Términos, condiciones y políticas de seguridad de Janalytics

Marco legal y de protección de datos para los servicios de inteligencia artificial agentic (Agentic OS)

Elaborado por

Jassen Aldair Camargo Caicedo

Administrador de empresas · Especialista en Analítica de datos

23 de septiembre de 2026 · Versión 1.0

TÉRMINOS, CONDICIONES Y POLÍTICAS DE SEGURIDAD

Control del documento

Documento	Autor	Versión	Fecha	Clasificación
Términos, condiciones y políticas de seguridad de Janalytics	Jassen Aldair Camargo Caicedo	1.0	23 de septiembre de 2026	Uso interno / técnico

Índice

Control del documento 2
Índice 3
1. Introducción y marco del documento 10
1.1 Propósito . . . 10
1.2 Alcance y a quién aplica . . . 10
1.3 Estructura del documento . . . 10
1.4 Metodología y fuentes . . . 11
2. Resumen ejecutivo 11
2.1 Qué ofrece Janalytics . . . 11
2.2 Los cuatro pilares de cumplimiento . . . 11
2.3 Estado de cumplimiento y compromisos . . . 12
2.4 Qué puede exigir el cliente . . . 12
3. Glosario 12
3.1 Términos legales . . . 12
3.2 Términos de inteligencia artificial y datos . . . 13
3.3 Términos contractuales . . . 14
4. Primer pilar: retención cero de datos (Zero Data Retention) 14
4.1 Qué significa exactamente retención cero . . . 14
4.2 Por qué importa . . . 15
4.3 Cómo lo implementa Janalytics . . . 15
4.4 Lo que Janalytics sí conserva . . . 15
4.5 Límites honestos de la retención cero . . . 16
5. Segundo pilar: datos sin entrenamiento de modelos 16
5.1 La distinción que casi nadie hace . . . 16
5.2 Qué compromete Janalytics . . . 16
5.3 Coherencia con el régimen de datos personales . . . 17
5.4 Verificación . . . 17
6. Tercer pilar: cumplimiento de la Ley 1581 de 2012 17
6.1 El régimen general de protección de datos personales . . . 17
6.2 Principios rectores . . . 18
6.3 Derechos de los titulares . . . 18
6.4 Roles: responsable y encargado . . . 19
6.5 Autorización y aviso de privacidad . . . 19
6.6 Políticas de tratamiento y su publicación . . . 19
6.7 Registro Nacional de Bases de Datos . . . 20
6.8 Transferencia y transmisión internacional . . . 20

6.9 Seguridad y responsabilidad demostrada . . . 20
6.10 Régimen sancionatorio . . . 20
7. Cuarto pilar: ISO/IEC 27001 e ISO/IEC 42001 21
7.1 Qué exige ISO/IEC 27001 . . . 21
7.2 Cómo se alinea Janalytics . . . 21
7.3 Por qué ISO/IEC 42001 y no solo ISO/IEC 27001 . . . 22
7.4 Aplicación conjunta en el Agentic OS . . . 22
7.5 Declaración de estado . . . 22
8. Marco normativo colombiano aplicable a los servicios de Janalytics 22
8.1 Criterio de identificación de normas . . . 22
8.2 Protección de datos personales . . . 23
8.3 Circular Externa 002 de 2024 de la SIC . . . 23
8.4 Circular Externa 003 de 2024 de la SIC . . . 24
8.5 Delitos informáticos: Ley 1273 de 2009 . . . 24
8.6 Comercio electrónico y validez del contrato digital: Ley 527 de 1999 . . . 24
8.7 Protección al consumidor: Ley 1480 de 2011 . . . 25
8.8 Propiedad intelectual: Ley 23 de 1982 y Decisión Andina 351 de 1993 . . . 25
8.9 Conectividad y continuidad . . . 25
9. Regulación emergente: inteligencia artificial en Colombia 25
9.1 Advertencia sobre el estado de las normas . . . 25
9.2 Política Nacional de Inteligencia Artificial: CONPES 4144 de 2025 . . . 26
9.3 Proyecto de Ley de Inteligencia Artificial . . . 26
9.4 Qué implica para Janalytics . . . 26
10. Marco internacional de referencia 27
10.1 Por qué mirar fuera de Colombia . . . 27
10.2 Reglamento General de Protección de Datos de la Unión Europea . . . 27
10.3 Reglamento Europeo de Inteligencia Artificial . . . 27
10.4 NIST AI Risk Management Framework . . . 27
10.5 Principios de la OCDE y normas ISO . . . 27
10.6 Políticas de datos de los proveedores de modelos . . . 27
11. Matriz de cumplimiento 28
11.1 Cómo leer la matriz . . . 28
11.2 Correspondencia con ISO/IEC 27001 . . . 29
12. Riesgos legales y de seguridad identificados 29
12.1 Metodología . . . 29
12.2 Matriz de riesgos . . . 29
12.3 Riesgos no cubiertos y límites . . . 30

13. Identificación del prestador del servicio 30
14. Objeto y descripción del servicio 31
14.1 Objeto . . . 31
14.2 Componentes del servicio . . . 31
14.3 Exclusiones . . . 31
14.4 Entregables . . . 31
15. Aceptación de los términos 32
15.1 Formas de aceptación . . . 32
15.2 Validez del contrato electrónico . . . 32
15.3 Documentos que integran el acuerdo . . . 32
16. Capacidad legal y registro 32
17. Naturaleza del servicio y supervisión humana 32
17.1 Obligación de medio . . . 32
17.2 Supervisión humana . . . 33
17.3 Deber de revisión del cliente . . . 33
17.4 Declaración sobre el uso de IA . . . 33
18. Acceso, cuentas, credenciales y pases 33
18.1 Usuarios autorizados . . . 33
18.2 Acceso por pase . . . 33
18.3 Credenciales y seguridad de la cuenta . . . 33
18.4 Suspensión de accesos . . . 33
19. Planes, precios, facturación y pagos 34
19.1 Planes . . . 34
19.2 Precios y moneda . . . 34
19.3 Facturación y pago . . . 34
19.4 Costos de terceros . . . 34
19.5 Impuestos . . . 34
20. Plazo, vigencia, suspensión y terminación 34
20.1 Vigencia . . . 34
20.2 Renovación . . . 34
20.3 Terminación . . . 34
20.4 Suspensión . . . 35
20.5 Efectos de la terminación . . . 35
21. Obligaciones de Janalytics 35
22. Obligaciones del cliente 35
23. Uso aceptable y usos prohibidos 36
23.1 Principio general . . . 36

23.2 Usos prohibidos . . . 36
23.3 Consecuencias . . . 36
24. Propiedad intelectual 37
24.1 Titularidad de la plataforma . . . 37
24.2 Datos y contenidos del cliente . . . 37
24.3 Entregables . . . 37
24.4 Contenido generado con inteligencia artificial . . . 37
24.5 Marcas y referencias . . . 37
24.6 Retroalimentación . . . 37
25. Confidencialidad 38
25.1 Alcance . . . 38
25.2 Excepciones . . . 38
25.3 Duración . . . 38
25.4 Personas con acceso . . . 38
26. Protección de datos personales: roles y garantías 38
26.1 Distribución de roles . . . 38
26.2 Obligaciones de Janalytics como encargado . . . 38
26.3 Subencargados . . . 38
26.4 Transferencia y transmisión internacional . . . 39
26.5 Incidentes que afecten datos personales . . . 39
26.6 Derechos de los titulares . . . 39
27. Garantías, responsabilidad e indemnidad 39
27.1 Garantías . . . 39
27.2 Limitación de responsabilidad . . . 39
27.3 Eximentes . . . 39
27.4 Responsabilidad frente a los titulares . . . 39
27.5 Indemnidad . . . 40
27.6 Seguro . . . 40
28. Niveles de servicio y soporte 40
28.1 Disponibilidad . . . 40
28.2 Tiempos de respuesta y resolución . . . 40
28.3 Ventanas de mantenimiento . . . 40
28.4 Exclusión del SLA . . . 40
29. Modificaciones de los términos 41
29.1 Regla general . . . 41
29.2 Límites . . . 41
29.3 Control de versiones . . . 41

30. Comunicaciones y notificaciones 41
31. Ley aplicable y solución de controversias 41
31.1 Ley aplicable . . . 41
31.2 Reclamación directa . . . 41
31.3 Jurisdicción . . . 41
31.4 Protección de datos . . . 42
32. Disposiciones varias 42
32.1 Integridad . . . 42
32.2 Divisibilidad . . . 42
32.3 Cesión . . . 42
32.4 Independencia de las partes . . . 42
32.5 Ausencia de renuncia . . . 42
32.6 Idioma . . . 42
32.7 Subsistencia . . . 42
33. Política de seguridad de la información 42
33.1 Declaración de la política . . . 42
33.2 Alcance del sistema de gestión . . . 43
33.3 Principios rectores . . . 43
33.4 Responsabilidades . . . 43
34. Modelo de seguridad y arquitectura de confianza 43
34.1 Aislamiento por cliente . . . 43
34.2 Exposición mínima . . . 43
34.3 Autenticación de las comunicaciones internas . . . 43
34.4 Principio de no confianza en el contenido . . . 44
34.5 Gestión de activos . . . 44
35. Gestión de accesos e identidad 44
35.1 Registro y aprobación de accesos . . . 44
35.2 Autenticación . . . 44
35.3 Mínimo privilegio y revisión . . . 44
35.4 Acceso de terceros . . . 44
35.5 Registro de actividad . . . 44
36. Cifrado y protección de datos 44
36.1 Cifrado en tránsito . . . 45
36.2 Cifrado en reposo . . . 45
36.3 Clasificación y manejo . . . 45
36.4 Separación de entornos . . . 45
36.5 Destrucción segura . . . 45

37. Ciclo de vida y retención de la información 45
37.1 Principio de conservación mínima . . . 45
37.2 Plazos de retención . . . 45
37.3 Supresión a solicitud . . . 46
37.4 Supresión a la terminación . . . 46
38. Seguridad de proveedores y subencargados 46
38.1 Evaluación previa . . . 46
38.2 Obligaciones contractuales . . . 46
38.3 Seguimiento . . . 46
38.4 Transparencia sobre proveedores . . . 46
39. Gestión de incidentes de seguridad y notificación 46
39.1 Definición y clasificación . . . 46
39.2 Ciclo de respuesta . . . 47
39.3 Notificación al cliente . . . 47
39.4 Colaboración con el responsable . . . 47
39.5 Medidas tras el incidente . . . 47
40. Continuidad del negocio y recuperación 47
40.1 Objetivo . . . 47
40.2 Copias de seguridad . . . 47
40.3 Objetivos de recuperación . . . 47
40.4 Pruebas . . . 47
40.5 Dependencia de terceros . . . 48
41. Auditoría, monitoreo y registros 48
41.1 Monitoreo . . . 48
41.2 Registros . . . 48
41.3 Retención de registros . . . 48
41.4 Auditoría interna . . . 48
41.5 Registro de tratamiento de datos . . . 48
42. Gestión de riesgos y cumplimiento continuo 48
42.1 Enfoque de riesgos . . . 48
42.2 Tratamiento . . . 48
42.3 Cumplimiento normativo . . . 48
42.4 Mejora continua . . . 49
42.5 Declaración de aplicabilidad . . . 49
43. Auditorías y derechos de verificación del cliente 49
43.1 Derecho de información . . . 49
43.2 Evidencia documental . . . 49

43.3 Auditorías del cliente . . . 49
43.4 Autoridades . . . 49
44. Formación y cultura de seguridad 49
44.1 Concienciación . . . 49
44.2 Compromiso del personal . . . 49
44.3 Selección y salida . . . 50
44.4 Cultura de reporte . . . 50
Anexo A. Política de tratamiento de datos personales 51
A.1 Identificación del responsable . . . 51
A.2 Ámbito de aplicación . . . 51
A.3 Finalidades del tratamiento . . . 51
A.4 Derechos del titular . . . 51
A.5 Persona responsable de la atención de solicitudes . . . 51
A.6 Procedimiento para ejercer los derechos . . . 51
A.7 Seguridad . . . 51
A.8 Vigencia . . . 51
Anexo B. Aviso de privacidad 53
Anexo C. Contrato de transmisión de datos personales 54
C.1 Partes y roles . . . 54
C.2 Alcance del tratamiento . . . 54
C.3 Obligaciones de Janalytics . . . 54
C.4 Subencargados y transmisión internacional . . . 54
C.5 Responsabilidad . . . 54
C.6 Duración . . . 55
Anexo D. Correspondencia con los controles de ISO/IEC 27001:2022 56
Anexo E. Referencias 57
E.1 Normatividad colombiana . . . 57
E.2 Circulares de la Superintendencia de Industria y Comercio . . . 57
E.3 Política pública y regulación emergente . . . 57
E.4 Estándares internacionales . . . 58
E.5 Políticas de datos de proveedores de modelos . . . 58
Anexo F. Historial de versiones 59

1. Introducción y marco del documento

1.1 Propósito

Este documento reúne, en un solo instrumento, los términos y condiciones que regulan la relación entre Janalytics y sus clientes, y las políticas de seguridad de la información y de protección de datos personales que Janalytics aplica en la operación de sus servicios de inteligencia artificial agentic. El objetivo es doble: primero, dar al cliente reglas claras, verificables y exigibles sobre cómo se contrata, se ejecuta y se termina el servicio; segundo, demostrar de forma documentada que el tratamiento de la información del cliente se realiza conforme al ordenamiento jurídico colombiano, en particular la Ley 1581 de 2012 y sus decretos reglamentarios.

El documento nace de una decisión de fondo: Janalytics no quiere ofrecer automatización con inteligencia artificial sin un respaldo jurídico y de seguridad explícito. Un agente que lee la nómina de una empresa, que procesa facturas, que responde tickets o que audita bases de datos maneja información sensible desde el punto de vista operativo y, con frecuencia, datos personales de terceros. Por eso, además de describir el servicio, este instrumento fija compromisos concretos de retención cero, no entrenamiento de modelos, cumplimiento normativo y gestión de seguridad, y los traduce en obligaciones contractuales.

1.2 Alcance y a quién aplica

Este documento aplica a todo cliente que contrate cualquiera de los servicios de Janalytics, con independencia del canal de contratación. Se aplica igualmente a los usuarios autorizados por el cliente, a los terceros que el cliente conecte al servicio y a los proveedores y subencargados que Janalytics utilice en la cadena de tratamiento. El documento cubre tres dimensiones del servicio:

- **Dimensión negocial**: cómo se contrata el servicio, qué se entrega, cuánto cuesta, cuánto dura, cómo se suspende y cómo se termina.
- **Dimensión jurídica**: propiedad intelectual, confidencialidad, responsabilidad, garantías y solución de controversias.
- **Dimensión de cumplimiento y seguridad**: protección de datos personales, retención cero, no entrenamiento de modelos, gestión de la seguridad de la información y atención de incidentes.

El documento describe la arquitectura del ecosistema Janalytics Agentic OS solo en los aspectos que tienen consecuencia jurídica o de seguridad. Los detalles puramente técnicos de infraestructura no forman parte de este instrumento y se entregan por separado al cliente que los requiera.

1.3 Estructura del documento

El documento se organiza en cinco partes. Las Partes I y II enmarcan el instrumento y profundizan en los cuatro pilares de cumplimiento que Janalytics adopta. La Parte III presenta el panorama regulatorio aplicable en Colombia a la creación y operación de agentes de inteligencia artificial, incluido el derecho vigente, el derecho en trámite y el marco internacional de referencia. La Parte IV desarrolla los términos y condiciones del servicio y la Parte V la política de seguridad de la información. El documento cierra con anexos operativos: la política de tratamiento de datos personales lista para publicación, el aviso de privacidad, las cláusulas del contrato de transmisión de datos, la correspondencia con los controles de ISO/IEC 27001 y el listado de referencias normativas y bibliográficas.

1.4 Metodología y fuentes

El contenido jurídico se construyó a partir de fuentes normativas primarias y secundarias verificables: textos consolidados de las leyes y decretos en portales oficiales, circulares de la Superintendencia de Industria y Comercio, documentos de política pública del Departamento Nacional de Planeación, normas internacionales ISO y materiales de referencia de proveedores de modelos de lenguaje. Cada afirmación normativa se apoya en una fuente citada al final del documento, en estilo APA de séptima edición. Cuando una cifra o una condición depende de un umbral legal, se explicita el umbral y se identifica la norma que lo fija.

