DUE LEGAL

GUÍA PARA LA GESTIÓN

PROTECCIÓN DE DATOS PERSONALES

CON BASE EN LAS CIRCULARES 002 Y 003 DE 2024 DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO Y LA LEY 2300 DE 2023.

Due Legal

Este documento te ofrece una guía para garantizar que tu empresa cumpla con las normativas de protección de datos personales. Basada en la Ley 2300 de 2023 y las Circulares 002 y 003 de 2024, esta guía te ayudará a proteger la privacidad de tus clientes, evitar sanciones y adoptar buenas prácticas de manera efectiva. Descubre cómo implementar políticas robustas y tecnologías como la inteligencia artificial de forma ética y responsable.

¡Asegura un manejo transparente y seguro de los datos con nuestra ayuda!

GLOSARIO

2024

- **Dato Personal**: Cualquier información vinculada a una persona natural.
- **Responsable**: Entidad que decide sobre la base de datos y el tratamiento de la información.
- **Habeas Data**: Derecho a la privacidad, a conocer, actualizar y rectificar la información.
- **Autorización del Titular**: Consentimiento previo, expreso e informado del titular para tratar sus datos.
- **Corresponsabilidad**: Obligación de los administradores societarios de supervisar el cumplimiento normativo.
- **Accountability**: Responsabilidad de demostrar el cumplimiento de las normativas.
- **Registro de Números Excluidos (RNE)**: Registro para evitar comunicaciones comerciales no deseadas.
- **Oficial de Protección de Datos (OPD)**: Encargado de supervisar el cumplimiento de normas de protección de datos.
- **Evaluación de Impacto en la Privacidad (PIA)**: Identificación de riesgos y medidas de mitigación antes del tratamiento de datos.
- **Privacidad desde el Diseño (Privacy by Design)**: Incorporar protección de datos desde el inicio de un proceso.
- **Sistema de Gestión de Seguridad de la Información (SGSI)**: Políticas y controles para gestionar la seguridad de la información bajo normas como la ISO 27001.

LEYES BASE:

01 Ley 1581 de 2012

02 LEY 1266 DE 2008

03 LEY 2300 DE 2023

04 CIRCULAR 002 DE 2023

05 CIRCULAR 003 DE 2024

01 LEY 1581 DE 2012

La **Ley 1581 de 2012**, conocida como la **Ley de Protección de Datos Personales** en Colombia, establece el marco legal para garantizar el derecho fundamental a la **protección de datos personales**. Su objetivo es regular el tratamiento de la información personal de los ciudadanos, independientemente del sector económico, garantizando que su recolección, almacenamiento, uso y circulación respeten los principios de **legalidad, libertad, transparencia, seguridad** y **confidencialidad**.

02 LEY 1266 DE 2008

La **Ley 1266 de 2008**, también conocida como la **Ley de Habeas Data** en Colombia, establece el marco legal para la **protección de la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países**. Su objetivo principal es regular el manejo de los datos personales relacionados con el historial crediticio de los ciudadanos, estableciendo las condiciones bajo las cuales las entidades pueden recolectar, procesar y divulgar esta información.

03 LEY 2300 DE 2023

La **Ley 2300 de 2023** tiene como principal objetivo **proteger el derecho a la intimidad de los consumidores** frente a comunicaciones comerciales no solicitadas. Esta ley establece el **Registro de Números Excluidos (RNE)**, una herramienta en la que los usuarios pueden inscribir sus números de teléfono para evitar recibir mensajes publicitarios o llamadas comerciales. El RNE es administrado por la **Comisión de Regulación de Comunicaciones (CRC)** y es de carácter gratuito para los usuarios.

¿Quiénes están obligados a cumplir con esta ley?

