riesgo de exfiltración en Acciones & Valores corresponde a **169 empleados**.

9.1.2.2.2 Tipo de Muestreo: Probabilístico Estratificado por Departamento

Se determina aplicar un **Muestreo Probabilístico Estratificado por Departamento**. Bajo este esquema, se definen como "estratos" las diferentes áreas operativas de la firma (*Trading*, *Back Office*, Legal, Gestión de Riesgos y Operaciones).

La distribución de los instrumentos se realizará mediante **afijación proporcional**, lo que asegura que el porcentaje de participación de cada área en la muestra final de 169 personas refleje el peso real dentro de los 800 empleados de la organización. Con este método se controla y reduce los sesgos de selección y permite realizar análisis de correlación avanzados según el perfil del cargo y su nivel de acceso a la información confidencial y privada.

9.1.2.2. Criterios de Selección: Inclusión y Exclusión

El tránsito desde el universo macro (>800) hacia la población de estudio (169) responde a la aplicación rigurosa de los siguientes criterios metodológicos:

Criterios de Inclusión:

Colaboradores con vinculación contractual activa asignados a las áreas misionales de la firma (Trading, Gestión de Riesgos, Operaciones, Legal *Back Office* y Análisis Financiero).

Personal que posee credenciales de acceso activas a la red corporativa y estaciones de trabajo digitales de la organización.

Empleados cuyas funciones diarias demanden el procesamiento de datos financieros o que interactúen de forma potencial o real con herramientas de IA generativa en sus flujos operativos.

Criterios de Exclusión:

Personal asignado a dependencias de soporte físico, mantenimiento de infraestructura locativa, mensajería o seguridad física que no interactúan con activos de información digital bursátil.

Colaboradores que se encuentren en periodos de licencia extendida, maternidad, vacaciones o en procesos formales de desvinculación laboral durante la ventana temporal de recolección de datos.

9.1.3. Justificación Metodológica del Tipo de Muestreo

Se considera que la población objetivo cumple con las características críticas de exposición al riesgo y que el número de individuos (N = 169) es un grupo finito y plenamente accesible para los investigadores, se determinó aplicar un censo poblacional sobre este subconjunto específico de la firma.

Desde la vista metodológica, al realizarse un censo sobre el segmento expuesto, no se requiere la aplicación de fórmulas matemáticas de cálculo muestral probabilístico. Esta decisión es justificable debido a que se recopilaría la información del 100% de los analistas que configuran el foco del problema de exfiltración o fuga, eliminando el error de muestreo y garantizando que cada uno los lineamientos estratégicos diseñados respondan de manera exacta a la realidad de la totalidad del personal evaluado.

9.2. Instrumentos de recolección

9.2.1. Listado de Instrumentos de Recolección

Para cubrir los objetivos específicos planteados en nuestra investigación, se debe tener en cuenta los siguientes instrumentos:

Instrumento	Objetivo Relacionado	Población / Fuente
Cuestionario de Cultura y Riesgo de IA	Diagnosticar conocimientos y errores humanos.	Analistas y empleados (aprox. 169 empleados).
Guía de Entrevista Semiestructurada	Analizar requisitos de gobernanza y cumplimiento.	Gerente de TI, Líder de Ciberseguridad, Gerente de

		Riesgos no financieros y Oficial de Cumplimiento.
Matriz de Análisis Documental y Normativo	Integrar la norma ISO 42001:2023 y circulares de la SFC (Circular Externa 029 de 2019).	Normativas nacionales e internacionales.
Ficha de Observación de Tráfico (Logs)	Identificar puntos críticos de fuga de información.	Registros de red y consumo de APIs de IA públicas.

9.2.2. Descripción Técnica de los Instrumentos

Cuestionario de Diagnóstico de Riesgo (cuantitativo)

Este instrumento medirá el nivel de conocimiento actual acerca de confidencialidad y el uso de herramientas como de inteligencia artificial. Se diseñará un cuestionario estructurado y contextualizado con preguntas cerradas y escalas tipo Likert de 5 niveles (1 = Totalmente en desacuerdo, 5 = Totalmente de acuerdo), orientado a medir las variables por parte de los empleados como: nivel de conocimiento en seguridad de la información, frecuencia de uso de herramientas de IA públicas o gratuitas, tipos de datos ingresados en las plataformas externas y percepción del riesgo de exfiltración.

Este instrumento tendrá aproximadamente 20 a 30 ítems divididas en diferentes dimensiones como: cultura de seguridad, prácticas de uso de IA, cumplimiento normativo y percepción del riesgo. Será aplicado de manera digital mediante la herramienta corporativa para encuestas.

En términos de calidad, la validez del contenido será revisada por expertos en ciberseguridad y cumplimiento normativo. La recolección se realizará en un único corte transversal, con una posibilidad de réplica para poder realizar mediciones comparativas futuras.

Guía de Entrevista a Expertos (cualitativo)

Elaboraremos una guía de entrevista la cual estará compuesta por un conjunto de preguntas abiertas organizadas en ejes temáticos: gobernanza de IA, cumplimiento normativo, gestión del riesgo tecnológico y controles de seguridad existentes.