Las afirmaciones sobre el estado de cumplimiento de Janalytics no son declaraciones de certificación. Janalytics describe en este documento su diseño de controles, su ruta de implementación y los compromisos que asume contractualmente; la certificación, cuando exista, se acredita con el certificado emitido por el organismo competente y se anexa al contrato. Las referencias a proyectos de ley se indican expresamente como derecho en trámite y no como derecho vigente.

2. Resumen ejecutivo

2.1 Qué ofrece Janalytics

Janalytics es un emprendimiento colombiano que presta servicios de analítica de datos y de automatización mediante agentes de inteligencia artificial. Su línea principal, el Janalytics Agentic OS, entrega a cada empresa cliente un agente autónomo preconfigurado que ejecuta tareas repetitivas concretas: procesamiento de nómina, respuesta asistida de tickets, auditoría de datos, procesamiento de facturas y monitoreo de información, entre otras. El agente opera dentro de un entorno aislado por cliente, con memoria y almacenamiento separados, y su uso se gobierna desde un panel central administrado por Janalytics.

La promesa comercial es simple y verificable: el agente hace el trabajo repetitivo y el resultado se entrega al cliente en un formato utilizable, con trazabilidad de lo ejecutado. Janalytics no vende un modelo de inteligencia artificial propio; vende un servicio operado, en el que el modelo es un componente y la responsabilidad de Janalytics es la de un prestador de servicios que organiza, configura, supervisa y responde por el resultado del proceso.

2.2 Los cuatro pilares de cumplimiento

Janalytics estructura su compromiso de confianza sobre cuatro pilares que el cliente puede exigir contractualmente. Los tres primeros son de datos y de seguridad; el cuarto es de derecho aplicable.

1. **Retención cero de datos (Zero Data Retention)**: los datos del cliente que pasan por el modelo no se conservan por parte de Janalytics ni por parte de los proveedores de modelos, salvo el mínimo estrictamente necesario para operar y auditar el servicio. Se profundiza en la sección 4.
2. **Datos sin entrenamiento de modelo**: la información del cliente no se utiliza para entrenar, afinar ni mejorar modelos de inteligencia artificial, propios ni de terceros. Se profundiza en la sección 5.
3. **Cumplimiento de la Ley 1581 de 2012**: tratamiento de datos personales conforme al régimen colombiano de protección de datos, con sus principios, derechos y obligaciones. Se profundiza en la sección 6.

4. **Seguridad de la información alineada con ISO/IEC 27001**: sistema de gestión de seguridad de la información y controles técnicos y organizativos, complementado con ISO/IEC 42001 para la gestión de la inteligencia artificial. Se profundiza en la sección 7.

2.3 Estado de cumplimiento y compromisos

Es importante distinguir entre lo que Janalytics ya tiene implementado, lo que está en ruta de implementación y lo que depende de terceros. La tabla siguiente resume el estado declarado a la fecha de esta versión. Janalytics se obliga a mantener esta declaración actualizada en cada revisión del documento.

Pilar	Estado al emitir este documento	Compromiso contractual
Retención cero (ZDR)	Diseño operativo definido; política de no persistencia aplicada a la capa del agente; pendiente de acuerdo formal con cada proveedor de modelo.	Janalytics no conservará datos del cliente más allá de lo necesario para operar, y exigirá a sus proveedores condiciones equivalentes.
No entrenamiento de modelos	Compromiso asumido; se seleccionan proveedores con política de no entrenamiento sobre datos de API.	La información del cliente nunca se usará para entrenar o mejorar modelos.
Ley 1581 de 2012	Políticas de tratamiento redactadas (Anexo A); contrato de transmisión disponible (Anexo C); responsables designados.	Cumplimiento permanente del régimen de protección de datos personales.
ISO/IEC 27001	Controles técnicos y organizativos implementados sobre la base del aislamiento por contenedor; SGSI documentado en construcción.	Implementar y mantener un SGSI alineado con ISO/IEC 27001 y avanzar hacia la certificación.
ISO/IEC 42001	Adopción como marco de referencia para gobierno de IA; certificación no iniciada.	Gestionar los sistemas de IA bajo prácticas de gobierno, transparencia y gestión de riesgos alineadas con ISO/IEC 42001.

2.4 Qué puede exigir el cliente

Con base en lo anterior, todo cliente de Janalytics puede exigir: (i) que sus datos no se retengan más allá de lo necesario y no se usen para entrenar modelos; (ii) que el tratamiento de datos personales se realice conforme a la Ley 1581 de 2012 y a las instrucciones que el cliente, como responsable, imparta a Janalytics como encargado; (iii) información razonable y verificable sobre las medidas de seguridad aplicadas; (iv) notificación de incidentes de seguridad que afecten sus datos; y (v) la posibilidad de auditar o solicitar evidencia del cumplimiento, en los términos de la sección 43.

Estos derechos no son una concesión graciable: se incorporan al contrato y se detallan en los términos y condiciones de la Parte IV y en la política de seguridad de la Parte V.

3. Glosario

Las definiciones siguientes rigen para la interpretación de todo el documento. Cuando una definición proviene de una norma colombiana, se indica la fuente. Los términos técnicos de seguridad e inteligencia artificial se definen según el uso internacional y se marcan como tales.

3.1 Términos legales

Titular	Persona natural cuyos datos personales son objeto de tratamiento (Ley 1581 de 2012, art. 3).
Dato personal	Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (Ley 1581 de 2012, art. 3).
Dato sensible	Dato que afecta la intimidad del titular o cuyo uso indebido puede generar discriminación; incluye salud, vida sexual, datos biométricos, origen racial o étnico, convicciones y orientación política (Decreto 1377 de 2013, art. 3).
Responsable del tratamiento	Persona natural o jurídica que decide sobre la base de datos y el tratamiento. En la relación con Janalytics, el cliente es normalmente el responsable.
Encargado del tratamiento	Persona que realiza el tratamiento por cuenta del responsable. Janalytics actúa como encargado respecto de los datos que le entrega el cliente.
Autorización	Consentimiento previo, expreso e informado del titular para el tratamiento de sus datos, o conducta inequívoca que permita concluirlo. El silencio nunca se asimila a autorización (Decreto 1377 de 2013, art. 7).
Transferencia internacional	Envío de datos por el responsable o encargado ubicado en Colombia a un receptor que es responsable y se encuentra dentro o fuera del país (Decreto 1377 de 2013, art. 3).
Transmisión internacional	Comunicación de datos dentro o fuera del país para que un encargado realice el tratamiento por cuenta del responsable (Decreto 1377 de 2013, art. 3).
Accountability	Deber de responsabilidad demostrada: el responsable debe poder probar que implementó medidas apropiadas y efectivas de cumplimiento (Decreto 1377 de 2013, art. 26).
RNBD	Registro Nacional de Bases de Datos, directorio público administrado por la Superintendencia de Industria y Comercio (SIC).
SIC	Superintendencia de Industria y Comercio, autoridad nacional de protección de datos personales y de protección al consumidor en Colombia.

3.2 Términos de inteligencia artificial y datos

Agente de IA	Software que, mediante un modelo de lenguaje y herramientas, planifica y ejecuta tareas con cierto grado de autonomía para alcanzar un objetivo definido.
Agente asistencial	Agente de IA configurado para ejecutar tareas repetitivas bajo supervisión humana, sin adoptar decisiones que afecten derechos del titular sin intervención de una persona.
Retención cero (Zero Data Retention, ZDR)	Práctica por la cual el proveedor de un modelo no conserva las entradas ni las salidas de una solicitud después de procesarla.
No entrenamiento (no-training)	Compromiso de no utilizar los datos de un cliente para entrenar, afinar o mejorar modelos. Es una condición distinta e independiente de la retención cero.
Modelo de lenguaje (LLM)	Modelo estadístico entrenado sobre grandes volúmenes de texto, capaz de generar y transformar lenguaje.

Subencargado	Tercero contratado por el encargado para realizar parte del tratamiento. Janalytics responde por sus subencargados.
DPA (Acuerdo de Tratamiento de Datos)	Contrato entre responsable y encargado que fija el alcance del tratamiento, las obligaciones del encargado y las garantías de seguridad. En Colombia corresponde al contrato de transmisión del artículo 25 del Decreto 1377 de 2013.
Prompt	Instrucción o entrada de texto que se envía al modelo de lenguaje.
Log	Registro de eventos de un sistema, con marca de tiempo, utilidad para auditoría y detección de incidentes.
Incidente de seguridad	Evento que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de la información.
SGSI	Sistema de Gestión de Seguridad de la Información; conjunto de políticas, procesos y controles para proteger la información (ISO/IEC 27001).
SGIA	Sistema de Gestión de Inteligencia Artificial; marco para gobernar el desarrollo y uso responsable de IA (ISO/IEC 42001).
MTTR	Tiempo medio de reparación o restauración tras un incidente.

3.3 Términos contractuales

Cliente	Persona natural o jurídica que contrata los servicios de Janalytics y que, en la relación de datos, actúa normalmente como responsable del tratamiento.
Usuario autorizado	Persona designada por el cliente para acceder al servicio, mediante credenciales o mediante un pase de acceso emitido por Janalytics.
Servicio	Conjunto de tareas de automatización ejecutadas por los agentes de Janalytics, más el acceso al panel de gobierno y a la aplicación del cliente.
Entregable	Resultado concreto producido por el agente (por ejemplo, un archivo procesado, un reporte o un borrador de respuesta).
SLA	Acuerdo de nivel de servicio; compromiso de disponibilidad y de tiempos de respuesta y resolución.
Pase de acceso	Mecanismo de acceso de un solo uso, emitido desde el panel, que habilita a un usuario autorizado a entrar a la aplicación de su empresa sin credenciales propias.

4. Primer pilar: retención cero de datos (Zero Data Retention)

4.1 Qué significa exactamente retención cero

La retención cero de datos, conocida en la industria como Zero Data Retention o ZDR, es el compromiso por el cual quien procesa una solicitud de inteligencia artificial no conserva las entradas ni las salidas de esa solicitud una vez terminado el procesamiento. En términos prácticos: el texto que el agente envía al modelo, la respuesta que el modelo devuelve y los archivos intermedios que se derivan de esa operación no quedan almacenados en los sistemas de Janalytics ni en los de sus proveedores de modelos con posterioridad a su uso.

Es fundamental entender que la retención cero no es lo mismo que la ausencia de registros operativos. Janalytics conserva registros mínimos de operación, necesarios para prestar el servicio, facturar y auditar la seguridad, pero esos registros no contienen el contenido de los datos del cliente. La sección 4.4 detalla esta distinción, que es una de las más malinterpretadas en los servicios de IA.

4.2 Por qué importa

Cuando una empresa entrega su nómina, sus facturas o sus bases de datos a un proveedor de inteligencia artificial, existe un riesgo legítimo: que esa información quede almacenada indefinidamente, que se mezcle con datos de otros clientes o que se use para fines distintos de los contratados. La retención cero reduce ese riesgo a su mínima expresión porque limita la ventana en que el dato existe. Menos tiempo de conservación significa menos superficie de exposición, menos obligaciones de custodia y menos consecuencias en caso de brecha.

Desde la perspectiva del régimen colombiano, la retención cero es coherente con dos principios de la Ley 1581 de 2012: el principio de finalidad, que exige que el tratamiento sirva a un propósito determinado e informado, y el principio de temporalidad o necesidad, que prohíbe conservar datos más allá de lo razonable y necesario. El artículo 11 del Decreto 1377 de 2013 desarrolla esta idea: los responsables y encargados solo pueden recolectar, almacenar, usar o circular datos durante el tiempo razonable y necesario, y deben suprimirlos una vez cumplida la finalidad, salvo que una norma legal o un vínculo contractual exija conservarlos.

4.3 Cómo lo implementa Janalytics

Janalytics diseña la operación de sus agentes bajo un principio de no persistencia del contenido. El diseño se apoya en cuatro decisiones concretas que se describen a continuación y que el cliente puede verificar en los términos de la sección 43.

1. **Procesamiento en el entorno del cliente.** Cada cliente opera en un entorno aislado con su propia memoria y su propio almacenamiento. Los datos no se concentran en un repositorio común de Janalytics.
2. **Selección de proveedores con ZDR.** Los proveedores de modelos que Janalytics utiliza deben ofrecer retención cero o la retención mínima técnicamente posible para sus servicios de API. Cuando un proveedor no ofrece ZDR, Janalytics no lo utiliza para datos de clientes.
3. **Ausencia de uso del contenido para fines secundarios.** El contenido procesado no se copia a entornos de analítica, no se agrega a paneles de negocio y no se reutiliza para otros clientes.
4. **Eliminación programada.** Los archivos temporales que un agente necesita para producir un entregable se eliminan en los plazos definidos en la política de retención del Anexo A, salvo que el cliente instruya conservarlos en su propio entorno.

4.4 Lo que Janalytics sí conserva

La retención cero del contenido convive con una retención operativa mínima, indispensable para que el servicio funcione y sea auditable. Janalytics conserva:

- **Metadatos de operación**: fecha y hora de ejecución, identificador de la tarea, estado del resultado (éxito o error) y duración. No incluyen el contenido de los datos.
- **Registros de seguridad**: eventos de acceso, inicios de sesión y cambios de configuración, con una retención alineada con la política de la sección 41.

- **Entregables en el entorno del cliente**: los archivos que el agente produce y que el cliente decide conservar en su propio espacio. Su custodia final corresponde al cliente.
- **Documentación contractual y contable**: contratos, facturas y soportes, conservados por los plazos legales aplicables.

La regla es sencilla: Janalytics conserva la prueba de que el trabajo se hizo y de que el sistema es seguro, pero no el contenido del trabajo del cliente. Cuando una obligación legal exige conservar un dato, Janalytics lo informa al cliente y limita la conservación a lo estrictamente exigido, con controles de acceso reforzados.

4.5 Límites honestos de la retención cero

Janalytics no oculta las limitaciones de este compromiso. La retención cero no es absoluta y no puede presentarse como tal. Existen tres límites reales:

1. Los proveedores de modelos pueden conservar datos por periodos cortos cuando existe una obligación legal de monitoreo de abuso o un requisito judicial. Janalytics informa al cliente qué proveedores ofrecen ZDR pleno y cuáles aplican retención mínima.
2. Los sistemas operativos y las copias de seguridad pueden contener datos residuales durante el ciclo de rotación de la copia. Janalytics define ventanas de rotación y comunica su duración.
3. Los registros de terceros ajenos al servicio, como el proveedor de correo del cliente o sus propios repositorios, escapan al control de Janalytics y siguen sus propias políticas.

Estos límites no debilitan el compromiso: lo hacen verificable. Un proveedor que declara retención cero sin matices probablemente no comprende su propia cadena de tratamiento.

5. Segundo pilar: datos sin entrenamiento de modelos

5.1 La distinción que casi nadie hace

Retención cero y no entrenamiento son dos compromisos distintos, y confundirlos es el error más frecuente en la contratación de servicios de inteligencia artificial. La retención cero se refiere a cuánto tiempo se conserva el dato. El no entrenamiento se refiere a para qué se usa el dato mientras existe. Un proveedor puede cumplir con retención cero y, aun así, no ofrecer garantías sobre el uso del dato antes de descartarlo; otro puede no entrenar con el dato y conservarlo por razones de seguridad durante un plazo. Ambas condiciones deben exigirse por separado.

La industria ha adoptado el no entrenamiento como estándar para los servicios empresariales de API. Proveedores como OpenAI y Anthropic declaran que los datos enviados a través de sus interfaces empresariales no se utilizan para entrenar modelos, y ofrecen además la opción de retención cero para clientes que califican. Janalytics exige ambas condiciones y no construye servicios de cliente sobre proveedores que entrenen con datos de API.

5.2 Qué compromete Janalytics

Janalytics asume frente al cliente un compromiso de no entrenamiento que cubre los datos del cliente en todas sus formas: los archivos que el cliente carga, el texto de las instrucciones que se envían al modelo, las respuestas que el modelo produce y cualquier dato derivado. El compromiso se concreta en las siguientes obligaciones:

- No usar los datos del cliente para entrenar, afinar (fine-tuning), calibrar o mejorar modelos de inteligencia artificial, propios ni de terceros.
- No usar los datos del cliente para evaluar modelos con fines de mejora del proveedor.
- No construir conjuntos de datos agregados o sintéticos a partir de información de clientes que permitan derivar información de un cliente concreto.
- Exigir contractualmente a los proveedores de modelos condiciones equivalentes de no entrenamiento y documentar esa exigencia.
- Informar al cliente, de forma previa y expresa, si en el futuro se pretendiera usar sus datos para un fin distinto, y obtener su autorización específica antes de hacerlo.