- Todas las entidades financieras que realizan **actividades de cobranza** de manera directa o a través de terceros están sujetas a cumplir con las disposiciones de la ley. Estas incluyen bancos, compañías de seguros, cooperativas de crédito, y otras entidades del sector financiero.
- Personas naturales o jurídicas que realicen actividades de cobro de deudas por cuenta propia o a través de terceros.
- Personas naturales o jurídicas que realicen **publicidad o actividades comerciales** a través de medios como llamadas telefónicas, mensajes de texto (SMS), correos electrónicos y aplicaciones de mensajería.
- Las empresas de **telecomunicaciones**, que suelen realizar promociones o ventas de productos a través de llamadas telefónicas o mensajes de texto.

Tipos de comunicaciones sobre las que recae la Ley 2300

La Ley 2300 prohíbe cualquier tipo de **comunicación comercial o publicitaria** dirigida a los usuarios que hayan inscrito sus números en el RNE. Esto incluye:

- Ofertas de productos o servicios.
- Promociones comerciales.
- Invitaciones a eventos comerciales.

Excepciones: Comunicaciones permitidas aún estando inscrito en el RNE

Aunque un número esté registrado en el RNE, **no todas las comunicaciones están prohibidas**. Existen ciertas excepciones en las que las empresas pueden seguir enviando mensajes, que incluyen:

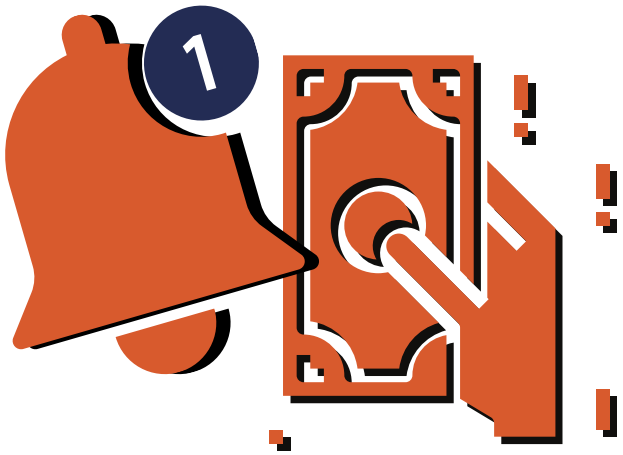
- **Comunicaciones relacionadas con la prestación de servicios contratados**:
  - Mensajes sobre el **estado de cuentas**, vencimientos de facturas o fechas de pago.
  - Notificaciones de **cortes de servicio** o cambios en las condiciones de los servicios contratados.
- **Comunicaciones solicitadas previamente por el usuario**: cualquier tipo de comunicación que haya sido solicitada de manera expresa por el usuario antes de registrarse en el RNE.
- **Mensajes no comerciales**: mensajes informativos que no tengan fines comerciales, como avisos de emergencia o información relevante sobre servicios públicos.
- De igual forma, se excluye en los casos en los que, a pesar de que el usuario esté registrado en el RNE, se conceda a la empresa **una autorización expresa** para el envío de información publicitaria.

Actividades de cobranza

La Ley 2300 de 2023 establece normas claras para proteger la privacidad de los consumidores durante el proceso de cobro de obligaciones financieras:

- **Canales Autorizados**: Contactar únicamente a través de los canales previamente autorizados por el consumidor.
- **Frecuencia y Horarios**:
  - Solo se puede contactar una vez al día y no por varios canales durante la misma semana.
  - Horarios permitidos: lunes a viernes (7 a.m. - 7 p.m.) y sábados (8 a.m. - 3 p.m.). No se permite el contacto los domingos ni festivos.
- **Protección de la Privacidad**: Respetar la intimidad del consumidor evitando el contacto excesivo o intrusivo.

Exclusión de contactos comerciales: aunque el **Registro de Números Excluidos (RNE)** protege al consumidor de recibir publicidad no deseada, **las gestiones de cobranza no se ven afectadas** por esta prohibición. Las comunicaciones relacionadas con el cobro de deudas pueden continuar, siempre que se respeten los **canales autorizados**, **horarios** y **frecuencia** mencionados.