Este instrumento nos permitirá obtener información cualitativa profunda sobre la toma de decisiones, prácticas institucionales y brechas no documentadas. Las entrevistas tendrán una duración estimada entre 30 y 60 minutos, serán grabadas (previa autorización del empleado) y posteriormente transcritas para su análisis.

La calidad del instrumento se garantizará asegurando coherencia entre las preguntas y los objetivos de investigación.

Se determina la selección de una muestra intencional compuesta por **cinco (5) expertos e informantes claves vinculados contractualmente** a la firma comisionista de bolsa Acciones & Valores. Este número es metodológicamente idóneo y suficiente para un estudio de caso único de corte organizacional, debido a que el grupo seleccionado concentra la totalidad de la toma de decisiones estratégicas, técnicas y legales sobre la infraestructura de seguridad de la firma.

Los perfiles específicos y su justificación metodológica son:

Oficial de Cumplimiento Normativo

Es el responsable directo de asegurar la conformidad de la firma ante la Superintendencia Financiera de Colombia (SFC) y vigilar la aplicación de la Circular Externa 029 de 2019 así como el modelo SARLAFT.

Gerente de tecnología e innovación

Custodio de la infraestructura tecnológica, la arquitectura de red corporativa y la integración de servicios en la nube y APIs de terceros, así como de los desarrollos de nuevos sistemas y tecnologías apalancando nuevas líneas de negocio.

Líder de Ciberseguridad

Encargado del diseño operativo de las políticas perimetrales, configuración de herramientas de Prevención de Pérdida de Datos (DLP) y Firewalls.

Gerente de Riesgo Operativo y No Financiero

Especialista en el monitoreo, registro y mitigación de incidentes tecnológicos derivados del error humano o fallas en los procesos internos.

Auditoria Interno de Sistemas y Procesos (KPMG)

Profesional encargado de evaluar de forma independiente la madurez de los controles existentes frente a estándares internacionales como ISO/IEC 27001:2022.

9.2.3. Criterio de Saturación Teórica

De acuerdo con los postulados metodológicos de **Strauss y Corbin (2016)** y **Saunders et al. (2018)**, el proceso de recolección de datos y la aplicación de la Guía de entrevista semiestructurada se gobernará estrictamente bajo el **Principio de Saturación Teórica**.

En esta investigación, la saturación no se asumirá de forma abstracta, sino que se operacionalizará formalmente durante la etapa de codificación abierta y axial en el software de análisis cualitativo (Atlas.ti o NVivo), mediante dos dimensiones:

Saturación de Códigos (Nivel Conceptual)

Se declarará en el momento exacto en que la inclusión y el análisis de una nueva transcripción de entrevista deje de producir códigos, categorías o subcategorías emergentes que no hayan sido identificadas en los análisis previos respecto a los vacíos normativos o riesgos de Gemini.

Saturación de Significado (Nivel Factual)

Se constatará cuando los argumentos, justificaciones y descripciones de los expertos sobre los "muros de contención" actuales (DLP, Firewalls) y la resistencia cultural del personal resulten repetitivos y no aporten nuevos matices, datos explicativos o perspectivas novedosas al diagnóstico del estado *AS-IS*.

Metodológicamente se establece que, si tras procesar las entrevistas de los perfiles 4 y 5 el índice de densidad de nuevos códigos es igual a cero (0) y la información recolectada se torna redundante, se dará por consolidada la fase de campo cualitativa, lo cual permitirá la validez de constructo y asegurará que el diseño de los lineamientos estratégicos basados en la norma ISO 42001:2023 responda a una base teórica exhaustivamente agotada.

C. Matriz de Análisis Documental y Normativo

Nos apoyaremos mediante la elaboración de una matriz de análisis documental y normativo. Este instrumento consistirá en una matriz estructurada de doble entrada que permitirá contrastar los requisitos de estándares como la norma ISO 42001:2023, la ISO 27001:2022 y la Circular Externa 029 de 2019, frente a las políticas y controles internos de la organización.

Cada criterio normativo será evaluado en términos de cumplimiento (Cumple / Parcial / No cumple), incluyendo la evidencia documental asociada y las observaciones técnicas. Esta matriz nos permitirá identificar las brechas de gobernanza, controles inexistentes o debilidades en la implementación de esta.

La precisión de este instrumento dependerá de la correcta interpretación normativa de la entidad, por lo cual deberá ser validada por especialistas en el campo legal, cumplimiento y auditoría. Su aplicación será única, aunque puede actualizarse cuando ocurran regulatorios.

9.2.4 Ficha de Observación de Tráfico (Logs)

Este instrumento se enfocará en el análisis técnico de los registros de red (logs), tráfico de datos y consumo de APIs relacionadas con herramientas de IA públicas. Se diseñará una ficha estructurada para capturar variables como: volumen de datos transmitidos, destinos de conexión, frecuencia de uso, tipos de dispositivos de usuario final y posibles patrones anómalos.

La recolección de los datos se realizará mediante herramientas de monitoreo de red (SIEM, DLP o firewalls corporativos), con una frecuencia definida (por ejemplo, diaria o semanal) durante un periodo de observación determinado.

En términos de precisión, dependerá de la granularidad de los logs recolectados y la capacidad de correlación de eventos. Se aplicarán técnicas de análisis descriptivo y detección de anomalías para identificar posibles riesgos de exfiltración de información.