5.3 Coherencia con el régimen de datos personales

El compromiso de no entrenamiento no es solo una buena práctica comercial: tiene consecuencias jurídicas bajo la Ley 1581 de 2012. Utilizar datos personales para entrenar un modelo es un tratamiento con una finalidad distinta de la contratada, y el régimen colombiano exige que toda finalidad nueva cuente con autorización previa, expresa e informada del titular. Además, la SIC ha señalado, en su Circular Externa 002 de 2024 sobre tratamiento de datos personales en sistemas de inteligencia artificial, que el tratamiento debe observar los principios de idoneidad, necesidad y proporcionalidad, y que los datos usados en IA deben ser veraces, completos, exactos y actualizados. Entrenar un modelo con los datos de un cliente sin base jurídica suficiente expondría al responsable y al encargado a sanciones.

Por lo anterior, Janalytics adopta el no entrenamiento como regla general y no como excepción configurable. Aun si un cliente lo autorizara, Janalytics mantiene la restricción como política interna, porque el riesgo de reidentificación y de uso indebido en un modelo entrenado es difícil de controlar y de revertir.

5.4 Verificación

El cliente puede verificar este compromiso por tres vías: solicitando la declaración de proveedores utilizados y sus políticas de datos; exigiendo la cláusula de no entrenamiento en el contrato de transmisión de datos (Anexo C); y solicitando, cuando exista, la documentación del proveedor que acredite la condición ZDR y la prohibición de entrenamiento sobre los datos de su interfaz empresarial.

6. Tercer pilar: cumplimiento de la Ley 1581 de 2012

6.1 El régimen general de protección de datos personales

La Ley 1581 de 2012, de naturaleza estatutaria, desarrolla el derecho constitucional al habeas data consagrado en el artículo 15 de la Constitución Política de Colombia. Su objeto es permitir que las personas conozcan, actualicen y rectifiquen la información recogida sobre ellas en bases de datos, y proteger sus demás derechos y garantías. La ley fija el ámbito de aplicación, los principios rectores, las categorías especiales de datos, los derechos de los titulares, los deberes de los responsables y encargados y el régimen de transferencia internacional. La Superintendencia de Industria y Comercio es la autoridad que vigila y sanciona su cumplimiento.

Dos normas reglamentan y complementan la ley. El Decreto 1377 de 2013 reglamenta parcialmente la Ley 1581 y detalla la autorización, las políticas de tratamiento, el ejercicio de los derechos, las

transferencias y transmisiones internacionales y el deber de responsabilidad demostrada. El Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, compila esa reglamentación y fija, entre otros aspectos, los plazos y umbrales asociados al Registro Nacional de Bases de Datos. En materia de datos financieros y crediticios rige además la Ley 1266 de 2008, que no resulta central para el objeto de Janalytics pero puede activarse cuando el servicio procesa información de este tipo.

6.2 Principios rectores

El artículo 4 de la Ley 1581 de 2012 consagra los principios que orientan el tratamiento de datos personales. Janalytics los incorpora como reglas operativas, porque son la base sobre la que la SIC evalúa el cumplimiento.

Principio	Qué exige	Cómo lo aplica Janalytics
Legalidad	El tratamiento debe sujetarse a la ley.	Tratamiento conforme a la Ley 1581 y su reglamentación.
Finalidad	El tratamiento debe servir a un fin determinado e informado.	Cada tarea del agente responde a una finalidad definida en el contrato y en la autorización.
Libertad	El tratamiento requiere consentimiento previo, expreso e informado, salvo excepción legal.	No se inicia tratamiento sin base jurídica; no se asimila el silencio a autorización.
Veracidad o calidad	El dato debe ser veraz, completo, exacto, actualizado y comprobable.	Los procesos de auditoría y validación buscan detectar datos incompletos o erróneos.
Transparencia	El titular debe poder conocer la existencia del tratamiento.	Política de tratamiento publicada y disponible.
Acceso y circulación restringida	El dato solo circula entre quienes deben intervenir.	Aislamiento por cliente y control de acceso por roles y pases.
Seguridad	Se deben adoptar medidas técnicas y humanas de protección.	Controles alineados con ISO/IEC 27001 (sección 7 y Parte V).
Confidencialidad	Quienes intervienen deben guardar reserva.	Cláusulas de confidencialidad y obligaciones para el personal y los terceros.
Temporalidad o necesidad	No conservar más allá de lo necesario.	Diseño de retención cero del contenido (sección 4).

6.3 Derechos de los titulares

La ley reconoce a los titulares cuatro derechos relevantes: conocer, actualizar, rectificar y suprimir sus datos, y revocar la autorización cuando sea procedente. El Decreto 1377 de 2013 y la propia ley fijan los procedimientos y, en particular, el artículo 21 del decreto regula el derecho de acceso con reglas de periodicidad gratuita. Janalytics, en su rol de encargado, no atiende directamente a los titulares cuando el cliente es el responsable: su obligación es apoyar al cliente para que atienda esas solicitudes dentro de los plazos legales. Para ello, Janalytics se compromete a:

- Habilitar un canal de comunicación con el cliente para recibir y tramitar solicitudes relacionadas con datos tratados por su cuenta.
- Responder al cliente en plazos que le permitan cumplir los términos legales de consulta y reclamo.

- Implementar, cuando el cliente lo instruya, la supresión o actualización de datos en los sistemas de Janalytics.
- Documentar la trazabilidad de cada solicitud y su respuesta.

6.4 Roles: responsable y encargado

Uno de los requisitos más importantes del régimen es definir con claridad quién decide y quién ejecuta. En la relación con Janalytics, la regla general es que el cliente es el responsable del tratamiento y Janalytics es el encargado. El cliente decide sobre la base de datos, sobre las finalidades y sobre las instrucciones; Janalytics ejecuta esas instrucciones y responde por la seguridad de lo que le fue confiado.

De esa distribución se derivan obligaciones concretas. Como encargado, Janalytics debe: tratar los datos conforme a los principios que rigen la materia; salvaguardar la seguridad de las bases de datos; guardar confidencialidad; no usar los datos para una finalidad distinta de la autorizada; y dar traslado de las consultas del titular al responsable. Estas obligaciones las exige el artículo 25 del Decreto 1377 de 2013 en el contrato de transmisión, y se recogen textualmente en el Anexo C de este documento.

6.5 Autorización y aviso de privacidad

La autorización es la base jurídica más común del tratamiento y debe obtenerse a más tardar en el momento de la recolección de los datos. El Decreto 1377 de 2013, en su artículo 7, admite que se manifieste por escrito, de forma oral o mediante conductas inequívocas del titular, y exige que los mecanismos permitan su consulta posterior. Janalytics exige a sus clientes que acrediten la existencia de la autorización de los titulares cuyos datos se procesarán y se reserve la prueba correspondiente, conforme al artículo 8 del mismo decreto.

Cuando no sea posible poner a disposición del titular la política de tratamiento, procede el aviso de privacidad, con el contenido mínimo del artículo 15 del decreto: identificación y datos de contacto del responsable, finalidades del tratamiento, derechos del titular y mecanismos para conocer la política. El Anexo B de este documento ofrece un modelo de aviso de privacidad adaptado al servicio.

El tratamiento de datos sensibles merece regla especial. La ley prohíbe tratarlos salvo en los casos expresamente previstos, y el decreto exige informar al titular que no está obligado a autorizar su tratamiento, informar de forma explícita cuáles datos son sensibles y obtener consentimiento expreso. Janalytics solicita al cliente declaración expresa sobre si el servicio tratará datos sensibles y, cuando sea el caso, refuerza los controles y la base jurídica.

6.6 Políticas de tratamiento y su publicación

El artículo 13 del Decreto 1377 de 2013 enumera el contenido mínimo de las políticas de tratamiento: identificación del responsable con domicilio y contacto; tratamiento y finalidad; derechos del titular; persona o área responsable de atender peticiones, consultas y reclamos; procedimiento para ejercer los derechos; y fecha de vigencia de la política y periodo de vigencia de la base de datos. La política debe constar en medio físico o electrónico, en lenguaje claro y sencillo, y estar a disposición de los titulares. El Anexo A de este documento contiene la política de tratamiento de datos personales de Janalytics, redactada para cumplir estos requisitos.

Cualquier cambio sustancial en la política —por ejemplo, en la identificación del responsable o en la finalidad del tratamiento— debe comunicarse al titular de forma oportuna y antes de implementar la

nueva política, y puede exigir una nueva autorización cuando se modifique la finalidad. Janalytics deja constancia de este deber en su procedimiento interno de cambios.

6.7 Registro Nacional de Bases de Datos

El Registro Nacional de Bases de Datos es un directorio público administrado por la SIC. La obligación de inscribirse recae, según la SIC, en las sociedades y entidades sin ánimo de lucro con activos totales superiores a 100.000 unidades de valor tributario (UVT) y en las personas jurídicas de naturaleza pública. Janalytics, como emprendimiento en etapa temprana, debe verificar su situación patrimonial frente a ese umbral; si lo supera, debe inscribir las bases de datos que administra. En todo caso, la obligación de registrar recae sobre el responsable del tratamiento, de modo que cuando Janalytics actúe como encargado, la inscripción corresponde al cliente.

6.8 Transferencia y transmisión internacional

La ley prohíbe la transferencia de datos personales a países que no proporcionen niveles adecuados de protección. Un país ofrece nivel adecuado cuando cumple los estándares fijados por la SIC, que no pueden ser inferiores a los que la ley exige en Colombia. La SIC desarrolló esos estándares en su Circular Externa 005 de 2017, que adicionó un capítulo a la Circular Única. La Corte Constitucional, en la sentencia C-748 de 2011, precisó que un país cuenta con nivel adecuado cuando su legislación contiene principios que abarcan obligaciones y derechos de las partes, y un procedimiento de protección que involucra autoridades que efectivizan esa protección.

Cuando el país receptor no cumple esos estándares, el responsable puede: (i) verificar si la operación está cubierta por una causal de excepción del artículo 26 de la Ley 1581; (ii) acreditar que el país cumple los estándares del numeral 3.1 de la circular; o (iii) solicitar una declaración de conformidad ante la Delegatura para la Protección de Datos Personales de la SIC. La SIC precisó este régimen en su Circular Externa 002 de 2025.

La distinción entre transferencia y transmisión es decisiva para Janalytics. Cuando Janalytics, como encargado, comunica datos del cliente a un proveedor de modelos en el exterior para que este realice el tratamiento por cuenta del cliente, existe típicamente una transmisión internacional. El artículo 24 del Decreto 1377 de 2013 señala que las transmisiones internacionales entre responsable y encargado no requieren ser informadas al titular ni contar con su consentimiento cuando existe un contrato en los términos del artículo 25. Por eso, el contrato de transmisión del Anexo C no es un formalismo: es el instrumento que da base jurídica a la operación transfronteriza del servicio.

6.9 Seguridad y responsabilidad demostrada

El artículo 19 del Decreto 1377 remite a la SIC para impartir instrucciones sobre medidas de seguridad, y el capítulo VI del decreto consagra el deber de responsabilidad demostrada. Janalytics debe poder demostrar, a petición de la SIC, que ha implementado medidas apropiadas y efectivas para cumplir sus obligaciones, en proporción a la naturaleza del responsable, la naturaleza de los datos, el tipo de tratamiento y los riesgos potenciales. El artículo 26 del decreto exige además que Janalytics pueda describir sus procedimientos de recolección, sus finalidades y la relevancia de los datos en cada caso, y suministrar evidencia sobre las medidas de seguridad implementadas. La política de seguridad de la Parte V y los registros de la sección 41 son la respuesta operativa a ese deber.

6.10 Régimen sancionatorio

El incumplimiento del régimen de protección de datos expone a sanciones que la SIC puede imponer, incluida la suspensión del tratamiento de datos y sanciones pecuniarias. Además, la Ley 1273 de 2009 tipificó como delito la violación de datos personales y el acceso abusivo a sistemas informáticos, entre otras conductas. Janalytics reconoce que la protección de datos no es solo una obligación administrativa: es un deber penal y reputacional, y diseña sus controles en consecuencia.

7. Cuarto pilar: ISO/IEC 27001 e ISO/IEC 42001

7.1 Qué exige ISO/IEC 27001

ISO/IEC 27001 es el estándar internacional que especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI). Su versión vigente es la de 2022, que reorganizó los controles del Anexo A en cuatro categorías: controles organizacionales (5.1 a 5.37), controles de personas (6.1 a 6.8), controles físicos (7.1 a 7.14) y controles tecnológicos (8.1 a 8.34), para un total de 93 controles.

La norma no consiste en una lista de productos de seguridad, sino en un ciclo de gestión: comprender el contexto y el alcance del SGSI; definir la política y las responsabilidades; evaluar y tratar los riesgos; implementar controles; medir, auditar internamente y revisar por la dirección; y mejorar de forma continua. Los controles del Anexo A se seleccionan según el análisis de riesgos, no se aplican todos por igual.

7.2 Cómo se alinea Janalytics

Janalytics adopta ISO/IEC 27001 como marco de referencia para su gestión de seguridad. No declara una certificación que aún no posee; declara un diseño y una ruta. La tabla siguiente resume la correspondencia entre los dominios del Anexo A y las medidas de Janalytics, con remisión a la Parte V, donde se detallan.

Categoría de control (Anexo A)	Aplicación en Janalytics	Sección
Organizacionales (5.x)	Políticas, roles, gestión de activos, control de proveedores, gestión de incidentes, continuidad y cumplimiento.	33, 34, 38, 39, 40, 42
De personas (6.x)	Selección, acuerdos de confidencialidad, formación y cultura de seguridad, trabajo remoto seguro.	44
Físicos (7.x)	Controles del proveedor de infraestructura (centros de datos), protección de equipos y escritorios.	34, 40
Tecnológicos (8.x)	Autenticación, control de acceso, cifrado, registros, respaldo, protección contra malware, gestión de vulnerabilidades.	35, 36, 37, 41

La ruta de certificación es progresiva. En la etapa actual, Janalytics documenta su SGSI, mantiene un registro de activos y riesgos, e implementa los controles técnicos prioritarios: aislamiento por cliente, autenticación robusta, cifrado en tránsito y en reposo, y registros de auditoría. La certificación formal exige una auditoría externa y se abordará cuando el volumen de clientes y la estructura societaria lo justifiquen. Janalytics se obliga a informar al cliente el estado real de este proceso y a no presentar como certificado lo que solo está diseñado.

7.3 Por qué ISO/IEC 42001 y no solo ISO/IEC 27001

ISO/IEC 27001 protege la información, pero no gobierna las particularidades de la inteligencia artificial: el sesgo, la trazabilidad de las decisiones, la explicabilidad o la gestión del ciclo de vida de un modelo. Para cubrir ese vacío, la Organización Internacional de Normalización publicó en 2023 la norma ISO/IEC 42001, que especifica los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de inteligencia artificial (SGIA).

ISO/IEC 42001 aporta un marco certificable que las organizaciones usan para desarrollar e implementar sistemas de IA de forma responsable, con énfasis en transparencia, gestión de riesgos y bienestar humano. Janalytics adopta ISO/IEC 42001 como referencia de gobierno de IA y articula ambos sistemas: ISO/IEC 27001 protege los datos y la infraestructura; ISO/IEC 42001 gobierna el comportamiento y el riesgo del agente.

7.4 Aplicación conjunta en el Agentic OS

La combinación de ambos marcos se traduce, en la operación de Janalytics, en un conjunto de decisiones concretas que se describen en la Parte V. En síntesis: el agente opera con alcance limitado a la tarea contratada; toda acción relevante queda registrada; las decisiones que afectan derechos o intereses del titular exigen supervisión humana; la calidad de las salidas se verifica por muestreo; y los riesgos del sistema se evalúan y se revisan periódicamente. Este diseño responde a la vez a ISO/IEC 27001, a ISO/IEC 42001 y a la Circular Externa 002 de 2024 de la SIC.

7.5 Declaración de estado

Janalytics declara expresamente que, a la fecha de esta versión: no cuenta con certificación ISO/IEC 27001 ni ISO/IEC 42001; utiliza ambos estándares como marco de diseño y de gestión; mantiene los controles descritos en la Parte V; y se compromete a informar al cliente cualquier cambio en ese estado. Esta declaración honesta es parte de la política de transparencia de la empresa y evita expectativas contractuales que no correspondan a la realidad.

