

		MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
KBT-SIG-MA01-PO02	Versión 1.0	Fecha: 09/09/2026	Página 1 de 10

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES¹

1. Objetivo

Establecer los lineamientos corporativos, legales, técnicos, administrativos y operativos para proteger los datos personales tratados por KBT S.A.S. en el desarrollo de sus actividades de consultoría especializada, interventorías integrales, gerencia de proyectos, servicios TIC, marketing digital y gestión administrativa interna.

La presente política tiene como finalidad garantizar que la recolección, almacenamiento, uso, circulación, transferencia, transmisión, consulta, actualización, supresión, conservación y disposición de datos personales se realice de forma lícita, segura, autorizada, transparente, proporcional y trazable, preservando los derechos de los titulares y cumpliendo los requisitos legales, contractuales y de seguridad de la información aplicables.

2. Alcance

Esta política aplica a todos los datos personales tratados por KBT S.A.S. en calidad de responsable, encargado, custodio, usuario autorizado o tercero que intervenga en el tratamiento de información personal.

Aplica a:

- Trabajadores.
- Contratistas.
- Proveedores.
- Representantes legales.
- Clientes.
- Contactos comerciales.
- Aliados estratégicos.
- Usuarios finales de proyectos.
- Visitantes.
- Candidatos a procesos de selección.
- Terceros relacionados con proyectos.

¹ Esta política es un extracto fiel realizado del documento KBT-SIG-MA01-PO02 MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN, el cual la contiene.

		MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
KBT-SIG-MA01-PO02	Versión 1.0	Fecha: 09/09/2026	Página 2 de 10

- Entidades públicas o privadas con las que la compañía tenga relación contractual, comercial, técnica, administrativa o legal.

El alcance se integra con el Sistema Integrado de Gestión de KBT S.A.S., que cubre los procesos estratégicos, misionales y de apoyo, incluyendo Gestión Estratégica, Gestión Comercial, Gestión Proyectos, Sistema Integrado de Gestión, Gestión TI, Gestión Financiera, Gestión Talento Humano, Gestión Documental y Administrativa, y Gestión Compras y Proveedores.

3. Lineamientos de la política

Principios generales de protección de datos personales

KBT S.A.S. adopta los siguientes principios para el tratamiento de datos personales:

1. Legalidad: todo tratamiento de datos personales deberá ajustarse a la legislación colombiana aplicable, contratos, autorizaciones y políticas internas.
2. Finalidad: los datos personales solo se tratarán para finalidades legítimas, informadas, autorizadas o legalmente permitidas.
3. Libertad: el tratamiento deberá contar con autorización del titular, salvo las excepciones legales aplicables.
4. Veracidad o calidad: los datos personales deberán ser exactos, completos, actualizados, comprobables y comprensibles.
5. Transparencia: el titular podrá conocer la existencia del tratamiento y ejercer sus derechos.
6. Acceso y circulación restringida: los datos personales solo podrán ser consultados, utilizados o compartidos por personas autorizadas.
7. Seguridad: los datos personales deberán protegerse contra pérdida, adulteración, acceso no autorizado, uso indebido, fuga, destrucción o consulta no autorizada.
8. Confidencialidad: todas las personas que intervengan en el tratamiento deberán mantener reserva sobre los datos personales.
9. Necesidad y minimización: solo se tratarán los datos estrictamente necesarios para la finalidad autorizada.
10. Responsabilidad demostrada: Se debe conservar evidencia de cumplimiento, controles, autorizaciones, respuestas y decisiones asociadas al tratamiento.

		MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
KBT-SIG-MA01-PO02	Versión 1.0	Fecha: 09/09/2026	Página 3 de 10

Autorización para el tratamiento de datos personales

Se debe obtener autorización previa, expresa e informada de los titulares cuando el tratamiento lo requiera.

La autorización debe informar como mínimo:

- Identidad de KBT S.A.S. como responsable o encargado, según aplique.
- Finalidad del tratamiento.
- Datos que serán tratados.
- Derechos del titular.
- Canales de atención.
- Posibilidad de transferencia o transmisión de datos, cuando corresponda.
- Referencia a la política de tratamiento de datos personales.