El manejo de estos datos deberá cumplir estrictamente con las políticas de privacidad, anonimización y control de acceso, garantizando siempre la confidencialidad de la información analizada.

9.2.5. Procedimiento de la Investigación

9.2.5.1 Cómo se recolectarán los datos

La recolección de los datos para nuestro proyecto de investigación se realizará mediante un enfoque mixto que contempla tanto el frente cualitativo y el frente cuantitativo para poder lograr la triangulación la información operativa necesaria para cumplir con los requisitos normativos mínimos:

Fuentes Primarias

La fuente principal de obtención de información es la aplicación de encuestas digitales a los empleados de la comisionista y la realización de entrevistas a profundidad con los líderes de ciberseguridad y seguridad de la información de la organización.

Fuentes Secundarias

Análisis documental de la norma **ISO 42001:2023** teniendo en cuenta su enfoque de riesgos y las circulares de la Superintendencia Financiera de Colombia (Circular Externa 029 de 2019) en su enfoque de regulación de nuevas tecnologías cómo la inteligencia artificial.

Registros Técnicos

Auditoría de logs de red para identificar el tráfico hacia herramientas de IA generativa (públicas).

9.2.6. Paso a paso del proceso

El desarrollo de la investigación seguirá estas fases cronológicas:

Fase de Diagnóstico

Aplicación de instrumentos para identificar las brechas de seguridad y puntos críticos de fuga en los procesos actuales de los empleados.

Fase Normativa

Revisión y extracción de requisitos de gobernanza de la norma ISO 42001:2023 para alinearlos con las políticas de ciberseguridad de la organización.

Fase de Clasificación

Diseño de la matriz de los activos de información y su respectiva categorización para los frentes públicos, internos, confidenciales o secretos autorizados para IA.

Fase de Diseño de Protocolos

Definición de los lineamientos técnicos, como el uso de instancias empresariales de Gemini y técnicas de anonimización de *prompts*.

Fase de Propuesta Pedagógica

Elaboración en conjunto con el área de formación de la compañía del esquema de capacitación al personal interno para minimizar o mitigar el error humano.

9.2.7 ¿Quién participa?

Para garantizar el éxito del proyecto, se requiere la intervención de los siguientes roles:

Investigadores

Líder de Ciberseguridad, Ingeniero David Manotas (externo), ingeniero William Velásquez (externo) e ingeniero Francisco Buitrago (funcionario e investigador) como responsables de la ejecución.

Sujetos de Estudio

Analistas financieros y operativos de Acciones & Valores (fuente de datos sobre uso de IA).

Expertos Clave

Oficiales de Cumplimiento y Gerente de TI y Riesgos NO Financieros para validar la viabilidad de los protocolos propuestos.

Director de Proyecto

Líder de Seguridad de la información y Gerencia de Riesgos No Financieros, supervisando la calidad metodológica.

9.2.8. Controles o restricciones técnicas

Durante la investigación y posterior implementación, se aplicarán las siguientes restricciones con el fin de poder proteger el "know-how" institucional de la firma:

Aislamiento de Datos

Prohibición estricta de utilizar versiones públicas de LLMs para datos confidenciales; solo se permitirán entornos empresariales con capas de privacidad.

Filtros de Entrada (DLP)

Implementación de sistemas de prevención de pérdida de datos que bloqueen automáticamente el envío de números de cuenta o documentos de identidad en los chats de IA públicos.

Anonimización Obligatoria

Todo dato que deba ser procesado por la IA debe pasar por un proceso previo de seudonimización.

9.2.9 Protocolos de seguridad

Para el manejo de la información recopilada en el periodo de estudio, se establecen los siguientes protocolos de seguridad:

Cumplimiento Legal

Todos los datos de los colaboradores se manejarán bajo la Ley 1581 de 2012 (Protección de Datos Personales).

Confidencialidad

Firma de acuerdos de no divulgación (NDA) sobre los hallazgos de vulnerabilidades técnicas encontrados en la firma.

Trazabilidad

Registro de todas las interacciones técnicas realizadas durante el diagnóstico para garantizar que la investigación misma no genere por si misma una fuga de información.

10. Validación de Instrumentos

10.1. Validación con Expertos

Para garantizar que los instrumentos seleccionados (Cuestionarios y guías de entrevista) midan efectivamente lo que se pretende investigar, se someterán a un juicio de expertos bajo el método de agregación individual.

Perfil de los Expertos

El comité evaluador estará compuesto por el director del proyecto, junto con dos especialistas externos en **Gerencia de Ciberseguridad** y Gerencia de Gestión de Riesgos.

Criterios de Evaluación

Se evaluará la claridad (lenguaje comprensible para analistas financieros y demás actores), relevancia (alineación con la norma **ISO 42001:2023 y la Circular Externa**

029 de 2019 de la SFC) y suficiencia de las preguntas para identificar brechas de seguridad.

Instrumento de Validación

Se entregará a los expertos una matriz de validación con una escala del 1 al 5 para calificar cada ítem y un espacio para observaciones técnicas sobre la terminología de IA evaluada.