8. Marco normativo colombiano aplicable a los servicios de Janalytics

8.1 Criterio de identificación de normas

No existe en Colombia, a la fecha de esta versión, una ley integral y vigente que regule específicamente la inteligencia artificial. Eso no significa que los agentes de IA operen en un vacío jurídico: significa que el servicio se rige por el derecho existente, aplicado analógicamente a la nueva tecnología. La SIC lo ha dicho con claridad: la normatividad sobre tratamiento de datos personales debe aplicarse al margen de los procedimientos, metodologías o tecnologías que se utilicen.

Para identificar el marco aplicable se partió de tres preguntas: (i) qué normas regulan la información que el servicio trata; (ii) qué normas regulan la relación comercial con el cliente; y (iii) qué normas regulan el comportamiento del sistema y su responsabilidad. La tabla siguiente ordena el resultado por materia.

Materia	Norma principal	Relevancia para Janalytics
Protección de datos personales	Ley 1581 de 2012; Decreto 1377 de 2013; Decreto 1074 de 2015	Núcleo del cumplimiento: régimen, autorización, políticas, transferencias y accountability.

Materia	Norma principal	Relevancia para Janalytics
Habeas data financiero	Ley 1266 de 2008	Aplicable cuando el servicio trata información crediticia o financiera.
Protección de datos en IA	Circular Externa 002 de 2024 de la SIC	Lineamientos específicos sobre tratamiento de datos en sistemas de IA.
Responsabilidad de administradores	Circular Externa 003 de 2024 de la SIC	Deberes de los administradores societarios frente a la protección de datos.
Delitos informáticos	Ley 1273 de 2009	Tipifica acceso abusivo, interceptación y violación de datos personales.
Comercio electrónico y firma	Ley 527 de 1999	Validez de mensajes de datos, contratos electrónicos y firma electrónica.
Protección al consumidor	Ley 1480 de 2011	Requisitos de contratos de adhesión, comercio electrónico, información y garantías.
TIC y conectividad	Ley 2108 de 2021	Reconoce el internet como servicio público esencial; incide en la continuidad del servicio.
Propiedad intelectual	Ley 23 de 1982; Decisión Andina 351 de 1993	Titularidad de obras, software y contenidos; tratamiento de obras generadas con IA.
Derecho constitucional	Constitución Política, arts. 15 y 20	Fundamento del habeas data y de la libertad de información.

8.2 Protección de datos personales

Es el eje del cumplimiento de Janalytics y se desarrolla in extenso en la sección 6. Conviene subrayar tres consecuencias para la creación de agentes. Primera: el agente no es un sujeto de derechos, de modo que las obligaciones siempre recaen en personas (el cliente como responsable y Janalytics como encargado). Segunda: cada tarea del agente debe tener una finalidad definida y una base jurídica, porque el agente ejecuta tratamiento de datos sin que ello cambie la exigencia legal. Tercera: la autorización de los titulares debe preexistir al tratamiento, y su prueba debe conservarse.

8.3 Circular Externa 002 de 2024 de la SIC

Esta circular, expedida en agosto de 2024, ofrece lineamientos específicos sobre el tratamiento de datos personales en sistemas de inteligencia artificial. Es, en la práctica, la norma más directamente aplicable al negocio de Janalytics y conviene detallarla. La SIC parte de una constatación: la inteligencia artificial requiere grandes volúmenes de datos, con frecuencia personales, y se usa para tomar decisiones autónomas o para asistir a un tomador de decisiones humano mediante recomendaciones y predicciones.

La circular fija un test de ponderación de cuatro criterios para el tratamiento de datos en IA: idoneidad (el tratamiento debe ser capaz de alcanzar el objetivo); necesidad (no debe existir una medida menos invasiva e igualmente eficaz); proporcionalidad; y, en general, salvaguarda de los principios de las leyes estatutarias de protección de datos. De este test se derivan varias exigencias operativas que Janalytics incorpora:

- Los administradores de datos deben adecuar sistemas de administración de riesgos asociados al tratamiento, con descripción detallada de las operaciones y de las medidas previstas para evitar la materialización de riesgos.
- Los datos personales tratados en sistemas de IA deben ser veraces, completos, exactos, actualizados, comprobables y comprensibles; se prohíbe tratar datos parciales, incompletos, fraccionados o que induzcan a error.
- Debe garantizarse el derecho del titular a obtener, en cualquier momento y sin restricciones, información sobre el tratamiento de sus datos.
- Debe aplicarse la privacidad desde el diseño, de modo que al hacer analítica de datos para alimentar sistemas de IA se apliquen técnicas que impidan identificar a la persona que proporciona la información, cuando ello sea posible.
- Se prohíbe apropiarse de datos privados, semiprivados o sensibles recolectados en internet y tratarlos para finalidades distintas sin autorización previa, expresa e informada del titular.
- Los riesgos deben estar sujetos a planificación y mitigación proporcionales a la gravedad del eventual daño, considerando sesgos humanos, fallas técnicas, vulnerabilidades de seguridad y fallas de implementación.

Janalytics adopta estos lineamientos como criterios de diseño. En particular, la empresa no realiza decisiones plenamente automatizadas que afecten derechos del titular: sus agentes producen resultados, borradores y alertas, y la decisión final queda en el cliente, que es quien la adopta bajo su responsabilidad.

8.4 Circular Externa 003 de 2024 de la SIC

Esta circular se dirige a los administradores societarios y les recuerda que pueden resultar responsables por el tratamiento de datos personales que realiza la sociedad. Instruye a los administradores para que establezcan lineamientos que fortalezcan continuamente las medidas de seguridad de la información y para que incorporen la protección de datos en la gobernanza de la empresa. Para un emprendimiento como Janalytics, la consecuencia práctica es que la protección de datos no es una tarea exclusiva del área tecnológica: es una responsabilidad de la administración, que debe dejar constancia de su gestión.

8.5 Delitos informáticos: Ley 1273 de 2009

La Ley 1273 de 2009 modificó el Código Penal y creó un capítulo de delitos informáticos. Entre las conductas relevantes están el acceso abusivo a un sistema informático, la obstaculización ilegítima de un sistema o red de telecomunicaciones, la interceptación de datos informáticos, el daño informático, el uso de software malicioso y, de forma central para Janalytics, la violación de datos personales del artículo 269F. Esta tipificación eleva el estándar de cuidado: una brecha de seguridad puede tener consecuencias no solo administrativas, sino penales.

Janalytics traduce esta norma en controles de acceso, cifrado, registro de actividades y verificación de proveedores, y en la obligación de reportar internamente cualquier sospecha de acceso no autorizado.

8.6 Comercio electrónico y validez del contrato digital: Ley 527 de 1999

La Ley 527 de 1999 define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y establece las entidades de certificación. Su regla central es

que no se negarán efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de estar en forma de mensaje de datos. Esta norma es la que permite que los términos y condiciones de Janalytics se acepten por medios electrónicos y que el contrato se perfeccione sin firma manuscrita.

La ley también regula la formación del contrato: salvo acuerdo expreso, la oferta y su aceptación pueden expresarse por medio de mensajes de datos, y no se niega validez a un contrato por haberse formado con mensajes de datos. Para la prueba, los mensajes de datos son admisibles como medios probatorios. Janalytics conserva evidencia de la aceptación de los términos, con marca de tiempo e identificación del aceptante, para poder acreditar el consentimiento si fuera necesario.

8.7 Protección al consumidor: Ley 1480 de 2011

El Estatuto del Consumidor es relevante porque sus normas son de orden público y se interpretan en la forma más favorable al consumidor. Cuando el cliente de Janalytics es una empresa, la relación suele ser de naturaleza mercantil y no de consumo; pero cuando el cliente es una persona natural que actúa como destinatario final, las reglas del Estatuto se activan. Janalytics asume un diseño compatible con ambos escenarios.

Tres exigencias del Estatuto condicionan la redacción de los términos. Primera: los contratos de adhesión deben usar el idioma castellano, sus condiciones deben ser concretas, claras y completas, y las cláusulas que permitan al proveedor modificar unilateralmente el contrato o sustraerse de sus obligaciones se tienen por no escritas. Segunda: el artículo 50 fija requisitos de información para el comercio electrónico, incluido el deber de publicar de forma accesible las condiciones generales del contrato, antes y después de la transacción, y el derecho de retracto cuando proceda. Tercera: las cláusulas abusivas que inviertan la carga de la prueba en perjuicio del consumidor o impliquen renuncia de sus derechos son ineficaces.

Janalytics redacta sus términos con lenguaje claro, evita cláusulas que restrinjan derechos irrenunciables y publica las condiciones generales de forma accesible en su sitio web, en cumplimiento del artículo 50.

8.8 Propiedad intelectual: Ley 23 de 1982 y Decisión Andina 351 de 1993

La Decisión Andina 351 de 1993 define la obra como una creación del intelecto humano y al autor como la persona física creadora. Esa definición tiene una consecuencia directa para la inteligencia artificial generativa: en el estado actual del derecho colombiano, los contenidos producidos de forma autónoma por un sistema de IA sin aporte creativo humano no encajan con facilidad en la categoría de obra protegida por derecho de autor. Janalytics aborda esta incertidumbre con transparencia en los términos de propiedad intelectual de la sección 24 y con una política de uso responsable de contenidos generados.

8.9 Conectividad y continuidad

La Ley 2108 de 2021 reconoce el acceso a internet como servicio público esencial, una declaración que refuerza la importancia de la continuidad en los servicios digitales. Janalytics la toma como referencia para su plan de continuidad de la sección 40, aun cuando el servicio no constituya por sí mismo una prestación de servicios de telecomunicaciones.

9. Regulación emergente: inteligencia artificial en Colombia

9.1 Advertencia sobre el estado de las normas

Las normas descritas en esta sección se encuentran en trámite o son instrumentos de política pública. Se presentan porque anticipan obligaciones futuras y porque Janalytics quiere diseñar su operación de modo que la transición al nuevo marco sea ordenada, no porque sean hoy derecho vigente y exigible. El documento identificará expresamente su carácter cuando corresponda.

9.2 Política Nacional de Inteligencia Artificial: CONPES 4144 de 2025

El 14 de febrero de 2025 el Gobierno Nacional aprobó el Documento CONPES 4144, que adopta la Política Nacional de Inteligencia Artificial. La política tiene por objeto generar las capacidades para la investigación, el desarrollo, la adopción y el aprovechamiento ético y sostenible de sistemas de IA, con el fin de impulsar la transformación social y económica del país, y se estructura en seis ejes estratégicos: ética y gobernanza; datos e infraestructura; investigación, desarrollo e innovación; desarrollo de capacidades y talento digital; mitigación de riesgos; y uso y adopción de la IA en el sector público, el tejido empresarial y los territorios.

El documento contiene más de cien acciones concretas hasta 2030 y una inversión estimada de 479.000 millones de pesos. Su implementación es liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones, el Departamento Administrativo de la Presidencia, el Ministerio de Ciencia, Tecnología e Innovación y el Departamento Nacional de Planeación. Para Janalytics, el eje de mitigación de riesgos y el de uso y adopción empresarial son los más relevantes: confirman que el país apuesta por la adopción responsable de IA y ofrecen un marco de referencia para el diseño de controles.

9.3 Proyecto de Ley de Inteligencia Artificial

El 28 de julio de 2025 el Gobierno presentó ante el Senado el Proyecto de Ley número 043 de 2025 Senado, 324 de 2025 Cámara, que busca regular la inteligencia artificial en Colombia para promover su desarrollo ético, responsable, competitivo e innovador. El proyecto define conceptos y principios de IA, clasifica los sistemas según niveles de riesgo (crítico, alto, con transparencia específica y otros), crea la figura del responsable de IA, exige evaluaciones de impacto para los sistemas de alto riesgo y designa al Ministerio de Ciencia, Tecnología e Innovación como autoridad nacional competente para orientar su implementación. La exposición de motivos reconoce que la Política Nacional de IA marcó un punto de partida, pero que el país carece aún de un marco jurídico integral.

Existen además otras iniciativas en trámite, entre ellas proyectos sobre el deber de información para el uso responsable de la IA, sobre el acceso de niños, niñas y adolescentes a plataformas de IA, y sobre lineamientos para el entrenamiento de modelos. La proliferación de proyectos indica una tendencia regulatoria clara, aunque ninguno es aún ley.

9.4 Qué implica para Janalytics

Janalytics no espera a que el marco se consolide para prepararse. Su diseño anticipatorio se apoya en cuatro decisiones que coinciden con lo que probablemente exigirá la futura ley:

1. Clasificación de sus agentes por nivel de riesgo y aplicación de controles proporcionales: sus servicios actuales se ubican en la categoría de asistencia a tareas repetitivas, no de decisión sobre derechos.
2. Mantenimiento de supervisión humana en las salidas del agente, evitando la decisión plenamente automatizada con efectos jurídicos sobre personas.

3. Documentación de finalidades, base jurídica y medidas de mitigación para cada tipo de tarea, en línea con las evaluaciones de impacto que se prevén.
4. Transparencia: el cliente y, cuando corresponda, el titular, deben poder saber que se está usando un sistema de IA y con qué propósito.

10. Marco internacional de referencia

10.1 Por qué mirar fuera de Colombia

Los clientes de Janalytics pueden operar en varios países, relacionarse con proveedores extranjeros o atender obligaciones contractuales de sus propios clientes. Además, la legislación colombiana se inspira en estándares internacionales, y las normas extranjeras anticipan con frecuencia el rumbo que seguirán las locales. Por eso Janalytics adopta un enfoque de cumplimiento por el estándar más exigente aplicable, sin declarar cumplimiento de normas que no le sean exigibles.

10.2 Reglamento General de Protección de Datos de la Unión Europea

El RGPD es la referencia global en protección de datos. Introduce principios como la minimización, la limitación de la finalidad y la limitación del plazo de conservación; derechos como el acceso, la rectificación, la supresión y la portabilidad; obligaciones como la protección desde el diseño y por defecto, y la notificación de brechas. Janalytics alinea su política de datos con estos principios porque son compatibles y en general más exigentes que los mínimos locales, y porque le permiten atender clientes con operación europea.

10.3 Reglamento Europeo de Inteligencia Artificial

El Reglamento Europeo de IA establece un enfoque basado en el riesgo: prohíbe determinadas prácticas, somete las aplicaciones de alto riesgo a obligaciones estrictas y exige transparencia para ciertas interacciones con sistemas de IA. No es una norma colombiana, pero su lógica —clasificar por riesgo, documentar, supervisar y ser transparente— coincide con la del proyecto de ley colombiano y con la de la Circular Externa 002 de 2024 de la SIC. Janalytics adopta ese enfoque como criterio de diseño.

10.4 NIST AI Risk Management Framework

El marco de gestión de riesgos de IA del Instituto Nacional de Estándares y Tecnología de Estados Unidos organiza la gestión en cuatro funciones: gobernar, mapear, medir y gestionar. Es una guía, no una norma certificable, y su utilidad es práctica: ofrece un lenguaje común para describir riesgos de IA. El documento CONPES 4144 lo cita como referencia, lo que refuerza su pertinencia para el contexto colombiano.

10.5 Principios de la OCDE y normas ISO

Los principios de la OCDE sobre inteligencia artificial —crecimiento inclusivo y bienestar sostenible, derechos humanos y valores democráticos, transparencia y explicabilidad, robustez y seguridad, y rendición de cuentas— constituyen el consenso internacional de referencia. A ellos se suman las normas ISO ya descritas: ISO/IEC 27001 para la seguridad de la información e ISO/IEC 42001 para la gestión de la inteligencia artificial.

10.6 Políticas de datos de los proveedores de modelos

En el plano operativo, la referencia internacional más relevante son las políticas de datos de los proveedores de modelos. OpenAI ofrece retención cero a los clientes empresariales elegibles de su API y mantiene un compromiso de no entrenamiento sobre los datos de esas interfaces. Anthropic declara que los datos enviados por su API no se utilizan para entrenar modelos sin permiso expreso y ofrece acuerdos de retención cero a clientes empresariales que califican. Janalytics se apoya en estas condiciones y las exige como requisito de selección de proveedor, y las documenta en el contrato de transmisión.

11. Matriz de cumplimiento

11.1 Cómo leer la matriz

La matriz relaciona cada obligación relevante con la norma que la impone y con la forma en que Janalytics la satisface. Sirve como herramienta de verificación para el cliente y como lista de control interna. La columna de evidencia indica dónde se documenta o se prueba el cumplimiento.