Se exceptuarán de autorización los casos permitidos por la legislación aplicable, previa validación del Área Legal.

Finalidades del tratamiento

En la compañía solo se podrán tratar datos personales para finalidades legítimas, necesarias y documentadas, tales como:

PROCESO	FINALIDADES PERMITIDAS
Gestión Comercial	Contacto con clientes, elaboración de propuestas, seguimiento comercial, gestión de relaciones comerciales y comunicaciones autorizadas.
Gestión Proyectos	Ejecución contractual, coordinación de actividades, gestión de entregables, soporte, interventoría, gerencia de proyectos y trazabilidad.
Gestión Talento Humano	Vinculación, administración laboral, seguridad social, nómina, bienestar, formación, evaluación, cumplimiento legal y archivo laboral.
Gestión Financiera	Facturación, pagos, contabilidad, impuestos, conciliaciones, soportes financieros y cumplimiento de obligaciones legales.
Gestión Compras y Proveedores	Selección, contratación, evaluación, pagos, gestión contractual y comunicaciones con proveedores.

PROCESO	FINALIDADES PERMITIDAS
Gestión TI	Administración de usuarios, soporte, monitoreo, logs, seguridad, respaldo, continuidad y atención de incidentes.
Gestión Documental y Administrativa	Archivo, conservación, control documental, correspondencia, evidencias, actas, contratos y registros.
Sistema Integrado de Gestión	Auditorías, indicadores, mejora continua, gestión de riesgos, cumplimiento normativo y seguimiento del SIG.

Tratamiento de datos sensibles y datos de menores de edad

Se restringirá el tratamiento de datos sensibles y datos de menores de edad a los casos estrictamente necesarios, autorizados o legalmente permitidos.

Reglas mínimas:

- No se solicitarán datos sensibles salvo necesidad legal, contractual, laboral, de SST, seguridad, proyecto o cumplimiento.
- El titular debe ser informado de que no está obligado a autorizar el tratamiento de datos sensibles, salvo obligación legal aplicable.
- Los datos sensibles deben contar con acceso restringido.
- Los datos de salud, biométricos, familiares, laborales sensibles o asociados a SST deben protegerse con controles reforzados.
- Los datos de menores de edad solo se tratarán cuando sea necesario, proporcional, legalmente permitido y atendiendo el interés superior del menor.
- Los datos sensibles no deben usarse para finalidades incompatibles con la autorización o base legal.

Transferencia y transmisión de datos personales

Toda transferencia o transmisión de datos personales debe contar con reglas, procedimientos, acuerdos o cláusulas que protejan la información durante todo el ciclo de intercambio.

Se debe cumplir los siguientes lineamientos:

- Toda transferencia de datos personales debe tener finalidad legítima.
- Se debe verificar la identidad y autorización del destinatario.

- Se prohíbe enviar datos personales por canales no autorizados.
- Los datos personales confidenciales o restringidos deben transferirse por canales seguros.
- Se deben evitar envíos masivos sin control.
- Los datos deben minimizarse antes de transferirse.
- Cuando sea posible, se deben usar datos enmascarados, anonimizados, seudonimizados o parciales.
- La transferencia a proveedores o terceros debe estar respaldada por contrato, acuerdo de confidencialidad o cláusula de tratamiento de datos.
- La transferencia física de documentos debe realizarse mediante sobres sellados, registro de entrega y destinatario autorizado.
- La transferencia por medios removibles debe ser excepcional, autorizada, protegida y registrada.

Requisitos legales, estatutarios, reglamentarios y contractuales

Se deben identificar, documentar, mantener actualizados y cumplir los requisitos legales, regulatorios, contractuales y estatutarios aplicables al tratamiento de datos personales.

Como mínimo, el Área Legal y el SIG debe mantener una matriz que incluya:

- Ley 1581 de 2012 y normas reglamentarias aplicables.
- Derechos de los titulares.
- Deberes como responsable o encargado del tratamiento.
- Requisitos de autorización.
- Requisitos de aviso de privacidad.
- Requisitos para transferencia y transmisión de datos.
- Requisitos sobre datos sensibles y menores de edad.
- Requisitos de seguridad de la información.
- Obligaciones de conservación.
- Obligaciones contractuales con clientes.
- Obligaciones contractuales con proveedores.
- Requisitos asociados al RNBD, cuando apliquen.
- Criterios de atención de consultas y reclamos.
- Requisitos de reporte ante incidentes, cuando apliquen.
- Compromisos de confidencialidad.

		MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
KBT-SIG-MA01-PO02	Versión 1.0	Fecha: 09/09/2026	Página 6 de 10

Privacidad y protección de PII

Se debe proteger la información de identificación personal mediante controles administrativos, técnicos, físicos, contractuales y documentales.

Reglas mínimas:

1. Los accesos a PII deben otorgarse bajo necesidad de uso y mínimo privilegio.
2. Los datos personales no deben compartirse con usuarios no autorizados.
3. Los archivos con PII deben almacenarse en repositorios corporativos autorizados.
4. Los datos personales en correos, documentos, reportes, hojas de cálculo y archivos compartidos deben protegerse contra envío accidental o acceso no autorizado.
5. Los logs no deben almacenar contraseñas, tokens, llaves API, credenciales, datos personales completos o información financiera completa.
6. Los backups que contengan PII deben protegerse con controles de acceso, retención y eliminación segura.
7. Los datos personales en ambientes de desarrollo, pruebas, capacitación o demostración deben ser enmascarados, anonimizados o seudonimizados, salvo autorización formal.
8. Los datos personales no deben publicarse en la página web corporativa ni en redes sociales sin autorización y validación.

Derechos de los titulares

KBT S.A.S. debe habilitar canales para que los titulares puedan ejercer sus derechos de:

- Conocer sus datos personales.
- Actualizar sus datos.
- Rectificar información.
- Solicitar prueba de autorización.
- Ser informado sobre el uso dado a sus datos.
- Presentar consultas o reclamos.
- Solicitar supresión cuando proceda.

- Revocar autorización cuando proceda.

Las solicitudes deberán gestionarse conforme al procedimiento interno de atención de consultas y reclamos de titulares, con participación del Área Legal, Seguridad de la Información, Gestión Documental y el proceso propietario de la base de datos.

Reglas específicas por activo

ACTIVO	LINEAMIENTO DE PROTECCIÓN DE DATOS PERSONALES
Base de datos de clientes	Debe contar con finalidad definida, control de acceso por rol, trazabilidad, respaldo, autorización o base contractual, restricción de exportaciones y prohibición de uso para fines personales o no autorizados.
Correos electrónicos corporativos	Los correos con datos personales deberán enviarse solo a destinatarios autorizados; se debe validar dirección, evitar reenvío a cuentas personales y usar enlaces controlados cuando aplique.
Equipos portátiles	No deben almacenar bases de datos personales completas como repositorio principal; deben contar con bloqueo, credenciales, antivirus y cifrado cuando aplique.
Documentos contractuales	Deben proteger datos de representantes, trabajadores, proveedores, contratistas y terceros; el acceso debe limitarse a Legal, Gerencia, Gestión Proyectos y usuarios autorizados.
Información financiera	Los datos personales contenidos en soportes financieros, pagos, facturación, proveedores o empleados deben tratarse con acceso restringido y finalidad contable, contractual o legal.
Software financiero	Debe contar con perfiles de acceso, segregación de funciones, trazabilidad, respaldo y restricción de exportaciones con datos personales.
Backups corporativos	Los backups con datos personales deben protegerse contra acceso no autorizado, copia, restauración indebida o conservación excesiva.
Dispositivos móviles	No deben almacenar datos personales sensibles o bases completas; deben contar con bloqueo, autenticación y debe realizarse reporte inmediato por pérdida o robo.
Base de datos de empleados	Debe tener protección reforzada por contener datos laborales y personales; acceso limitado a Talento Humano, Gerencia y usuarios autorizados.
Servicios en la nube	Deben configurarse permisos, MFA, control de enlaces externos, retención, trazabilidad y restricción de acceso público a documentos con datos personales.
Archivos compartidos	Las carpetas con datos personales deben tener propietario, permisos mínimos, revisión periódica y prohibición de enlaces públicos.
Logs de sistemas	Deben contener solo datos técnicos necesarios; se prohíbe almacenar credenciales, tokens o datos personales completos.
Conocimiento del personal	La documentación de conocimiento no debe exponer datos personales innecesarios de trabajadores, clientes, proveedores o terceros.

		MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
KBT-SIG-MA01-PO02	Versión 1.0	Fecha: 09/09/2026	Página 8 de 10

Protección de datos personales en proyectos

En los proyectos de consultoría, interventoría, gerencia de proyectos, servicios TIC y marketing digital, se debe:

- Identificar si el proyecto involucra datos personales.
- Definir si la compañía actúa como responsable, encargado o custodio.
- Identificar bases de datos, fuentes y titulares.
- Definir finalidades del tratamiento.
- Establecer controles de acceso.
- Incluir cláusulas de protección de datos en contratos y acuerdos.
- Proteger datos recibidos de clientes o entidades públicas.
- Evitar uso de datos reales en pruebas o capacitaciones sin autorización.
- Definir reglas de transferencia y devolución de información.
- Eliminar, archivar o devolver datos al cierre del proyecto según contrato, ley o procedimiento.

Conservación y eliminación de datos personales

Se conservarán los datos personales durante el tiempo necesario para cumplir la finalidad autorizada, obligaciones legales, contractuales, contables, laborales, fiscales, auditorías, gestión de proyectos o defensa jurídica.

Reglas mínimas:

- No se conservarán datos personales indefinidamente sin justificación.
- La eliminación deberá ser segura y verificable.
- Los datos personales en backups se gestionarán conforme a la política de copias de seguridad.
- Los documentos físicos con datos personales deberán destruirse de forma segura cuando corresponda.
- Los datos personales asociados a proyectos cerrados deberán archivarse, devolverse o eliminarse según contrato y tabla de retención.
- Las solicitudes de supresión se atenderán siempre que no exista deber legal, contractual o legítimo de conservación.

		MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
KBT-SIG-MA01-PO02	Versión 1.0	Fecha: 09/09/2026	Página 9 de 10

Seguridad de datos personales en logs, respaldos y ambientes no productivos

1. Los logs deben limitarse a datos técnicos necesarios.
2. Los respaldos deben protegerse con controles de acceso y retención.
3. Los ambientes de prueba, capacitación o demostración deben usar datos anonimizados, enmascarados o ficticios.
4. La restauración de backups con datos personales debe ser autorizada.
5. Las evidencias de incidentes con datos personales deben protegerse y conservarse bajo custodia.
6. Los datos personales en archivos temporales deben eliminarse cuando ya no sean necesarios.

Incidentes relacionados con datos personales

Se considerarán incidentes de seguridad relacionados con datos personales, entre otros:

- Acceso no autorizado a bases de datos personales.
- Envío de datos personales a destinatario incorrecto.
- Pérdida o robo de equipo con datos personales.
- Publicación accidental de información personal.
- Fuga de datos por correo, nube, enlace público o repositorio compartido.
- Modificación no autorizada de datos personales.
- Eliminación no autorizada.
- Malware o ransomware que afecte información personal.
- Uso de datos personales para finalidades no autorizadas.
- Exposición de datos personales en logs o reportes.

Todo incidente deberá reportarse inmediatamente a Seguridad de la Información, Gestión TI, Legal y al propietario del activo, para su análisis, contención, investigación, comunicación y acciones correctivas.

Excepciones

		MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
KBT-SIG-MA01-PO02	Versión 1.0	Fecha: 09/09/2026	Página 10 de 10

Toda excepción a esta política deberá documentarse y aprobarse antes de realizar el tratamiento excepcional.

La excepción debe incluir:

- Descripción del tratamiento.
- Datos personales involucrados.
- Base legal o justificación.
- Finalidad.
- Titular o grupo de titulares.
- Activo afectado.
- Responsable interno.
- Riesgos identificados.
- Controles compensatorios.
- Periodo de vigencia.
- Aprobación del área legal.
- Aprobación del Encargado de seguridad de la información.
- Evidencia de cierre.

No se permiten excepciones permanentes sin revisión legal y análisis de riesgos.