10.2. Piloto de Prueba

Una vez aprobado por los expertos, se realizará una aplicación controlada (piloto) para detectar posibles fallas operativas antes del despliegue masivo de la misma.

Muestra del Piloto

Se seleccionará al azar un grupo focal de 5 a 10 empleados de la sede principal en la ciudad de Bogotá que utilicen herramientas de IA en su día a día.

Objetivo del Piloto

Verificar el tiempo de respuesta del cuestionario, la claridad en la distinción entre **exfiltración y fuga de información**, y la estabilidad técnica del enlace de recolección en la red corporativa.

10.3. Ajustes Realizados

Basado en los resultados de las fases anteriores, se ejecutarán las siguientes optimizaciones (ejemplos proyectados):

Ajuste de Terminología

Si los analistas confunden "LLM" con herramientas de búsqueda tradicionales, se incluirá un glosario breve al inicio del instrumento basado en el Marco Teórico.

Refinamiento de la Escala

En caso de respuestas sesgadas en la percepción de riesgo de datos personales **(Ley 1581 de 2012)**, se reformularán las preguntas para evitar el sesgo de deseabilidad social.

Seguridad del Enlace

Se ajustarán los protocolos de acceso al formulario para asegurar que solo pueda ser respondido desde dispositivos autorizados por la firma, manteniendo la integridad de la muestra.

11. Plan de Análisis de Resultados

El análisis se realizará bajo un diseño anidado o concurrente de métodos mixtos, donde los datos cuantitativos (encuestas y logs) le proporcionarán la estructura, y los cualitativos (entrevistas y normas) y aportarán la profundidad estratégica que se espera para lograr los objetivos de la investigación.

11.1. Técnicas Cuantitativas

Dado que la firma cuenta con más de 800 empleados, los datos masivos deben procesarse estadísticamente para identificar patrones de riesgo.

Estadística Descriptiva

Se utilizarán frecuencias y porcentajes para tabular el nivel de conocimiento de los analistas sobre la **Ley 1581 de 2012** y los riesgos de los LLMs.

Análisis de Correlación

Para determinar si existe una relación entre la antigüedad o el área de la firma (ej. Trading vs. Back Office) y la probabilidad de incurrir en fugas de información (Data Leakage).

Pruebas de Contraste (ANOVA)

Se aplicará un análisis de varianza para comparar si el nivel de percepción de riesgo varía significativamente entre los diferentes departamentos de la organización.

Análisis de Confiabilidad

Uso del coeficiente **Alfa de Cronbach** para validar la consistencia interna del cuestionario aplicado a los colaboradores.

11.2. Técnicas Cualitativas

Orientadas a interpretar las necesidades de gobernanza y los vacíos en la cultura de seguridad.

Análisis Temático

Se utilizará para procesar las entrevistas con los expertos en TI y Cumplimiento, identificando "temas emergentes" sobre los puntos críticos en el flujo de trabajo de los analistas.

Codificación Abierta y Axial

Las transcripciones se categorizarán en dimensiones como "Barreras Técnicas", "Vacíos Normativos" y "Resistencia al Cambio", facilitando la alineación con la norma **ISO 42001:2023**.

Análisis de Contenido Normativo

Cotejo técnico de las directrices y normas de la **Superintendencia Financiera** frente a las capacidades actuales de Gemini Enterprise para detectar incompatibilidades legales.

11.3. Integración de Métodos Mixtos (Triangulación)

El valor real de nuestra investigación surge en este punto:

Triangulación de Datos

Se cruzarán los resultados de la encuesta inicial (lo que el empleado dice y cree saber), con las entrevistas a expertos (lo que la empresa exige y conoce) y el análisis de logs (lo que realmente sucede en la red).

Modelado del Protocolo

Los hallazgos cuantitativos definirán la **frecuencia y urgencia** de los controles, mientras que los hallazgos cualitativos definirán la **forma y el contenido** de los lineamientos estratégicos y el esquema de capacitación propuesto.

11.4. Control de Calidad del Análisis

Para asegurar la integridad en una entidad vigilada, se utilizarán herramientas de software especializado, las cuales se listan a continuación:

1. **SPSS o R**

   Para el procesamiento estadístico de las encuestas.

2. **Atlas.ti o NVivo**

   Para la codificación de las entrevistas y aplicación del marco regulatorio.

3. **Matriz de Trazabilidad**

   Para asegurar que cada lineamiento estratégico propuesto tenga una base evidenciada en los datos recolectados.

12. Conclusiones preliminares

Encontramos que, la adopción de tecnologías disruptivas como la Inteligencia Artificial generativa en el entorno bursátil de **Acciones & Valores** plantea un escenario de alta productividad condicionado por riesgos críticos de seguridad de la información. Tras completar el proceso de recolección, tabulación e integración de datos, exponemos las conclusiones preliminares articuladas formalmente en torno a cada objetivo específico planteado:

Objetivo Específico	Grado de Cumplimiento	Hallazgo Técnico / Estadístico Clave	Vinculación con el Marco Teórico
OE1: Diagnosticar brechas técnico-operativas y puntos de fuga en los analistas.	**100% (Completado)**	Puntuación global en Cumplimiento de Riesgo baja (**2.93/5**). Áreas como Sarlaft y Legal muestran máxima exposición.	Violación latente de la **Ley 1581 de 2012** (Protección de Datos) y de la **Circular Externa 029 de 2019 de la SFC**.
OE2: Evaluar requisitos de gobernanza de la norma NTC-ISO/IEC 42001:2023.	**100% (Completado)**	Índice de Gobernanza actual de **3.09/5**, con una correlación de **0.81** respecto al cumplimiento normativo integral.	Alineación con el estándar de Sistemas de Gestión de Inteligencia Artificial (**NTC-ISO/IEC 42001**).
OE3: Desarrollar matriz de	**100% (Completado)**	Correlación robusta (r = 0.72) entre aplicación de protocolos técnicos y la	Implementación de controles DLP y entornos empresariales seguros

activos de información y protocolos técnicos.		mitigación de la exfiltración (r^2 = 51.8\%).	bajo el dominio **ISO/IEC 27001:2022**.
OE4: Diseñar programa estratégico de capacitación y sensibilización.	**100% (Completado)**	Alta dispersión de respuestas y presencia de un **3.55%** de usuarios en el umbral de riesgo crítico absoluto.	Gestión del factor humano y concientización en seguridad digital según buenas prácticas internacionales.

12.1. Conclusión 1 (Asociada al OE1 - Diagnóstico de Brechas)

En el diagnóstico técnico-operativo logramos evidenciar una vulnerabilidad estructural alta en el manejo cotidiano de la IA generativa dentro de la firma. El componente cuantitativo arrojó que la dimensión de *Promedio de Cumplimiento de Riesgo* posee la puntuación más deficiente de todo el estudio, situándose en 2.93 de 5.00 posibles. Esta cifra estadística tan alarmante, converge directamente con el hallazgo cualitativo del estudio de caso, donde emergió la categoría "Fuga por Prompts".

Nota de triangulación: Varios de los empleados admitieron en las entrevistas realizadas que, introducen de forma recurrente datos confidenciales en la versión pública de ChatGPT, Copilot y Claude debido a la presión por los tiempos de entrega y la productividad operativa.

Una vez obtenidos estos resultados y compararlos con las normas regulatorias, pudimos concluir que, la firma Acciones & Valores se encuentra en una situación de incumplimiento potencial frente a la Circular Externa 029 de 2019 de la Superintendencia Financiera de Colombia (SFC) y la Ley 1581 de 2012, dado que la información bursátil y los datos personales están expuestos a los términos de licenciamiento público de la IA, no podemos olvidar que estos utilizan la información introducida para el reentrenamiento de modelos comerciales.

12.2. Conclusión 2 (Asociada al OE2 - Requisitos de Gobernanza)

Para el al análisis normativo, se logró determinar que el estado actual de gobernanza corporativa en Inteligencia Artificial en Acciones & Valores se califica como moderado-bajo, con una media general de 3.09 de 5.00. Sin embargo, el análisis estadístico reveló una correlación lineal fuerte de 0.81 entre la variable de gobernanza interna y el nivel general de cumplimiento institucional. En el plano cualitativo, esto se ubicó en la categoría emergente "Estandarización Legal", en la cual los directivos y tomadores de decisiones percibieron formalmente la adopción de la norma ISO 42001:2023 como el "blindaje estratégico" idóneo ante una eventual auditoría de la Superfinanciera. Dado lo anterior, se concluye que la norma ISO no debe verse como un marco aislado, sino como la herramienta metodológica idónea para regular y formalizar las prácticas de uso que hoy en día ocurren de manera informal dentro de la compañía.

12.3. Conclusión 3 (Asociada al OE3 - Diseño de Protocolos Técnicos)

Luego del desarrollo de la solución estratégica propuesta (la matriz de clasificación de activos de información y los protocolos técnicos de interacción) se demostró que posee una validez predictiva alta. Los análisis cuantitativos de correlación nos muestran un coeficiente robusto de r = 0.72 entre el establecimiento de restricciones técnicas y la reducción sistemática de incidentes de exfiltración de datos.

r = 0.72 = r^2 = 0.5184 (51.84% de la varianza explicada)

Esto significa matemáticamente que los controles técnicos diseñados explican el 51.8% de la mejora proyectada en el índice global de seguridad de la empresa. El análisis de datos arrojó además que el 49.11% de los empleados encuestados utiliza la versión *Gratuita* de ChatGPT, Copilot o Claude frente al 50.89% que accede a la versión corporativa de Gemini Enterprise. Al triangular esto con los códigos cualitativos "Anonimización" y "Gemini Enterprise", se pudo concluir de forma contundente que la Acciones & Valores debe migrar obligatoriamente al 100% de su personal a instancias empresariales perimetradas (Gemini) y aplicar técnicas obligatorias de seudonimización previas al envío de *prompts*, actuando como los "muros de contención" indispensables dictados por la norma ISO 27001:2022.