Obligación	Norma	Cómo la cumple Janalytics	Evidencia
Obtener autorización previa del titular	Ley 1581 de 2012, art. 9; Decreto 1377 de 2013, arts. 5-8	Exige al cliente la base jurídica y conserva constancia; no inicia tratamiento sin ella.	Contrato de transmisión (Anexo C)
Informar la finalidad del tratamiento	Ley 1581 de 2012, art. 9	Finalidad definida por tarea en el contrato y en la política.	Política de tratamiento (Anexo A)
No conservar datos más de lo necesario	Decreto 1377 de 2013, art. 11	Diseño de retención cero del contenido.	Política de retención
Atender derechos de los titulares	Ley 1581 de 2012, art. 8 y ss.	Canal con el cliente y tramitación de solicitudes en plazos.	Procedimiento de solicitudes
Designar responsable de protección de datos	Decreto 1377 de 2013, art. 23	Área responsable designada y publicada.	Política de tratamiento
Demostrar responsabilidad (accountability)	Decreto 1377 de 2013, art. 26	SGSI, registro de activos y riesgos, medición y auditoría interna.	Parte V del documento
Base jurídica para transferencia o transmisión internacional	Ley 1581 de 2012, art. 26; Decreto 1377 de 2013, art. 25	Contrato de transmisión y verificación de proveedores.	Anexo C
Medidas de seguridad apropiadas	Decreto 1377 de 2013, art. 19; Circular 002 de 2024	Controles alineados con ISO/IEC 27001.	Parte V
No entrenar modelos con datos del cliente	Política de Janalytics; Circular 002 de 2024	Compromiso contractual y selección de proveedores.	Sección 5; Anexo C
Guardar confidencialidad	Ley 1581 de 2012; contrato	Cláusulas de confidencialidad y acuerdo con personal y terceros.	Contrato; contratos de subencargados
Informar y publicar condiciones del contrato	Ley 1480 de 2011, arts. 37 y 50	Términos en castellano, claros, publicados de forma accesible.	Sitio web; este documento

Obligación	Norma	Cómo la cumple Janalytics	Evidencia
Validez del contrato electrónico	Ley 527 de 1999	Aceptación electrónica con evidencia de identificación y marca de tiempo.	Registro de aceptación
Supervisión humana de la IA	Circular 002 de 2024; ISO/IEC 42001	El agente produce resultados; la decisión final es del cliente.	Sección 17; Parte V

11.2 Correspondencia con ISO/IEC 27001

Además de la matriz normativa, Janalytics mantiene una correspondencia entre sus controles y el Anexo A de ISO/IEC 27001:2022, incluida en el Anexo D. Esa correspondencia permite al cliente verificar la cobertura por dominio y a Janalytics detectar vacíos.

12. Riesgos legales y de seguridad identificados

12.1 Metodología

Janalytics evalúa sus riesgos con una matriz de probabilidad por impacto. La escala de probabilidad es baja, media o alta; la de impacto, también baja, media o alta. El nivel de riesgo resulta del cruce, y cada riesgo tiene una respuesta asociada. La matriz se revisa periódicamente y se actualiza cuando cambian el servicio, los proveedores o el marco normativo.

12.2 Matriz de riesgos

Riesgo	Prob.	Impacto	Respuesta
Tratamiento de datos personales sin autorización válida del titular.	Media	Alto	Exigir declaración y soporte al cliente; contrato de transmisión; revisión previa de cada nueva tarea.
Uso de los datos del cliente para entrenar modelos por parte de un proveedor.	Baja	Alto	Selección de proveedores con no entrenamiento; cláusulas contractuales; verificación documental.
Brecha de seguridad con exposición de datos.	Media	Alto	Cifrado, control de acceso, aislamiento por cliente, registros, plan de respuesta a incidentes.
Transferencia internacional a país sin nivel adecuado de protección.	Media	Alto	Contrato de transmisión; verificación de estándares de la SIC; declaración de conformidad cuando aplique.
Fallo del proveedor de modelos o cambio en sus políticas de datos.	Media	Medio	Diversificación de proveedores; cláusula de notificación de cambios; revisión contractual.
Resultado del agente erróneo que induce una decisión del cliente.	Media	Medio	Supervisión humana; validación por muestreo; advertencias de uso; limitación de responsabilidad.

Riesgo	Prob.	Impacto	Respuesta
Tratamiento de datos sensibles sin base jurídica reforzada.	Baja	Alto	Declaración previa del cliente; controles reforzados; consentimiento expreso.
Uso del servicio para fines ilícitos o lesivos.	Baja	Alto	Política de uso aceptable; suspensión ante indicios; reporte.
Sanciones de la SIC por incumplimiento en protección de datos.	Baja	Alto	Accountability documentada; auditoría interna; asesoría legal periódica.
Reclamaciones de propiedad intelectual sobre contenidos generados.	Media	Medio	Claridad contractual sobre titularidad; política de uso de contenido generado.
Indisponibilidad del servicio por falla de infraestructura.	Media	Medio	Copias de seguridad; plan de continuidad; SLA con compromiso de recuperación.
Dependencia de un único proveedor de infraestructura.	Media	Medio	Diseño portable; procedimiento de migración; evaluación periódica.

12.3 Riesgos no cubiertos y límites

Janalytics declara con honestidad los riesgos que no controla: el comportamiento de los proveedores de modelos frente a órdenes judiciales o requerimientos legales en sus jurisdicciones; la exactitud absoluta de las salidas de un modelo de lenguaje, que por su naturaleza puede equivocarse; y el uso que el cliente haga de los resultados una vez entregados. Estos límites se reflejan en las cláusulas de responsabilidad de la sección 27 y en la descripción de la naturaleza del servicio de la sección 17.

13. Identificación del prestador del servicio

El servicio es prestado por Jassen Aldair Camargo Caicedo, quien actúa como persona natural comerciante, titular de un establecimiento de comercio bajo el nombre comercial Janalytics. La actividad se desarrolla en su condición personal: no existe una sociedad interpuesta, de modo que los derechos y obligaciones derivados de este documento corresponden directamente a su titular. Sus datos de identificación son los siguientes.

Campo	Dato
Denominación comercial	Janalytics
Titular	Jassen Aldair Camargo Caicedo
NIT	1005180164
Naturaleza jurídica	Persona natural comerciante con establecimiento de comercio
Domicilio	Santander, Barrancabermeja, Dg 56 N 43-30
Matrícula mercantil	[completar número de matrícula y cámara de comercio]
Teléfono	315 444 9545
Correo de contacto general	administracion@janalytics.com.co

Campo	Dato
Correo de protección de datos	administracion@janalytics.com.co
Correo de seguridad	administracion@janalytics.com.co
Sitio web	https://www.janalytics.com.co
Área responsable de protección de datos	Jassen Aldair Camargo Caicedo

Janalytics es el nombre comercial con el que se identifica el establecimiento de comercio. Al tratarse de una persona natural, no existe la separación patrimonial propia de las sociedades: el titular responde con su patrimonio por las obligaciones que asume, sin perjuicio de los límites que la ley establezca. Esta circunstancia se refleja en las cláusulas de responsabilidad de la sección 27 y el cliente debe conocerla.

14. Objeto y descripción del servicio

14.1 Objeto

Janalytics presta servicios de automatización de tareas repetitivas mediante agentes de inteligencia artificial, y servicios conexos de analítica de datos, configuración, soporte y mantenimiento. El objeto del contrato se define en cada caso por la descripción de tareas acordada con el cliente, que forma parte integrante de los términos.

14.2 Componentes del servicio

El servicio (en adelante, el Agentic OS) comprende, según el plan contratado, los siguientes componentes:

- **Agente de IA por cliente**: un agente configurado para ejecutar las tareas acordadas, con memoria y almacenamiento separados del resto de clientes.
- **Panel de gobierno**: interfaz administrativa desde la cual Janalytics administra empresas, usuarios y tareas.
- **Aplicación del cliente**: interfaz mediante la cual los usuarios autorizados conversan con su agente, cargan y descargan archivos, consultan tareas y resultados y gestionan tareas programadas.
- **Mecanismo de acceso por pase**: sistema por el cual un usuario autorizado accede a la aplicación de su empresa mediante un pase emitido desde el panel, sin credenciales propias.
- **Soporte y mantenimiento**: atención de incidencias y ajustes, en los términos de la sección 28.

14.3 Exclusiones

Salvo pacto expreso y por escrito, no forman parte del servicio: el suministro de hardware o conectividad del cliente; la corrección de la calidad de los datos de origen del cliente; el cumplimiento de obligaciones legales propias del cliente (tributarias, laborales, contables o de protección de datos como responsable); la toma de decisiones de negocio; la asesoría jurídica, contable o financiera; y la atención de titulares de datos personales cuando el cliente actúa como responsable.

14.4 Entregables

Cada tarea produce un entregable definido en la descripción acordada: por ejemplo, un archivo procesado, un reporte de anomalías o un borrador de respuesta. Los entregables se ponen a

disposición del cliente en su aplicación y su custodia final corresponde al cliente. Janalytics no garantiza la utilización que el cliente haga del entregable ni el resultado de negocio derivado de él.

15. Aceptación de los términos

15.1 Formas de aceptación

Estos términos se entienden aceptados por el cliente cuando realiza cualquiera de las siguientes conductas: (i) firma electrónica o manuscrita del contrato o de la orden de servicio; (ii) aceptación expresa mediante casilla de verificación, botón de aceptación o mecanismo equivalente en el sitio web o en la aplicación; (iii) utilización del servicio tras haber recibido estos términos; o (iv) cualquier conducta inequívoca que permita concluir razonablemente que otorgó su aceptación, en los términos del artículo 7 del Decreto 1377 de 2013 aplicado analógicamente. El silencio no constituye aceptación.

15.2 Validez del contrato electrónico

De conformidad con la Ley 527 de 1999, la oferta y su aceptación pueden expresarse por medio de mensajes de datos, y no se niega validez ni fuerza obligatoria al contrato por haberse formado mediante mensajes de datos. La firma electrónica tiene la misma validez y efectos jurídicos que la firma manuscrita cuando cumple los requisitos legales. Janalytics conserva evidencia de la aceptación, con identificación del aceptante y marca de tiempo, para efectos probatorios.

15.3 Documentos que integran el acuerdo

Forman parte del acuerdo: estos términos y condiciones; la descripción de tareas acordada con el cliente; la política de tratamiento de datos personales (Anexo A); el contrato de transmisión de datos personales (Anexo C); y las órdenes de servicio o cotizaciones aceptadas. En caso de conflicto entre documentos, prevalecerá el documento más específico sobre el general, y dentro de cada uno, la cláusula manuscrita o negociada sobre la condición general.

16. Capacidad legal y registro

El cliente declara que actúa con capacidad legal suficiente y, cuando contrata en nombre de una persona jurídica, que cuenta con las facultades necesarias para obligarla. El cliente se obliga a suministrar información veraz sobre su identidad y la de sus usuarios autorizados, y a mantenerla actualizada.

El cliente es responsable de verificar que la contratación y el uso del servicio cumplen las normas aplicables a su propia actividad, incluido su régimen sectorial, sus obligaciones de protección de datos como responsable y cualquier autorización que requiera. Janalytics no es responsable por el incumplimiento de esas obligaciones propias del cliente.

17. Naturaleza del servicio y supervisión humana

17.1 Obligación de medio

El servicio se presta como una obligación de medio, no de resultado. Janalytics se obliga a ejecutar las tareas contratadas con diligencia, aplicando los controles de calidad y de seguridad descritos en este documento, pero no garantiza un resultado específico de negocio ni la ausencia absoluta de error en las salidas del agente. Los modelos de lenguaje son herramientas probabilísticas: pueden

producir respuestas inexactas, incompletas o inapropiadas, y su uso exige revisión humana.

17.2 Supervisión humana

Janalytics diseña sus agentes como asistentes, no como decisores. El agente propone, calcula, clasifica o redacta; la decisión que afecta derechos o intereses del cliente o de terceros corresponde a una persona. Esta arquitectura responde a la ambigua regulación local y a los lineamientos de la SIC: los agentes de Janalytics no toman decisiones plenamente automatizadas sobre personas, y el cliente conserva la responsabilidad final sobre los resultados que utilice.

17.3 Deber de revisión del cliente

El cliente se obliga a revisar los entregables antes de utilizarlos, especialmente cuando tengan efectos frente a terceros o frente a una autoridad. Cuando el entregable se destine a una obligación legal del cliente (por ejemplo, una declaración o un pago), la verificación previa es una carga ineludible del cliente.

17.4 Declaración sobre el uso de IA

Cuando el cliente se relacione con terceros o con titulares de datos mediante contenido producido con asistencia de IA, deberá informarlo de forma clara cuando la norma aplicable o la naturaleza de la interacción lo exija. Janalytics pone a disposición del cliente esta declaración como parte del servicio.

18. Acceso, cuentas, credenciales y pases

18.1 Usuarios autorizados

El cliente designa a los usuarios autorizados que podrán acceder al servicio y responde por su uso. Cada usuario es personal e intransferible. El cliente debe informar a Janalytics sobre el retiro de usuarios y mantener actualizada la lista de personas con acceso.

18.2 Acceso por pase

En el modelo de acceso por pase, el usuario autorizado accede a la aplicación de su empresa mediante un pase de un solo uso emitido desde el panel de gobierno. El pase es personal, tiene vigencia limitada y no puede compartirse ni reutilizarse. El cliente es responsable de que el enlace o pase no se difunda a personas no autorizadas.

18.3 Credenciales y seguridad de la cuenta

Cuando el acceso requiera credenciales, el cliente se obliga a: usar contraseñas robustas y no compartirlas; activar los mecanismos de segundo factor que el servicio ofrezca; no permitir el acceso simultáneo desde ubicaciones no autorizadas; y notificar de inmediato a Janalytics cualquier sospecha de uso indebido. Janalytics nunca solicitará al usuario su contraseña por correo ni por teléfono.

18.4 Suspensión de accesos

Janalytics podrá suspender o revocar un acceso cuando exista un riesgo de seguridad, un uso contrario a la sección 23, una orden de autoridad competente o el incumplimiento de las obligaciones de pago, dando aviso al cliente cuando sea posible.

19. Planes, precios, facturación y pagos

19.1 Planes

Janalytics ofrece planes de servicio definidos por el alcance de las tareas, la frecuencia de ejecución, el número de usuarios y el nivel de soporte. El detalle de cada plan se documenta en la cotización o en la orden de servicio aceptada.

19.2 Precios y moneda

Los precios se expresan en la moneda y con los impuestos que indique la cotización. Janalytics podrá actualizar los precios de los servicios de ejecución continua avisando al cliente con una antelación razonable. Los cambios de precio no afectan los servicios ya facturados.

19.3 Facturación y pago

La facturación sigue la periodicidad acordada. Cuando se pacte un pago inicial, este habilita el inicio de la configuración. El cliente debe pagar dentro del plazo indicado en la factura; el retardo faculta a Janalytics a suspender el servicio conforme a la sección 20.4 y a cobrar los intereses de mora que autorice la ley.

19.4 Costos de terceros

Los servicios pueden implicar costos de terceros, como el consumo de interfaces de modelos de lenguaje, la infraestructura de servidores o los servicios de mensajería. Salvo pacto expreso, esos costos se facturan al cliente y Janalytics no los absorbe. Janalytics informa su estimación y procura evitar consumos desproporcionados.

19.5 Impuestos

Los precios no incluyen los impuestos aplicables, que serán asumidos por el cliente conforme a la ley colombiana. El cliente suministrará la información fiscal necesaria para la facturación.

20. Plazo, vigencia, suspensión y terminación

20.1 Vigencia

El contrato tiene la vigencia pactada en la orden de servicio. A falta de pacto, se entiende de duración indefinida, con posibilidad de terminación por cualquiera de las partes mediante aviso previo por escrito con la antelación acordada. Cuando la relación califique como de consumo, se respetarán los límites legales sobre permanencia mínima y las reglas de renovación del Estatuto del Consumidor.

20.2 Renovación

Cuando se pacte renovación automática, el cliente será informado de su derecho a manifestar su voluntad de no renovar antes de la fecha de renovación. Janalytics no renewará servicios que generen costos al cliente sin su aceptación expresa cuando la norma aplicable lo prohíba.

20.3 Terminación

Son causales de terminación: el mutuo acuerdo; el vencimiento del plazo sin renovación; el incumplimiento grave no subsanado dentro del plazo razonable que Janalytics conceda; el uso del servicio contrario a la sección 23; y la imposibilidad sobreviniente de prestar el servicio por causas

técnicas atribuibles al proveedor de infraestructura, con aviso al cliente.

20.4 Suspensión

Janalytics podrá suspender el servicio, dando aviso al cliente cuando sea posible, por: falta de pago; riesgo de seguridad; requerimiento de autoridad; o incumplimiento de las obligaciones del cliente. La suspensión no exonera al cliente de las obligaciones causadas antes de su adopción.