Medios en los que los usuarios pueden pedir exclusión de comunicaciones

- **Llamadas telefónicas** (tanto fijas como móviles).
- **Mensajes de texto** (SMS).
- Mensajes enviados a través de aplicaciones web (como **WhatsApp o similares**).
- **Correos electrónicos**.

Consulta del registro de números excluidos

Las empresas deben acceder a la **plataforma oficial de la Comisión de Regulación de Comunicaciones (CRC)** a través del siguiente enlace: http://www.tramitescrcom.gov.co.

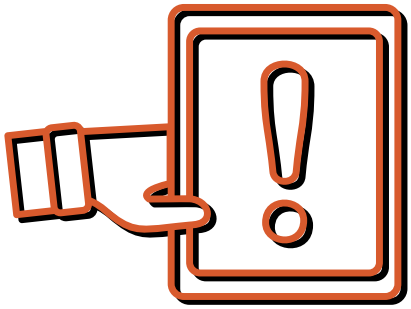
En el sitio web, deberán seleccionar la opción correspondiente al **Registro de Números Excluidos (RNE)**. Este proceso les permitirá verificar si los números de teléfono de sus clientes están inscritos en el registro.

Frecuencia de actualización de la información

El **RNE se actualiza diariamente**, entonces, dado que los usuarios pueden registrarse o eliminar su número en cualquier momento, es importante revisar el RNE antes de cada campaña de comunicación o marketing.

Sanciones por incumplimiento

El incumplimiento de las obligaciones establecidas en la Ley 2300 puede derivar en sanciones impuestas por la Superintendencia de Industria y Comercio o por la Superintendencia Financiera, como multas de hasta 2.000 salarios mínimos mensuales legales vigentes.

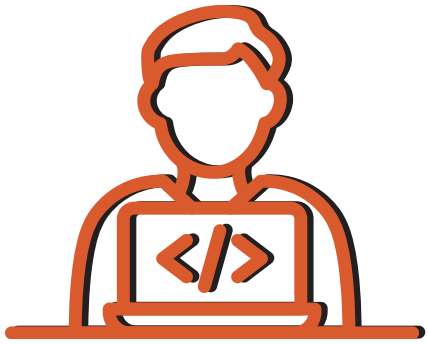


04 CIRCULAR 002 DE 2023

La **Circular 002 de 2024** emitida por la **Superintendencia de Industria y Comercio** establece lineamientos para el tratamiento de datos personales en sistemas de **Inteligencia Artificial (IA)**.

¿Quiénes están obligados a cumplir con esta ley?

- **Responsables y Encargados del Tratamiento de Datos Personales**: Incluye tanto entidades públicas como privadas que desarrollen, desplieguen o utilicen sistemas de IA que involucren el tratamiento de datos personales.
- **Desarrolladores de IA**: Empresas y personas que diseñen o entrenen sistemas de IA que procesen datos personales también están sujetas a esta normativa.



¿Qué deben tener en cuenta las empresas para su cumplimiento?

- **Cumplir con la regulación de datos personales:** el tratamiento de datos personales mediante IA debe respetar los principios establecidos en las **Leyes Estatutarias 1266 de 2008** y **1581 de 2012**.
- **Evaluación de impacto en la privacidad (PIA)**: antes de implementar un sistema de IA, las empresas deben realizar y documentar un **estudio de impacto de privacidad**. Este debe identificar los posibles riesgos que la IA puede tener sobre los derechos de los titulares de los datos personales y definir medidas para mitigarlos.
- **Privacidad desde el diseño y por defecto (Privacy by Design and by Default)**: los sistemas de IA deben ser diseñados para incorporar medidas de privacidad desde su implementación.
- **Aplicación de la responsabilidad demostrada ("Accountability")**: las empresas deben ser capaces de **demostrar** que han implementado medidas apropiadas para cumplir con las normativas de protección de datos personales al utilizar IA.
- **Adopción de medidas de seguridad:** es obligatorio implementar **medidas de seguridad técnicas y administrativas** para proteger los datos personales de accesos no autorizados, uso indebido o manipulación.
- **Información**: las empresas que utilicen IA deben garantizar que los titulares de los datos tengan el derecho a obtener una explicación clara sobre cómo el sistema toma decisiones que los afectan.