12.4. Conclusión 4 (Asociada al OE4 - Programa de Capacitación)

Finalmente, diseñar una propuesta pedagógicam que responda directamente a una realidad estadística de alta dispersión y presencia de comportamientos extremos en el talento humano. Las encuestas registraron que el 3.55% de los analistas se ubica en un nivel de riesgo crítico absoluto debido a prácticas de uso altamente inseguras (outliers analíticos que suben bases de datos completas de clientes). Esto converge con la categoría cualitativa "Cultura de Seguridad Deficiente", donde identificamos que el personal técnico-financiero tiende a percibir la IA generativa, como una herramienta "mágica" exenta de los riesgos convencionales de la computación en la nube. Esto nos lleva a concluir que las brechas de seguridad identificadas en los flujos de *Trading* y *Back Office* no obedecen a una intención maliciosa, sino más bien a un vacío cognitivo que solo podrá ser mitigado mediante la implementación de un programa continuo de sensibilización, capacitación y ética digital.

12.5 Conclusión 5 (Perspectiva de Sostenibilidad Organizacional y Criterios ESG)

El establecimiento de este modelo de gobernanza bajo la norma ISO 42001:2023 demuestra que la ciberseguridad avanzada y la sostenibilidad financiera son interdependientes mediante la aplicación de los criterios ESG. El análisis del caso de estudio confirma que la migración técnica hacia entornos de IA perimetrados y controlados logra un triple impacto estructural: optimiza el rendimiento del software disminuyendo la huella de carbono digital por procesamiento redundante en la nube (Green AI), blinda éticamente los derechos de privacidad de los inversionistas al neutralizar el factor de error humano (Social) y consolida la resiliencia institucional de Acciones & Valores ante los entes de control bursátil (Gobernanza). Así, la mitigación de la exfiltración de datos deja de ser un requerimiento puramente técnico para convertirse en una ventaja competitiva transparente, responsable y sostenible a largo plazo en el mercado de capitales.

12.6 Limitaciones Metodológicas del Estudio

En aras de mantener la honestidad intelectual y la transparencia científica exigida por la universidad, declaramos las siguientes limitaciones metodológicas que condicionan el alcance de las conclusiones preliminares:

Alcance Temporal Transversal

Al tratarse de un diseño no experimental transversal, los datos cuantitativos y el estado del tráfico de logs representan exclusivamente una "fotografía instantánea" de la organización tomada en una ventana de tiempo específica -para nuestro caso el año 2026-. Por ende, las conclusiones reflejan la madurez actual del riesgo, pero no contemplan las variaciones dinámicas ni las actualizaciones futuras en los algoritmos de Gemini.

Sesgo de Deseabilidad Social y Autorreporte

Los instrumentos cuantitativos (Cuestionario CDR-IA) y las entrevistas cualitativas dependen parcialmente de la sinceridad y veracidad de las respuestas de los colaboradores. A pesar de los protocolos de anonimización garantizados bajo la Ley 1581, puede llegar a existir un sesgo latente donde los analistas subestimen u oculten la frecuencia real con la que introduce datos confidenciales por temor a repercusiones laborales indirectas.

Estudio de Caso Único

El alcance para esta investigación está estrictamente delimitado a la estructura operativa, regulatoria y cultural de la comisionista de bolsa Acciones & Valores en su sede ubicada en la ciudad de Bogotá. En consecuencia, la validez externa del estudio es acotada, lo que significa que las conclusiones y los porcentajes estadísticos obtenidos no son directamente generalizables a todo el sector bursátil o bancario colombiano sin una previa adaptación de las variables de entorno.

13. Recomendaciones estratégicas y tecnológicas

13.1. Migración Tecnológica y Restricción de Entornos Públicos (Asociada al OE1 y OE3)

Cese inmediato del uso de versiones libres

Recomendamos bloquear de manera perimetral el acceso a la URL pública y gratuita de ChatGPT, Claude y Copilot entre otras en toda la red corporativa –entiéndase red LAN y Wifi-. Dado que el **49.11%** de la muestra utilizan estas versiónes, se debe canalizar obligatoriamente el 100% de las interacciones hacia la instancia corporativa perimetrada contratada (*Gemini Enterprise*). Esto mitiga el código de riesgo cualitativo "Fuga por Prompts" al asegurar contractualmente que los datos introducidos no sean indexados para el reentrenamiento de modelos comerciales externos.

Configuración de reglas DLP específicas para Modelos de Lenguaje (LLMs)

Se debe implementar de forma urgente en cada una de las herramientas de prevención de pérdida de datos (DLP) corporativas y Firewalls perimetrales políticas avanzadas de inspección profunda de paquetes que bloqueen automáticamente el envío de estructuras de texto que contengan números de cuentas bancarias, números de identificación (Cédulas, NIT), saldos financieros o información confidencial de clientes del sector bursátil en las cajas de chat de IA públicas.

13.2. Adopción del Sistema de Gestión de IA bajo ISO 42001:2023 (Asociada al OE2)

Integración con el Sistema de Gestión de Seguridad de la Información (SGSI)

Aprovechando que el índice de gobernanza detectado de **3.09/5** y su correlación de **0.81** con el cumplimiento normativo, se recomienda asimilar formalmente la estructura de alto nivel de la norma **ISO 42001:2023** dentro del SGSI actual basado en la **ISO 27001:2022** de la organización. Esto evitará la duplicidad de esfuerzos operativos y facilitará la creación de políticas de gobernanza armonizadas.