20.5 Efectos de la terminación

A la terminación, Janalytics: (i) pondrá a disposición del cliente, por un plazo razonable, los entregables que se encuentren en su poder; (ii) procederá a la supresión de los datos del cliente conforme a la sección 6.7 y a la política de retención, salvo que una norma legal exija conservarlos; y (iii) cesará el tratamiento de datos personales por cuenta del cliente, devolviéndolos o suprimiéndolos según las instrucciones que reciba. Las obligaciones de confidencialidad, propiedad intelectual y responsabilidad subsisten a la terminación en los términos de la ley.

21. Obligaciones de Janalytics

Janalytics se obliga a:

1. Prestar el servicio con diligencia y con los estándares de seguridad y de protección de datos descritos en este documento.
2. Mantener el aislamiento entre clientes y no acceder a los datos de un cliente para finalidades distintas de la prestación del servicio, la seguridad o el cumplimiento legal.
3. No conservar los datos del cliente más allá de lo necesario y no utilizarlos para entrenar modelos, conforme a las secciones 4 y 5.
4. Implementar y mantener los controles de seguridad de la Parte V y revisarlos periódicamente.
5. Notificar al cliente los incidentes de seguridad que afecten sus datos, en los términos de la sección 39.
6. Apoyar al cliente, como responsable, en la atención de solicitudes de titulares y en el cumplimiento de sus obligaciones de protección de datos.
7. Exigir a sus subencargados condiciones equivalentes de seguridad, confidencialidad y no entrenamiento, y responder por su actuación.
8. Informar al cliente sobre cambios sustanciales en el servicio, los proveedores o las políticas de datos.
9. Guardar confidencialidad sobre la información del cliente conforme a la sección 25.
10. Cumplir la normatividad colombiana aplicable, en particular la Ley 1581 de 2012 y las circulares de la SIC.

22. Obligaciones del cliente

El cliente se obliga a:

1. Suministrar información veraz, completa y actualizada, y contar con la autorización de los titulares de datos personales que entregue al servicio, conservando su prueba.
2. Informar a Janalytics si el servicio tratará datos sensibles o datos de niños, niñas y adolescentes, y obtener las autorizaciones reforzadas que la ley exija.

3. Designar y controlar a sus usuarios autorizados, custodiar las credenciales y los pases, y reportar el retiro de usuarios.
4. Revisar los entregables antes de utilizarlos, conforme a la sección 17.3.
5. No utilizar el servicio para fines ilícitos ni para las conductas prohibidas de la sección 23.
6. Cumplir sus obligaciones de pago y suministrar la información fiscal necesaria.
7. Cumplir las obligaciones legales que le corresponden como responsable del tratamiento y como empresario en su actividad.
8. Informar a Janalytics sobre los cambios en su operación que afecten el alcance del servicio, la seguridad o el tratamiento de datos.
9. Mantener indemne a Janalytics frente a reclamaciones de terceros derivadas del incumplimiento de las obligaciones del cliente, en los términos de la sección 27.5.

23. Uso aceptable y usos prohibidos

23.1 Principio general

El servicio debe utilizarse para automatizar tareas legítimas de la operación del cliente y en el marco de la ley. Janalytics puede suspender el servicio ante un uso contrario a esta sección, sin perjuicio de las demás consecuencias contractuales.

23.2 Usos prohibidos

El cliente no podrá utilizar el servicio para:

1. Realizar tratamiento de datos personales sin autorización válida del titular o sin base jurídica suficiente.
2. Tratar datos sensibles o de niños, niñas y adolescentes sin el cumplimiento de las condiciones legales reforzadas.
3. Tomar decisiones plenamente automatizadas que afecten derechos o intereses de personas sin supervisión humana.
4. Generar o difundir contenido engañoso, fraudulento, difamatorio, discriminatorio o que induzca a error.
5. Suplantar la identidad de personas o de entidades, o simular comunicaciones oficiales.
6. Realizar actividades ilícitas, incluidas el fraude, el lavado de activos, la corrupción o cualquier conducta tipificada en la ley penal, y en particular las conductas de la Ley 1273 de 2009.
7. Vulnerar derechos de propiedad intelectual de terceros o usar contenido sin la autorización correspondiente.
8. Intentar acceder a datos de otros clientes, vulnerar el aislamiento de la plataforma o superar los controles de seguridad.
9. Eludir la facturación, revender el servicio sin autorización o utilizarlo para prestar servicios a terceros fuera del alcance contratado.
10. Utilizar el servicio de forma que pueda causar daño a Janalytics, a otros clientes o a terceros.

23.3 Consecuencias

El uso prohibido faculta a Janalytics a suspender el servicio de inmediato, a terminar el contrato por incumplimiento grave y a exigir la indemnización de los perjuicios causados. Cuando exista un deber legal de reportar la conducta, Janalytics informará a la autoridad competente.

24. Propiedad intelectual

24.1 Titularidad de la plataforma

La plataforma Janalytics, incluidos su código fuente, su arquitectura, sus herramientas, sus componentes de software, su marca, sus logotipos, sus manuales y su documentación, son propiedad de Janalytics o de sus licenciantes y están protegidos por las normas de propiedad intelectual, en particular la Ley 23 de 1982 y la Decisión Andina 351 de 1993. El contrato no transfiere al cliente ningún derecho de propiedad sobre la plataforma: otorga únicamente una licencia de uso limitada, no exclusiva, no transferible y revocable, vigente mientras dure el contrato y limitada al alcance contratado.

24.2 Datos y contenidos del cliente

El cliente conserva todos los derechos sobre sus datos, archivos y contenidos. Janalytics no adquiere titularidad alguna sobre ellos y solo los trata para prestar el servicio, conforme a la sección 26. El cliente otorga a Janalytics una licencia limitada y necesaria para procesar esos datos con la única finalidad de ejecutar las tareas contratadas.

24.3 Entregables

Los entregables producidos por el agente a partir de los datos del cliente se ponen a disposición del cliente para su uso interno. Janalytics no reclama titularidad sobre ellos. En la medida en que un entregable consista en contenido textual generado por un modelo, se aplican las consideraciones de la sección 24.4.

24.4 Contenido generado con inteligencia artificial

Janalytics informa con transparencia una limitación del derecho vigente: la Decisión Andina 351 de 1993 define la obra como una creación del intelecto humano y al autor como la persona física creadora. Por ello, el contenido producido de forma autónoma por un sistema de IA, sin aporte creativo humano, puede no ser susceptible de protección por derecho de autor bajo el marco aplicable en Colombia. Janalytics no garantiza la existencia de derechos de autor sobre el contenido íntegramente generado por IA, y recomienda al cliente que aporte valor creativo humano cuando necesite protección. Janalytics no asume responsabilidad por reclamaciones de terceros derivadas del uso de contenido generado, salvo dolo o culpa grave.

24.5 Marcas y referencias

Ninguna parte podrá usar la marca, el nombre comercial o los logotipos de la otra sin autorización previa y escrita. Janalytics podrá mencionar al cliente como referencia comercial solo con su consentimiento.

24.6 Retroalimentación

Las sugerencias, comentarios o mejoras que el cliente aporte sobre la plataforma podrán ser utilizados por Janalytics sin restricción y sin contraprestación, sin que ello implique revelar información confidencial del cliente.

25. Confidencialidad

25.1 Alcance

Cada parte se obliga a mantener en reserva la información confidencial de la otra a la que acceda con ocasión del contrato, y a usarla únicamente para ejecutarlo. Se considera confidencial toda información no pública, incluidos datos personales, datos de negocio, precios, procesos y secretos empresariales.

25.2 Excepciones

No es confidencial la información que: sea de dominio público sin culpa del receptor; hubiera sido conocida legítimamente antes del contrato; sea recibida legítimamente de un tercero sin deber de reserva; o deba revelarse por mandato legal o de autoridad competente. En este último caso, la parte obligada dará aviso previo a la otra cuando sea posible.

25.3 Duración

La obligación de confidencialidad subsiste durante la vigencia del contrato y por un plazo razonable posterior a su terminación, sin límite cuando se trate de datos personales o de secretos empresariales protegidos por ley.

25.4 Personas con acceso

Janalytics limita el acceso a la información confidencial a las personas que lo necesitan para prestar el servicio y las obliga a guardar reserva. La misma regla se exige a los subencargados.

26. Protección de datos personales: roles y garantías

26.1 Distribución de roles

En la relación de tratamiento derivada del servicio, el cliente es responsable del tratamiento y Janalytics es encargado. El cliente decide sobre las bases de datos, las finalidades y las instrucciones; Janalytics ejecuta esas instrucciones y responde por la seguridad y la confidencialidad de la información que le fue confiada.

26.2 Obligaciones de Janalytics como encargado

Janalytics, como encargado, se obliga a: tratar los datos personales conforme a los principios de la Ley 1581 de 2012 y a las instrucciones del cliente; salvaguardar la seguridad de las bases de datos; guardar confidencialidad; no tratar los datos para una finalidad distinta de la autorizada; no transferir los datos a terceros sin instrucción o base jurídica, salvo los subencargados necesarios para prestar el servicio; dar traslado al cliente de las consultas y reclamos de los titulares; y suprimir o devolver los datos al terminar el contrato, según la instrucción del cliente. Estas obligaciones corresponden a las que exige el artículo 25 del Decreto 1377 de 2013 y se detallan en el Anexo C.

26.3 Subencargados

Janalytics podrá utilizar subencargados, en particular proveedores de modelos de lenguaje e infraestructura, para prestar el servicio. Janalytics: informa al cliente la categoría de subencargados utilizados; impone a cada subencargado obligaciones equivalentes de seguridad, confidencialidad y no entrenamiento; y responde frente al cliente por la actuación de sus subencargados. El cliente podrá oponerse a un subencargado concreto por razones fundadas de seguridad o cumplimiento; en

tal caso, las partes acordarán la mejor alternativa disponible.

26.4 Transferencia y transmisión internacional

Cuando el servicio implique comunicación de datos a proveedores ubicados en el exterior, se aplican las reglas de la sección 6.8. Janalytics verificará que el proveedor cuente con nivel adecuado de protección en los términos de la SIC o que exista una causal de excepción, y en todo caso suscribirá el contrato de transmisión del artículo 25 del Decreto 1377 de 2013. La operación transfronteriza no se realizará si no se cumplen estas condiciones.

26.5 Incidentes que afecten datos personales

Ante un incidente de seguridad que afecte datos personales tratados por cuenta del cliente, Janalytics notificará al cliente sin dilación indebida, con la información disponible, para que el cliente, como responsable, cumpla sus obligaciones de información y de atención. La sección 39 define el procedimiento.

26.6 Derechos de los titulares

Cuando un titular ejerza sus derechos ante Janalytics, esta dará traslado al cliente como responsable y prestará el apoyo necesario para atender la solicitud dentro de los plazos legales.

27. Garantías, responsabilidad e indemnidad

27.1 Garantías

Janalytics garantiza que: prestará el servicio con diligencia y conforme a la descripción contratada; posee las autorizaciones necesarias para ofrecer el servicio; el servicio no infringe, hasta donde conoce, derechos de propiedad intelectual de terceros; y aplicará las medidas de seguridad y de protección de datos descritas en este documento. Janalytics no garantiza la ausencia total de error en las salidas del agente, la disponibilidad ininterrumpida del servicio ni un resultado de negocio determinado.

27.2 Limitación de responsabilidad

Salvo dolo o culpa grave, y sin perjuicio de los derechos irrenunciables del consumidor cuando aplique, la responsabilidad total de Janalytics derivada del contrato se limita al monto efectivamente pagado por el cliente por el servicio durante los doce meses anteriores al hecho que origina la reclamación. Janalytics no responde por lucro cesante, daño indirecto, pérdida de oportunidad ni daño consecuencial.

27.3 Eximentes

Janalytics no responde por el daño derivado de: la calidad o legalidad de los datos suministrados por el cliente; el uso que el cliente haga de los entregables; la inexactitud inherente a las salidas de un modelo de lenguaje cuando el cliente omitió la revisión debida; el hecho de un tercero ajeno al control de Janalytics; el incumplimiento por el cliente de sus obligaciones legales; y los casos de fuerza mayor o caso fortuito.

27.4 Responsabilidad frente a los titulares

Frente a los titulares de datos personales, la responsabilidad principal es del cliente como responsable. Janalytics responde en su calidad de encargado en los términos de la ley y de este

documento. La distribución de responsabilidades se detalla en el Anexo C.

27.5 Indemnidad

El cliente mantendrá indemne a Janalytics frente a reclamaciones, sanciones o perjuicios derivados de: datos suministrados sin base jurídica; uso del servicio contrario a la sección 23; incumplimiento de las obligaciones del cliente; y reclamaciones de terceros por el uso que el cliente dé a los entregables. Recíprocamente, Janalytics mantendrá indemne al cliente frente a reclamaciones derivadas de un incumplimiento atribuible a Janalytics en la prestación del servicio.

27.6 Seguro

Cuando la operación lo justifique, Janalytics podrá contratar un seguro de responsabilidad civil. La existencia y el alcance del seguro se informarán al cliente que lo solicite. A la fecha de esta versión, [indicar si existe póliza vigente y sus coberturas].

28. Niveles de servicio y soporte

28.1 Disponibilidad

Janalytics procurará mantener la disponibilidad del servicio conforme al nivel comprometido en el plan contratado. El nivel de disponibilidad se calcula sobre el tiempo del periodo de medición y excluye las ventanas de mantenimiento programado y las interrupciones atribuibles a terceros o al cliente.

28.2 Tiempos de respuesta y resolución

Los incidentes se clasifican por severidad y cada nivel tiene un tiempo objetivo de primera respuesta y de resolución. La tabla siguiente es una referencia que se concreta en cada contrato.

Severidad	Descripción	Respuesta objetivo	Resolución objetivo
Crítica	Servicio no disponible o riesgo de seguridad con afectación de datos.	2 horas hábiles	8 horas hábiles
Alta	Función principal degradada sin alternativa.	4 horas hábiles	2 días hábiles
Media	Función secundaria afectada con alternativa disponible.	1 día hábil	5 días hábiles
Baja	Consulta, mejora o ajuste menor.	2 días hábiles	Según acuerdo

28.3 Ventanas de mantenimiento

Janalytics podrá realizar mantenimientos programados, procurando avisar al cliente con antelación razonable y ejecutarlos en horarios de bajo impacto. Los mantenimientos de urgencia por razones de seguridad podrán ejecutarse sin aviso previo, informando al cliente después.

28.4 Exclusión del SLA

El nivel de servicio no aplica a interrupciones derivadas de: causa imputable al cliente; uso indebido; fallas de conectividad del cliente; interrupciones de proveedores de infraestructura o de modelos fuera del control de Janalytics; y fuerza mayor.

29. Modificaciones de los términos

29.1 Regla general

Janalytics podrá modificar estos términos por razones normativas, técnicas o de seguridad, o para introducir mejoras. Las modificaciones se comunicarán al cliente con antelación razonable y entrarán en vigencia en la fecha indicada. El cliente podrá terminar el contrato sin penalidad si no acepta los cambios sustanciales, dentro del plazo que se le informe.

29.2 Límites

Janalytics no podrá modificar unilateralmente las cláusulas que la ley sustrae de la disposición de las partes, ni las que impliquen renuncia de derechos irrenunciables. Cuando la relación sea de consumo, se respetarán las prohibiciones del Estatuto del Consumidor sobre cláusulas que permitan al proveedor modificar unilateralmente el contrato o sustraerse de sus obligaciones.

29.3 Control de versiones

Cada versión de este documento se identifica con un número y una fecha. El historial de versiones se incluye en el Anexo F y la versión vigente estará publicada en el sitio web.

30. Comunicaciones y notificaciones

Las comunicaciones entre las partes se realizarán por los canales indicados en la sección 13 y en la orden de servicio. Se reconocen como válidas las comunicaciones por correo electrónico dirigidas a las direcciones registradas, que constituyen mensajes de datos con plena eficacia probatoria conforme a la Ley 527 de 1999. Cada parte debe informar a la otra el cambio de sus datos de contacto.

Las notificaciones relativas a incidentes de seguridad, suspensión o terminación se realizarán por correo electrónico y, cuando la urgencia lo justifique, por un canal adicional acordado.

31. Ley aplicable y solución de controversias

31.1 Ley aplicable

Este contrato se rige por las leyes de la República de Colombia. Se aplican en particular la Ley 1581 de 2012 y sus decretos reglamentarios, la Ley 527 de 1999, la Ley 1480 de 2011 cuando corresponda y las normas de propiedad intelectual aplicables.