05 CIRCULAR 003 DE 2024

La Circular 003 de 2024 establece obligaciones para los administradores de entidades vigiladas por la SIC, enfocándose en la corresponsabilidad y accountability para asegurar la protección óptima de los datos personales.

¿Qué deben tener en cuenta las empresas para su cumplimiento?

- **Corresponsabilidad**: Los administradores comparten la responsabilidad de cumplir las normas de protección de datos junto con la entidad.
- **Responsabilidad Demostrada (Accountability)**: Los administradores deben demostrar la implementación y auditoría de políticas para cumplir con las normativas de protección de datos.
- **Políticas Internas Efectivas**: Las empresas deben tener políticas claras y monitoreadas para garantizar el tratamiento adecuado de datos personales.
- **Mecanismos de Cumplimiento**: Implementar mecanismos para garantizar el cumplimiento de las políticas, incluyendo la designación de un Oficial de Protección de Datos (OPD).
- **Evaluación de Impacto en la Privacidad (PIA)**: Realizar evaluaciones de riesgos antes de proyectos que involucren datos personales.
- **Medidas de Seguridad y Gestión de Riesgos**: Implementar medidas preventivas para proteger los datos y mejorar la seguridad, incluyendo la gestión de riesgos.

RECOMENDACIONES

En relación con la Ley 2300 de 2024:

- Implementar un sistema de consulta periódica del RNE: las empresas deben establecer un procedimiento regular para consultar el **Registro de Números Excluidos (RNE)**, disponible a través de la plataforma de la **CRC**. Esta consulta debe realizarse **antes de cada campaña publicitaria** para evitar sanciones por contactar a usuarios inscritos.
- Definir procesos claros de obtención de consentimiento, si bien la ley 2300 prohíbe las comunicaciones comerciales no deseadas, es posible seguir contactando a clientes que han dado su **consentimiento expreso** para recibir comunicaciones.
- Establecer un lineamiento en el que se identifiquen las excepciones del RNE, tales como como mensajes relacionados con la prestación de servicios contratados (facturación, cortes de servicio, etc.).
- Documentar todas las acciones relacionadas con el cumplimiento de la Ley 2300. Esto incluye registrar las consultas al RNE, las actualizaciones de bases de datos, y las políticas internas de comunicaciones comerciales.
- Implementar mecanismos de quejas y reclamos para los clientes. Esto puede incluir un canal digital donde los clientes puedan reportar si su número está inscrito en el RNE y, aun así, recibieron comunicaciones no solicitadas.
- Realizar procesos internos de monitoreo y seguimiento sobre la actualización de bases de datos, seguimiento de procedimientos y una adecuada gestión del consentimiento de los usuarios.

En relación con la Circular 003 de 2024

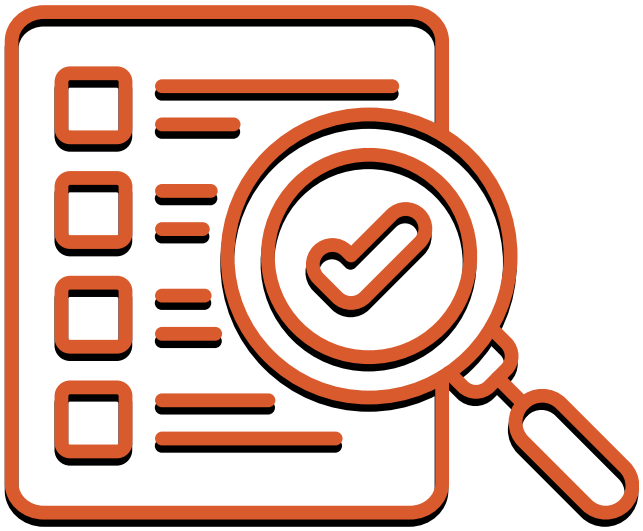
- Designar un área o persona responsable, como el Oficial de Protección de Datos Personales (OPD), si bien la normativa colombiana no establece de manera explícita la designación de un OPD, se recomienda altamente que las empresas nombren una persona o área encargada de supervisar el cumplimiento de las normas de protección de datos.
- Crear un sistema de programas, políticas y manuales para garantizar la protección y una adecuada gestión de los datos personales, los cuales se implementen desde la alta gerencia hasta las áreas operativas.
- Implementar una política de identificación y gestión de riesgos, de manera que se cuente con un sistema de monitoreo constante, planes de acción y de mejora, en caso de que exista un potencial riesgo o llegue a materializarse