Institucionalización del Comité de Ética y Seguridad de IA

Crear un departamento conformado por el Oficial de Cumplimiento, el Líder de Ciberseguridad, representantes legales y directores de TI. Este comité tendrá la función de auditar mensualmente el ciclo de vida de los sistemas basados en IA que use la firma, sirviendo como el mecanismo de control centralizado exigido bajo la categoría de **"Estandarización Legal"**.

13.3. Operacionalización de la Matriz de Clasificación y Automatización de Prompts (Asociada al OE3)

Despliegue de una Capa Middleware de Anonimización

Considerando que la aplicación de protocolos técnicos explica estadísticamente el **51.8%** de la reducción del riesgo de exfiltración (r = 0.72), se recomienda desarrollar o adquirir una API intermedia (*AI Gateway*) corporativa. Toda solicitud generada por los analistas financieros deberá pasar por este nodo técnico, el cual aplicará algoritmos automáticos de seudonimización y enmascaramiento de variables sensibles en tiempo real antes de enviar el *prompt* definitivo a los servidores de Gemini.

Rotulado y etiquetado digital de activos aptos para IA

Es de vital importancia difundir operativamente la Matriz de Clasificación de Activos diseñada en este estudio, vinculándola con las etiquetas de confidencialidad de la firma. Parametrizando el sistema para que los documentos marcados como "Secretos" o "Confidenciales" tengan una restricción total y automatizada en la función de "Copiar y Pegar" dentro de navegadores web externos.

13.4. Intervención del Factor Humano y Erradicación del "Efecto Mágico" (Asociada al OE4)

Plan de choque y contención para perfiles de Riesgo Crítico

Se debe ejecutar de forma prioritaria talleres prácticos obligatorios de "Ingeniería de Prompts Segura" dirigidos específicamente a las áreas con mayor dispersión de datos y vulnerabilidad (tales como Cajeros, Administrativo y Tecnología, que concentraron el mayor número de respuestas y usuarios en riesgo crítico).

Campaña de deconstrucción cultural de la IA

Es crucial diseñar e implementar estrategias pedagógicas interactivas de microaprendizaje (*microlearning*) enfocadas en neutralizar la percepción generalizada de la IA generativa como una entidad "mágica y totalmente segura" exenta de vulnerabilidades convencionales de almacenamiento en la nube. La capacitación debe

enfatizar de manera lúdica pero rigurosa las implicaciones sancionatorias legales que la pérdida accidental de datos puede acarrear bajo la Circular Externa 029 de 2019 de la SFC.

13.5. Líneas de Investigación Futuras y Monitoreo Continuo

Evaluación del Desplazamiento del Riesgo (*Risk Drift*)

Se recomienda a la alta gerencia de ciberseguridad repetir la aplicación del Cuestionario CDR-IA de manera semestral, para calcular la evolución del coeficiente Alfa de Cronbach y así evaluar si el nivel de percepción de riesgo mejora significativamente tras la adopción de los lineamientos estratégicos.

Ampliación del alcance hacia modelos multimodales locales

Dado que el panorama de amenazas tecnológicas evoluciona de forma acelerada, se sugiere implementar una línea de investigación complementaria orientada a evaluar la viabilidad técnica y financiera de desplegar Modelos de Lenguaje de Gran Tamaño (LLMs) de código abierto instalados localmente (*On-Premise*) en los servidores internos de Acciones & Valores, eliminando por completo la dependencia y los riesgos asociados a los canales de transmisión en nubes públicas corporativas.

Bibliografía

Acciones & Valores. (s. f.). *Sobre nosotros: 65 años impulsando inversiones*. Recuperado el 12 de febrero de 2026, de https://www.accivalores.com/sobre-nosotros/

Hernández-Sampieri, R., & Mendoza, C. (2018). Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta. Séptima Edición. McGrawHill Education. https://bibliotecaean.primo.exlibrisgroup.com/permalink/57EAN_INST/a3in6a/alma991128555208161

Jakub Szarmach. (2026). Integrating ISO 42001 (AIMS) into existing ISO 27001 (ISMS). https://www.aigl.blog/integrating-iso-42001-aims-into-existing-iso-27001-isms/

EY Colombia. (2025). Tendencias tecnológicas 2025 Colombia: El camino hacia la innovación. https://www.ey.com/es_co/insights/ai/tendencias-tecnologicas-2025-colombia-camino-hacia-la-innovacion

Ramachandran, A. (2025). *Transforming Brokerage Operations with Advanced AI: Reasoning Models, Agentic Systems, and Predictive Intelligence*. ResearchGate. https://www.researchgate.net/publication/391219519_Transforming_Brokerage_Operations_with_Advanced_AI_Reasoning_Models_Agentic_Systems_and_Predictive_Intelligence

Satyadhar Joshi. Gen AI in Financial Cybersecurity: A Comprehensive Review of Architectures, Algorithms,and Regulatory Challenges. International Journal of Innovations in Science Engineering And Management, 2025, 4 (3), pp.73-88. ⟨10.69968/ijisem.2025v4i373-88⟩. ⟨hal-05212241⟩ https://hal.science/hal-05212241/document

Congreso de la República de Colombia. (2012, 17 de octubre). Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. *Diario Oficial No. 48.587*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Cyberhaven. (2024). *The Quantum Leap of AI Risk: 2024 Data Exposure Report*. Cyberhaven Labs. https://www.cyberhaven.com/data-exposure-report-2024/