31.2 Reclamación directa

Antes de acudir a una instancia judicial o arbitral, las partes procurarán resolver la controversia mediante comunicación directa y, si es del caso, mediante conciliación extrajudicial ante un centro de conciliación legalmente establecido. La reclamación directa podrá presentarse por escrito o por medios electrónicos.

31.3 Jurisdicción

Agotada la etapa anterior sin acuerdo, las controversias se someterán a la jurisdicción ordinaria colombiana, salvo que las partes acuerden por escrito un mecanismo arbitral. Cuando el cliente sea consumidor, se respetarán las reglas de competencia y las acciones jurisdiccionales de protección al consumidor del Estatuto del Consumidor, que son irrenunciables.

31.4 Protección de datos

Cuando la controversia verse sobre protección de datos personales, el titular o el responsable podrán acudir a la Superintendencia de Industria y Comercio en ejercicio de las facultades que la ley le confiere, sin perjuicio de las demás acciones.

32. Disposiciones varias

32.1 Integridad

Este documento, junto con los documentos que lo integran según la sección 15.3, constituye el acuerdo completo entre las partes sobre su objeto y reemplaza cualquier entendimiento anterior sobre las mismas materias.

32.2 Divisibilidad

Si una cláusula fuera declarada nula o ineficaz, las demás conservarán su validez y la cláusula afectada se interpretará de modo que se aproxime mejor a la intención de las partes dentro de la ley, conforme al artículo 44 de la Ley 1480 de 2011.

32.3 Cesión

El cliente no podrá ceder el contrato sin autorización previa y escrita de Janalytics. Janalytics podrá cederlo a un tercero, incluida una sociedad que asuma la prestación del servicio, informando al cliente y preservando las condiciones de protección de datos y de seguridad.

32.4 Independencia de las partes

El contrato no crea una relación laboral, de sociedad, de agencia ni de representación entre las partes. Cada parte actúa de forma independiente.

32.5 Ausencia de renuncia

La tolerancia de una parte frente a un incumplimiento de la otra no constituye renuncia a exigirlo en el futuro.

32.6 Idioma

El contrato se celebra en idioma castellano, conforme al artículo 37 de la Ley 1480 de 2011. Cualquier traducción es solo informativa.

32.7 Subsistencia

Subsisten a la terminación las cláusulas de confidencialidad, propiedad intelectual, protección de datos, limitación de responsabilidad e indemnidad, y las que por su naturaleza deban perdurar.

33. Política de seguridad de la información

33.1 Declaración de la política

Janalytics protege la información que le confían sus clientes como condición de existencia de su negocio, no como un requisito accesorio. La dirección de la empresa asume el compromiso de establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información, de proteger la confidencialidad, integridad y disponibilidad de la información, de cumplir los requisitos legales y contractuales aplicables y de mejorar de forma continua el

desempeño de seguridad. Esta declaración corresponde al control A.5.1 de ISO/IEC 27001:2022 y se concreta en las políticas de las secciones siguientes.

33.2 Alcance del sistema de gestión

El alcance del sistema de gestión de seguridad de la información de Janalytics comprende: la plataforma Agentic OS; los entornos de los agentes por cliente; el panel de gobierno; la aplicación del cliente; los datos tratados por cuenta de los clientes; y las personas, procesos y proveedores que intervienen en su operación. Quedan fuera del alcance los sistemas personales de los usuarios del cliente y los servicios de terceros que el cliente conecte por fuera de Janalytics.

33.3 Principios rectores

- **Privacidad desde el diseño y por defecto**: la protección se incorpora en el diseño de cada componente y se activa sin requerir acción del usuario.
- **Mínimo privilegio**: cada persona y cada componente accede solo a lo necesario para su función.
- **Defensa en profundidad**: controles en capas, de modo que la falla de uno no comprometa todo el sistema.
- **Aislamiento por cliente**: la información de un cliente no se mezcla con la de otro.
- **No persistencia del contenido**: los datos del cliente no se conservan más allá de lo necesario, conforme a la sección 4.
- **Trazabilidad**: las acciones relevantes quedan registradas y son auditables.
- **Mejora continua**: los controles se revisan, se miden y se ajustan.

33.4 Responsabilidades

La dirección de Janalytics responde por la aprobación de la política, la asignación de recursos y la revisión periódica del sistema. Un responsable de seguridad coordina la implementación de los controles, la gestión de incidentes y la relación con los proveedores. Un responsable de protección de datos atiende las funciones del artículo 23 del Decreto 1377 de 2013. Todo el personal con acceso a información de clientes asume deberes de confidencialidad y de uso adecuado.

34. Modelo de seguridad y arquitectura de confianza

34.1 Aislamiento por cliente

La decisión arquitectónica central del Agentic OS es el aislamiento. Cada cliente opera en un entorno propio, con su propia memoria y su propio almacenamiento, de modo que la información no se comparte ni se agrega entre clientes. Este aislamiento es la principal barrera contra la fuga de datos entre organizaciones y corresponde al principio de acceso y circulación restringida de la Ley 1581 de 2012.

34.2 Exposición mínima

Los entornos de los agentes no exponen puertos a internet: solo la capa de acceso autorizada es accesible, y lo hace mediante conexiones cifradas. Los servicios internos se comunican en canales internos, no expuestos. Este diseño reduce la superficie de ataque y limita las posibilidades de acceso no autorizado que tipifica la Ley 1273 de 2009.

34.3 Autenticación de las comunicaciones internas

Las comunicaciones entre componentes del sistema se autentican mediante secretos compartidos y firmas de integridad, de modo que un componente no autorizado no pueda suplantar a otro ni alterar el contenido de una instrucción. Cada entorno tiene su propio secreto, que se rota periódicamente.

34.4 Principio de no confianza en el contenido

Janalytics asume que las entradas —documentos, textos y archivos— pueden contener contenido malicioso o instrucciones no previstas. Los agentes operan con alcance limitado a la tarea contratada y no ejecutan acciones sobre el sistema fuera de ese alcance. Las herramientas disponibles para el agente se restringen a las necesarias para la tarea.

34.5 Gestión de activos

Janalytics mantiene un inventario de activos de información —datos, sistemas, infraestructura, cuentas y proveedores— con su propietario y su clasificación. La clasificación distingue información pública, interna, confidencial y restringida, y define los controles aplicables a cada nivel, conforme al control A.5.9 de ISO/IEC 27001:2022.

35. Gestión de accesos e identidad

35.1 Registro y aprobación de accesos

Todo acceso a sistemas y datos se otorga previa aprobación, se asocia a una persona identificada y se limita a lo necesario para su función. No existen cuentas compartidas ni genéricas, salvo las estrictamente técnicas, que se custodian de forma reforzada y se auditan.

35.2 Autenticación

El acceso a los sistemas administrativos exige autenticación con credenciales individuales y, cuando el servicio lo permite, un segundo factor. Las contraseñas se almacenan cifradas mediante funciones de derivación, nunca en texto claro. El acceso de los usuarios autorizados del cliente se realiza mediante el mecanismo de pase de un solo uso descrito en la sección 18.2, que reduce la exposición de credenciales persistentes.

35.3 Mínimo privilegio y revisión

Los permisos se asignan por rol y se revisan periódicamente. Cuando una persona cambia de función o cesa su relación, sus accesos se ajustan o se revocan. Janalytics mantiene un procedimiento de baja que incluye la revocación de credenciales y la devolución de activos.

35.4 Acceso de terceros

El acceso de proveedores a información de clientes se limita a lo indispensable, requiere justificación, se registra y se somete a los mismos deberes de confidencialidad. Cuando un proveedor no necesita acceso a datos, se le niega por diseño.

35.5 Registro de actividad

Janalytics registra los eventos de autenticación, los cambios de configuración y las acciones administrativas relevantes, con marca de tiempo y responsable. Los registros permiten reconstruir quién hizo qué y cuándo, y son la base de la detección de incidentes.

36. Cifrado y protección de datos

36.1 Cifrado en tránsito

Toda comunicación entre el usuario y el servicio, y entre los componentes internos que lo requieran, se realiza mediante protocolos cifrados con certificados válidos. Las conexiones cifradas protegen la información frente a la interceptación, conducta tipificada por la Ley 1273 de 2009.

36.2 Cifrado en reposo

La información almacenada se protege mediante cifrado a nivel de volumen y de archivo, según el componente. Las credenciales y los secretos se almacenan cifrados y se gestionan de forma separada del código.

36.3 Clasificación y manejo

La información se clasifica y se maneja conforme a su nivel. La información confidencial y restringida exige controles reforzados de acceso, registro y transferencia. Los datos sensibles, cuando el cliente los declare, se tratan con el nivel de protección más alto disponible.

36.4 Separación de entornos

Janalytics separa los entornos de desarrollo, pruebas y producción. No se utilizan datos reales de clientes en entornos de desarrollo: cuando se requiere información representativa, se emplean datos sintéticos o anonimizados, conforme a la privacidad desde el diseño que exige la Circular Externa 002 de 2024 de la SIC.

36.5 Destrucción segura

Cuando la información debe suprimirse, se aplican procedimientos de borrado que impiden su recuperación razonable, incluida la eliminación de copias y de versiones residuales dentro de los ciclos de rotación.

37. Ciclo de vida y retención de la información

37.1 Principio de conservación mínima

La información se conserva únicamente durante el tiempo necesario para la finalidad que justificó su tratamiento, salvo que una norma legal o un vínculo contractual exija conservarla. Esta regla desarrolla el principio de temporalidad o necesidad de la Ley 1581 de 2012 y el artículo 11 del Decreto 1377 de 2013.

37.2 Plazos de retención

La tabla siguiente resume los plazos aplicados por Janalytics. Los plazos son referenciales y se concretan en la política de retención interna, sujeta a revisión.

Tipo de información	Retención	Fundamento
Contenido de datos del cliente enviado al modelo	No se retiene; se elimina al terminar el procesamiento	Retención cero (sección 4)
Archivos temporales de trabajo del agente	Se eliminan al completar la tarea, salvo instrucción del cliente	Minimización
Entregables	Custodia del cliente en su entorno	El cliente es responsable final
Metadatos de operación	Plazo definido para operación y auditoría, sin contenido	Necesidad operativa

Tipo de información	Retención	Fundamento
Registros de seguridad y auditoría	Plazo alineado con la sección 41	Seguridad y accountability
Documentación contractual y contable	Plazos legales aplicables	Obligación legal

37.3 Supresión a solicitud

Cuando el cliente instruya la supresión de datos, Janalytics la ejecutará en los sistemas bajo su control dentro del plazo acordado y le confirmará el resultado. Cuando una obligación legal impida la supresión inmediata, Janalytics lo informará y limitará el tratamiento al mínimo exigido.

37.4 Supresión a la terminación

A la terminación del contrato, Janalytics devolverá o suprimirá los datos personales tratados por cuenta del cliente, según la instrucción de este, conforme al artículo 25 del Decreto 1377 de 2013 y a la sección 20.5.

38. Seguridad de proveedores y subencargados

38.1 Evaluación previa

Antes de contratar un proveedor que trate información de clientes, Janalytics evalúa su idoneidad: condiciones de seguridad, políticas de datos, ubicación del tratamiento, subcontratación y garantías de cumplimiento normativo. Un proveedor que no ofrezca condiciones de no entrenamiento o que no acredite medidas de seguridad razonables no es contratado para datos de clientes.

38.2 Obligaciones contractuales

Janalytics exige a cada subencargado, mediante contrato: tratar los datos solo según sus instrucciones; aplicar medidas de seguridad adecuadas; guardar confidencialidad; no usar los datos para entrenar modelos; asistir en la atención de incidentes y de solicitudes de titulares; y suprimir o devolver la información al terminar. Estas obligaciones replican las que Janalytics asume frente a sus clientes.

38.3 Seguimiento

Janalytics revisa periódicamente el desempeño de sus proveedores críticos y se mantiene informado de los cambios en sus políticas de datos, de sus incidentes relevantes y de sus certificaciones. Cuando un cambio afecta el servicio, se informa al cliente.

38.4 Transparencia sobre proveedores

Janalytics informa al cliente, a solicitud, la categoría y la identidad de los subencargados que tratan sus datos, y notifica cambios relevantes con antelación razonable para que el cliente pueda ejercer su derecho de objeción fundada.

39. Gestión de incidentes de seguridad y notificación

39.1 Definición y clasificación

Un incidente de seguridad es todo evento que comprometa o pueda comprometer la confidencialidad, integridad o disponibilidad de la información. Los incidentes se clasifican por severidad según su impacto sobre los datos, sobre la continuidad del servicio y sobre los derechos

de los titulares.

39.2 Ciclo de respuesta

Janalytics sigue un ciclo de respuesta que comprende: detección; contención; erradicación de la causa; recuperación del servicio; y análisis posterior. Cada incidente relevante produce un registro con su causa, su alcance y las medidas adoptadas, que alimenta la mejora continua.

39.3 Notificación al cliente

Cuando un incidente afecte datos del cliente, Janalytics se lo notificará sin dilación indebida y a más tardar dentro de las 48 horas siguientes a su detección confirmada, con la información disponible: naturaleza del incidente, datos potencialmente afectados, medidas adoptadas y recomendaciones. La notificación se actualizará a medida que avance la investigación.

39.4 Colaboración con el responsable

Como el cliente es el responsable del tratamiento, la notificación a los titulares y a la Superintendencia de Industria y Comercio corresponde al cliente. Janalytics prestará la información y el apoyo técnico necesarios para que el cliente cumpla esa obligación dentro de los plazos legales, y coordinará la comunicación cuando corresponda.

39.5 Medidas tras el incidente

Tras un incidente, Janalytics documenta las lecciones aprendidas e implementa acciones correctivas verificables. Cuando el incidente revela una vulnerabilidad sistémica, se informa a los clientes afectados y se ajusta la arquitectura o los procesos.

40. Continuidad del negocio y recuperación

40.1 Objetivo

Janalytics mantiene planes para prevenir, responder y recuperarse de interrupciones que afecten la prestación del servicio, buscando proteger la información y mantener la operación en niveles aceptables. La referencia de la Ley 2108 de 2021 sobre el carácter esencial de la conectividad refuerza la importancia de estos planes.

40.2 Copias de seguridad

Janalytics realiza copias de seguridad periódicas de la configuración, los metadatos y la información necesaria para operar, con verificación de su restauración. Las copias se almacenan con cifrado y con acceso restringido, y se someten a los mismos principios de retención mínima.

40.3 Objetivos de recuperación

Janalytics define objetivos de tiempo de recuperación y de punto de recuperación para los componentes críticos. Estos objetivos se revisan periódicamente y se informan al cliente que los solicite, dentro de los límites de la seguridad de la información.

40.4 Pruebas

Los planes de continuidad y de recuperación se prueban de forma periódica. El resultado de las pruebas se documenta y se usa para mejorar los procedimientos.

40.5 Dependencia de terceros

Janalytics reconoce su dependencia de proveedores de infraestructura y de modelos. Para reducir el riesgo, diseña componentes portables, evalúa alternativas y mantiene procedimientos de migración que reduzcan el impacto de una falla prolongada de un proveedor.

41. Auditoría, monitoreo y registros

41.1 Monitoreo

Janalytics monitorea la disponibilidad del servicio, los eventos de seguridad y el desempeño de los agentes. El monitoreo busca detectar anomalías, errores y posibles incidentes antes de que escalen.

41.2 Registros

Janalytics mantiene registros de: autenticación y accesos; cambios de configuración; ejecución de tareas y sus resultados (sin el contenido de los datos); incidentes y respuestas; y operación de los subencargados relevantes. Los registros se protegen contra alteración y se conservan por el plazo definido en la política de retención.

41.3 Retención de registros

Los registros de seguridad se conservan por un plazo alineado con las necesidades de auditoría y de cumplimiento, con rotación automática y sin incluir el contenido de los datos personales del cliente. Janalytics no conserva los registros más allá de lo necesario.

41.4 Auditoría interna

Janalytics realiza auditorías internas periódicas de su sistema de gestión de seguridad, con el fin de verificar la eficacia de los controles y detectar oportunidades de mejora. Los hallazgos se registran y se gestionan con acciones correctivas.

41.5 Registro de tratamiento de datos

Janalytics mantiene un registro de las actividades de tratamiento que realiza por cuenta de sus clientes, con la descripción de las operaciones, las finalidades y las medidas de seguridad, en respuesta al deber de responsabilidad demostrada del artículo 26 del Decreto 1377 de 2013.