- El uso de IA en el tratamiento de datos debe ser **ético, seguro y respetuoso de los derechos de los titulares** de datos personales. Para lograrlo se recomienda:
  - Informar claramente a los titulares de los datos cuando se utilicen sistemas de IA para su tratamiento. Es necesario explicar **cómo se recolectan y utilizan los datos**, y ofrecer a los titulares la posibilidad de **optar por no participar**.
  - Garantizar que las decisiones automatizadas por la IA sean explicables. Los titulares de datos deben tener derecho a conocer cómo la IA ha llegado a una determinada conclusión, especialmente en casos de decisiones que les afecten directamente.
- Antes de implementar sistemas de IA que involucren datos personales, es necesario realizar una **evaluación de impacto en la privacidad** (PIA) que incluya un adecuado proceso de identificación, evaluación y mitigación de riesgos.
- La **privacidad desde el diseño y por defecto** es un principio esencial al implementar IA, esto implica asegurar que los sistemas de IA protejan los datos personales desde el momento en que se diseñan y durante todo su ciclo de vida.
- Contar con procesos de **auditoría y mejora continua**: los sistemas deben ser auditados regularmente para garantizar que siguen respetando los principios de privacidad, y ser adaptados si cambian los riesgos o se materializan.

Recomendaciones generales para el tratamiento de datos personales

- **Aplicación del principio de responsabilidad demostrada:** las empresas deben cumplir y demostrar el cumplimiento de las normativas. Esto implica mantener registros detallados de cómo se diseña, implementa y gestiona el uso de IA, justificando su necesidad y las medidas de seguridad adoptadas. Además, es fundamental realizar auditorías periódicas, tanto internas como externas, revisadas por el Oficial de Protección de Datos (OPD).
- **Implementar programas de capacitación y sensibilización:** capacitar al personal sobre la normativa y la importancia de proteger los datos personales es esencial para asegurar el cumplimiento. La sensibilización ayuda a todos a comprender su papel en la protección de la información y garantiza procesos adecuados.
- **Políticas Internas de Tratamiento de Datos**: ser recomienda implementar políticas claras para la recolección, uso y eliminación de datos personales. Estas políticas deben incluir controles de seguridad robustos y un sistema efectivo de gestión de riesgos. Para garantizar su eficacia, es recomendable basarse en estándares internacionales, como la ISO 37301 (compliance), ISO 27001 (seguridad de la información), ISO 31000 (gestión de riesgos), e ISO 27701 (privacidad).

- Seguridad de la información: se recomienda implementar un Sistema de Gestión de Seguridad de la Información (SGSI), basado en estándares como ISO 27001. Este sistema protege la confidencialidad, integridad y disponibilidad de los datos, incluyendo políticas claras sobre manejo de información, controles de acceso, cifrado y gestión de incidentes.
- Para que la implementación de estos programas sea exitosa, es fundamental realizar auditorías periódicas para verificar la eficacia de los controles y actualizar las medidas según los cambios tecnológicos y nuevas amenazas. Capacitar al personal es clave para fomentar una cultura de protección de datos en toda la organización.



GUÍA PARA LA GESTIÓN

PROTECCIÓN DE DATOS PERSONALES

CON BASE EN LAS CIRCULARES 002 Y 003 DE 2024 DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO Y LA LEY 2300 DE 2023.

Due Legal