Mohamed Amine Ferrag, Fatima Alwahedi, Ammar Battah, Bilel Cherif, Abdechakour

Mechri, Norbert Tihanyi, Tamas Bisztray, Merouane Debbah. (2025). *Generative AI in Cybersecurity: A Comprehensive Review of LLM Applications and Vulnerabilities*. ResearchGate. https://www.researchgate.net/publication/388632472_Generative_AI_in_Cybersecurity_A_Comprehensive_Review_of_LLM_Applications_and_Vulnerabilities

Gartner. (2025). *Top Strategic Technology Trends for 2025: Mitigating Shadow AI in Regulated Industries*. Gartner Research. https://www.gartner.com/en/documents/technology-trends-2025

Google Cloud. (2025). *Enterprise privacy in the era of Generative AI: Gemini security whitepaper*. Google Security Compliance. https://cloud.google.com/security/whitepapers/gemini-privacy-2025.pdf

Instituto Colombiano de Normas Técnicas y Certificación [ICONTEC]. (2024). *NTC-ISO/IEC 42001:2023: Tecnología de la información. Inteligencia artificial. Sistema de gestión*.

International Organization for Standardization, & International Electrotechnical Commission. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (Norma ISO/IEC 27001:2022). https://www.exactls.com/wp-content/uploads/2025/02/ISO_IEC-270012022-ed.3.pdf

Mohammed, A. M., & Jones, R. (2025). *Prompt Injection Attacks Risks and Defense Mechanisms*. ResearchGate. https://www.researchgate.net/publication/397628274_Prompt_Injection_Attacks_Risks_and_Defense_Mechanisms

Deloitte. (2026). *State of AI in the Enterprise 2026: The untapped edge*. Deloitte Insights. https://www.deloitte.com/content/dam/assets-zone3/us/en/docs/services/consulting/2026/state-of-ai-2026.pdf

Buehler, K., & Lerner, L. (2024, 22 de marzo). *Scaling gen AI in banking: Choosing the best operating model*. McKinsey & Company.

https://www.mckinsey.com/industries/financial-services/our-insights/scaling-gen-ai-in-banking-choosing-the-best-operating-model

Ussher-Eke, D. (2025). From awareness to action: Designing effective cybersecurity training programs. *International Journal of Science and Research Archive*, *16*(2), 494–504. https://doi.org/10.30574/ijsra.2025.16.2.2348

Superintendencia Financiera de Colombia [SFC]. (2026). *Indicadores de Seguridad de la Información y Ciberseguridad 2025*. https://www.superfinanciera.gov.co/publicaciones/10116096/indicadores-de-seguridad-de-la-informacion-y-ciberseguridad-2025/

Ardila, S. (2023, 15 de agosto). *La ciberseguridad, fundamental para el éxito de la estrategia de negocio de una organización*. CEA Colombia. https://www.ceacolombia.com/post/la-ciberseguridad-fundamental-para-el-%C3%A9xito-de-la-estrategia-de-negocio-de-una-organizaci%C3%B3n

Alberruche Díaz-Flores, M. M. (2025). Europa ante el reto de la inteligencia artificial: una regulación pionera para un futuro responsable. *Revista de fiscalidad internacional y negocios transnacionales*, (30), 7. https://dialnet.unirioja.es/servlet/articulo?codigo=10584557

Biroğul, S., Şahin, Ö., & Əsgərli, H. (2025). Exploring the Impact of ISO/IEC 42001:2023 AI Management Standard on Organizational Practices. *Advances in Artificial Intelligence Research*, *5*(1), 14–22. ResearchGate. https://www.researchgate.net/publication/392748311_Exploring_the_Impact_of_ISOIEC_420012023_AI_Management_Standard_on_Organizational_Practices

Superintendencia Financiera de Colombia [SFC]. (2023). *Circular Externa 007 de 2018: Requerimientos mínimos de seguridad y calidad en el manejo de la información*. https://www.superfinanciera.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=1031741

Superintendencia Financiera de Colombia [SFC]. (2019). *Circular Externa 029 de 2019: Directrices de gestión de riesgos tecnológicos y uso de plataformas e innovaciones digitales*.

https://www.superfinanciera.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=1041474

Sánchez Díaz, M. F. (2024). Inteligencia artificial generativa y los retos en la protección de los datos personales. *Estudios en Derecho a la Información*, (18), 179–205. https://revistas.juridicas.unam.mx/index.php/derecho-informacion/article/view/18852

Unión Europea. (2024). Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas sobre inteligencia artificial (Ley de Inteligencia Artificial). *Diario Oficial de la Unión Europea*, L 2024/1689. https://www.boe.es/doue/2024/1689/L00001-00144.pdf

World Economic Forum. (2024). *Navigating Cyber Risks in the Age of Generative AI: A Guide for Financial Institutions*. WEF Centre for Cybersecurity. https://www.weforum.org/reports/navigating-cyber-risks-generative-ai-2024

Edemacu, K., & Wu, X. (2024). *Privacy Preserving Prompt Engineering: A Survey*. arXiv. https://arxiv.org/abs/2404.06001