42. Gestión de riesgos y cumplimiento continuo

42.1 Enfoque de riesgos

Janalytics identifica, evalúa y trata los riesgos de seguridad de la información y de protección de datos de forma sistemática, conforme al requisito 6.1 de ISO/IEC 27001:2022. Los riesgos se evalúan según criterios de probabilidad e impacto, se documentan y se revisan periódicamente.

42.2 Tratamiento

Para cada riesgo se define una opción de tratamiento —mitigar, evitar, transferir o aceptar— y los controles correspondientes. La matriz de riesgos de la sección 12 es parte visible de este proceso.

42.3 Cumplimiento normativo

Janalytics identifica y mantiene actualizada la normatividad que le aplica, en especial la Ley 1581 de 2012 y sus decretos reglamentarios, las circulares de la SIC y las normas emergentes sobre

inteligencia artificial. Cuando una norma nueva exige ajustes, se actualiza la política y, si es necesario, se informa al cliente.

42.4 Mejora continua

El sistema de gestión se revisa al menos una vez al año por la dirección, con base en los resultados de monitoreo, auditoría, incidentes y retroalimentación de clientes. Las decisiones de mejora se documentan.

42.5 Declaración de aplicabilidad

Janalytics mantiene una declaración de aplicabilidad de los controles de ISO/IEC 27001:2022, que identifica los controles seleccionados y justifica las exclusiones. Se pone a disposición del cliente que la solicite, con el debido resguardo de la información sensible.

43. Auditorías y derechos de verificación del cliente

43.1 Derecho de información

El cliente tiene derecho a recibir información razonable y verificable sobre las medidas de seguridad aplicadas a sus datos. Janalytics atenderá las solicitudes de información dentro de un plazo razonable y con el nivel de detalle que no comprometa la seguridad del sistema ni la información de otros clientes.

43.2 Evidencia documental

Janalytics podrá entregar al cliente, cuando lo solicite y con acuerdo de confidencialidad: el resumen de su política de seguridad; la declaración de aplicabilidad de controles; la lista de subencargados; y los informes de auditoría interna en la parte que le concierne.

43.3 Auditorías del cliente

Cuando el contrato lo prevea o la ley lo exija, el cliente podrá realizar auditorías sobre las medidas de seguridad aplicadas a sus datos. Las auditorías se acuerdan previamente en alcance, fecha y metodología, se realizan sin afectar la operación ni la seguridad de otros clientes, y sus resultados se tratan como confidenciales. Cuando una auditoría directa no sea viable, Janalytics podrá aportar informes de terceros o evidencia equivalente.

43.4 Autoridades

Janalytics colabora con las autoridades competentes —en particular con la Superintendencia de Industria y Comercio— y con las autoridades judiciales, atendiendo sus requerimientos conforme a la ley y dando traslado al cliente cuando corresponda.

44. Formación y cultura de seguridad

44.1 Concienciación

Janalytics forma a su equipo en seguridad de la información y en protección de datos. La formación cubre los principios de la Ley 1581 de 2012, el manejo de datos sensibles, la detección de phishing y la respuesta ante incidentes. Corresponde al control A.6.3 de ISO/IEC 27001:2022.

44.2 Compromiso del personal

El personal con acceso a información de clientes firma acuerdos de confidencialidad y de uso adecuado de la información. Las obligaciones subsisten después del cese de la relación.

44.3 Selección y salida

Janalytics verifica la idoneidad de las personas que se vinculan a funciones sensibles y aplica un procedimiento de salida que incluye la revocación de accesos y la devolución de activos.

44.4 Cultura de reporte

Janalytics promueve el reporte interno de fallas y de incidentes sin temor a represalias, porque la detección temprana es la mejor defensa. Todo miembro del equipo tiene el deber de reportar cualquier sospecha de incidente de seguridad.

Anexo A. Política de tratamiento de datos personales

A.1 Identificación del responsable

Esta política corresponde a Jassen Aldair Camargo Caicedo, persona natural comerciante titular del establecimiento de comercio identificado con el nombre comercial Janalytics, con NIT 1005180164, domicilio en Santander, Barrancabermeja, Dg 56 N 43-30, teléfono 315 444 9545 y correo electrónico administracion@janalytics.com.co. En adelante, Janalytics. La política cumple el contenido mínimo del artículo 13 del Decreto 1377 de 2013.

A.2 Ámbito de aplicación

Esta política aplica a las bases de datos y a los tratamientos de datos personales que Janalytics realiza directamente como responsable, en particular los datos de sus clientes, proveedores, contactos comerciales y personal. Respecto de los datos que Janalytics trata por cuenta de sus clientes, opera como encargado y aplica la política de tratamiento del cliente responsable, con las garantías contractuales del Anexo C.

A.3 Finalidades del tratamiento

Janalytics trata datos personales para las siguientes finalidades: gestionar la relación contractual con clientes y proveedores; prestar los servicios contratados; facturar y gestionar el cobro; atender consultas, peticiones y reclamos; cumplir obligaciones legales, contables y tributarias; gestionar la seguridad de la información; y, con autorización previa, enviar comunicaciones comerciales e información sobre servicios.

A.4 Derechos del titular

El titular tiene derecho a: conocer, actualizar, rectificar y suprimir sus datos; revocar la autorización cuando sea procedente; solicitar prueba de la autorización; presentar quejas ante la Superintendencia de Industria y Comercio; y acceder de forma gratuita a sus datos al menos una vez cada mes calendario y cada vez que existan modificaciones sustanciales de la política.

A.5 Persona responsable de la atención de solicitudes

La persona o área responsable de atender las peticiones, consultas y reclamos es Jassen Aldair Camargo Caicedo, a quien el titular puede dirigirse por correo electrónico a administracion@janalytics.com.co o por los canales indicados en el sitio web.

A.6 Procedimiento para ejercer los derechos

El titular puede presentar consultas y reclamos por los canales habilitados. Las consultas se atenderán en los términos legales y los reclamos se tramitarán conforme al procedimiento del artículo 15 de la Ley 1581 de 2012. Toda solicitud debe permitir acreditar la identidad del titular o de su representante. Janalytics conservará registro de las solicitudes atendidas.

A.7 Seguridad

Janalytics aplica las medidas técnicas, humanas y administrativas descritas en la Parte V de este documento, orientadas a proteger la confidencialidad, integridad y disponibilidad de la información y a evitar accesos no autorizados.

A.8 Vigencia

Esta política entra en vigencia en 23 de septiembre de 2026 y las bases de datos asociadas tendrán el periodo de vigencia que corresponda a sus finalidades, salvo norma legal en contrario. Cualquier cambio sustancial se comunicará oportunamente a los titulares antes de implementarse.

Anexo B. Aviso de privacidad

El siguiente es el contenido mínimo del aviso de privacidad que Janalytics pone a disposición de los titulares cuando no sea posible dar a conocer la política completa en el momento de la recolección, conforme al artículo 15 del Decreto 1377 de 2013.

- **Responsable**: Jassen Aldair Camargo Caicedo (persona natural comerciante, nombre comercial Janalytics), NIT 1005180164, domicilio Santander, Barrancabermeja, Dg 56 N 43-30, correo administracion@janalytics.com.co, teléfono 315 444 9545.
- **Tratamiento y finalidad**: los datos se usarán para gestionar la relación, prestar los servicios, facturar, atender solicitudes y cumplir obligaciones legales. Cuando aplique, para comunicaciones comerciales con autorización.
- **Derechos del titular**: conocer, actualizar, rectificar y suprimir sus datos, y revocar la autorización.
- **Acceso a la política**: la política de tratamiento completa está disponible en el sitio web https://www.janalytics.com.co y puede solicitarse por correo a administracion@janalytics.com.co.
- **Datos sensibles**: cuando se soliciten datos sensibles, el titular no está obligado a autorizar su tratamiento y se le informará expresamente cuáles datos tienen ese carácter y con qué finalidad se tratan.

Anexo C. Contrato de transmisión de datos personales

El contrato de transmisión cumple la función del artículo 25 del Decreto 1377 de 2013 y da base jurídica a la comunicación de datos entre responsable y encargado, incluida la transmisión internacional del artículo 24. Las cláusulas siguientes son el contenido esencial que Janalytics incorpora en sus contratos con clientes.

C.1 Partes y roles

El cliente actúa como responsable del tratamiento y Janalytics como encargado. El cliente decide sobre las bases de datos, las finalidades y las instrucciones; Janalytics ejecuta el tratamiento por cuenta y riesgo del cliente.

C.2 Alcance del tratamiento

Se describen: las categorías de datos tratados; las categorías de titulares; las finalidades específicas por tarea; la duración del tratamiento; y la naturaleza de las operaciones. Janalytics no tratará los datos para una finalidad distinta de la descrita.

C.3 Obligaciones de Janalytics

1. Tratar los datos personales conforme a los principios de la Ley 1581 de 2012 y a las instrucciones del cliente.
2. Salvaguardar la seguridad de las bases de datos en las que se contengan datos personales.
3. Guardar confidencialidad respecto del tratamiento de los datos personales.
4. No usar los datos para entrenar, afinar o mejorar modelos de inteligencia artificial.
5. No transferir ni transmitir los datos a terceros fuera de los subencargados autorizados, sin base jurídica o instrucción del cliente.
6. Aplicar las medidas de seguridad descritas en la Parte V y notificar los incidentes.
7. Asistir al cliente en la atención de los derechos de los titulares y en el cumplimiento de sus obligaciones legales.
8. Suprimir o devolver los datos al terminar la relación, según la instrucción del cliente.
9. Acreditar, cuando se le requiera, las condiciones del tratamiento.

C.4 Subencargados y transmisión internacional

Janalytics informa la categoría de subencargados y exige a cada uno obligaciones equivalentes. Cuando la transmisión implique a un proveedor ubicado en el exterior, Janalytics verificará el nivel adecuado de protección en los términos de la SIC o la existencia de una causal de excepción, conforme a las secciones 6.8 y 26.4. Las transmisiones internacionales entre responsable y encargado no requieren información adicional al titular ni su consentimiento cuando existe este contrato, según el artículo 24 del Decreto 1377 de 2013.

C.5 Responsabilidad

El cliente responde por la legalidad de los datos y por la existencia de la autorización de los titulares. Janalytics responde por el cumplimiento de las obligaciones que asume como encargado. Frente a terceros y frente a los titulares, la responsabilidad se distribuye según los artículos de la Ley 1581 de 2012.

C.6 Duración

El contrato dura mientras Janalytics trate datos personales del cliente. A su terminación, Janalytics devolverá o suprimirá los datos según la instrucción del cliente, salvo obligación legal de conservarlos.

Anexo D. Correspondencia con los controles de ISO/IEC 27001:2022

La tabla relaciona los dominios del Anexo A de ISO/IEC 27001:2022 con las secciones de este documento que los desarrollan. Los 93 controles se agrupan en cuatro categorías; la selección efectiva se documenta en la declaración de aplicabilidad.

Categoría	Controles (rango)	Secciones de este documento
Organizacionales	A.5.1 a A.5.37	33, 34, 35.4, 38, 39, 40, 42, 43
De personas	A.6.1 a A.6.8	35, 44
Físicos	A.7.1 a A.7.14	34, 40
Tecnológicos	A.8.1 a A.8.34	35, 36, 37, 39, 41

Anexo E. Referencias

E.1 Normatividad colombiana

Congreso de Colombia. (1999). Ley 527 de 1999, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276

Congreso de Colombia. (2008). Ley 1266 de 2008, por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales financieras, crediticias y comerciales. Disponible en el Gestor Normativo del Estado colombiano.

Congreso de Colombia. (2009). Ley 1273 de 2009, por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado denominado de la protección de la información y de los datos. Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Congreso de Colombia. (2011). Ley 1480 de 2011, por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones. Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=44306

Congreso de Colombia. (2012). Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales. Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso de Colombia. (2021). Ley 2108 de 2021, por medio de la cual se modifica la Ley 142 de 1994 y se reconoce el acceso a internet como servicio público esencial y universal. Gestor Normativo del Estado colombiano.

Corte Constitucional de Colombia. (2011). Sentencia C-748 de 2011 (control de constitucionalidad de la Ley Estatutaria 1581 de 2012). https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=50042

Presidencia de la República de Colombia. (2013). Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012. Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Presidencia de la República de Colombia. (2015). Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=76608

E.2 Circulares de la Superintendencia de Industria y Comercio

Superintendencia de Industria y Comercio. (2017). Circular Externa 005 de 2017, que adiciona un capítulo a la Circular Única sobre transferencia internacional de datos personales. Compilación Jurídica de la DIAN. https://normograma.dian.gov.co/dian/compilacion/docs/circular_superindustria_0005_2017.htm

Superintendencia de Industria y Comercio. (2024). Circular Externa 002 de 2024, Lineamientos sobre el tratamiento de datos personales en sistemas de inteligencia artificial. Cancillería de Colombia. https://www.cancilleria.gov.co/normograma/compilacion/docs/circular_superindustria_0002_2024.htm

Superintendencia de Industria y Comercio. (2024). Circular Externa 003 de 2024, Instrucciones para los administradores societarios. Alcaldía de Bogotá. https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=163877

Superintendencia de Industria y Comercio. (2025). Alcance de la Circular 002 de 2025 sobre transferencias internacionales de datos. Sede Electrónica SIC. https://sedeelectronica.sic.gov.co/publicaciones/boletin-juridico/concepto/alcance-de-la-circular-002-de-2025-sobre-transferencias-internacionales-de-datos

E.3 Política pública y regulación emergente

Departamento Nacional de Planeación. (2025). Documento CONPES 4144: Política Nacional de Inteligencia Artificial. DNP. https://www.dnp.gov.co/publicaciones/Planeacion/Paginas/conpes-4144-hoja-de-ruta-colombia-inteligencia-artificial-retos-actuales-transformacion-futura.aspx

Congreso de la República de Colombia. (2025). Proyecto de Ley número 043 de 2025 Senado, 324 de 2025 Cámara, por medio del cual se regula la inteligencia artificial en Colombia. Cámara de Representantes. https://www.camara.gov.co/wp-content/uploads/2025/12/proyectos-ley/publicaciones/proyecto-35981/PPDSC-PL-043-25S-324-25C-INTELIGENCIA-ARTIFICIAL-SC.pdf

Ministerio de Ciencia, Tecnología e Innovación. (2025). Minciencias lidera el proyecto de ley que busca regular el desarrollo ético, seguro y responsable de la inteligencia artificial en Colombia. https://minciencias.gov.co/sala_de_prensa/minciencias-lidera-el-proyecto-ley-que-busca-regular-el-desarrollo-etico-seguro-y

E.4 Estándares internacionales

International Organization for Standardization. (2022). ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO. https://www.iso.org/standard/54534.html

International Organization for Standardization. (2023). ISO/IEC 42001:2023, Information technology — Artificial intelligence — Management system. ISO. https://www.iso.org/standard/42001

National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST. https://www.nist.gov/itl/ai-risk-management-framework

E.5 Políticas de datos de proveedores de modelos

Estas referencias documentan las políticas de datos de los proveedores considerados. Las condiciones no son equivalentes: no todos ofrecen las mismas garantías de retención y de no entrenamiento, y Janalytics solo los emplea para datos de clientes cuando la garantía correspondiente está acreditada. Ver las secciones 4 y 5.

OpenAI. (2025). Offering zero data retention for frontier models. https://openai.com/index/offering-zero-data-retention-for-frontier-models/

Anthropic. (2025). API and data retention. Claude Platform Docs. https://platform.claude.com/docs/en/manage-claude/api-and-data-retention

DeepSeek. (s. f.). DeepSeek Privacy Policy. https://cdn.deepseek.com/policies/en-US/deepseek-privacy-policy.html

DeepSeek. (s. f.). DeepSeek Open Platform Terms of Service. https://cdn.deepseek.com/policies/en-US/deepseek-open-platform-terms-of-service.html

Alibaba Cloud. (s. f.). Security certifications and privacy notice — Model Studio. https://www.alibabacloud.com/help/en/model-studio/privacy-notice

Alibaba. (s. f.). Qwen Privacy Policy. https://qwen.ai/privacypolicy

Anexo F. Historial de versiones

Versión	Fecha	Cambios
1.0	23 de septiembre de 2026	Emisión inicial. Incluye profundización de los cuatro pilares, panorama regulatorio colombiano e internacional, términos y condiciones del servicio y política de seguridad de la información.

La versión vigente de este documento se publica en https://www.janalytics.com.co. Los cambios sustanciales se comunican a los clientes con antelación razonable, conforme a la sección 29.