Política de protección y tratamiento de datos personales

Newrest Services Colombia S.A.S., NIT 890.929.877-1; Newrest Catering Colombia S.A.S., NIT 808.001.297-6, y Newrest Inflight Colombia S.A.S. ZF, NIT 900.960.881-5 en adelante **NEWREST,** tratan datos personales de trabajadores, candidatos, clientes, consumidores, proveedores, contratistas y visitantes en desarrollo de su operación de catering aéreo, alimentación institucional y servicios en sitios remotos. En ese tratamiento actúan como Responsables y, respecto de los trabajadores de sus clientes corporativos, como Encargadas.

NEWREST declara que el tratamiento de datos personales se sujeta a la Ley 1581 de 2012, a la Ley 1266 de 2008, al Decreto 1074 de 2015 y a las instrucciones de la Superintendencia de Industria y Comercio (SIC), y se rige por los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

En consecuencia, **NEWREST** se obliga a recolectar únicamente los datos pertinentes y adecuados a la finalidad informada al Titular; a obtener y conservar la autorización previa, expresa e informada cuando la ley la exija; a garantizar dentro de los términos legales el ejercicio de los derechos de conocer, actualizar, rectificar y suprimir los datos y de revocar la autorización; a adoptar las medidas técnicas, humanas y administrativas necesarias para preservar la seguridad y la confidencialidad de la información; a exigir de sus Encargados las mismas garantías mediante contrato de transmisión; y a reportar a la autoridad los incidentes que lo ameriten.

La Dirección Legal, en cabeza del Oficial de Cumplimiento, es el área responsable de la atención de peticiones, consultas y reclamos de los Titulares. Los canales dispuestos para el efecto son protecciondatos@newrest.eu | politica.datosco@newrest.eu.

El desarrollo de esta política consta en el documento MAN-ITC-101-CO, y su aplicación operativa en el manual MAN-ITC-100-CO y en los procedimientos, instructivos y formatos del sistema documental de protección de datos personales. Su cumplimiento es obligatorio para administradores, trabajadores, contratistas y terceros que traten datos personales por cuenta de **NEWREST;** su inobservancia da lugar a las medidas previstas en el Reglamento Interno de Trabajo y en los respectivos contratos, sin perjuicio de las responsabilidades legales.

Esta política rige a partir de su expedición y deja sin efecto la versión anterior.

Bogotá D.C
Septiembre 2026

Diana Ximena Solano Vargas
Representante Legal

TABLA DE CONTENIDO

0. DEFINICIONES 3
1. OBJETIVO 4
2. ALCANCE 4
3. CONTENIDO MÍNIMO LEGAL Y SU UBICACIÓN EN ESTE DOCUMENTO 4
4. IDENTIFICACIÓN DE LOS RESPONSABLES DEL TRATAMIENTO 4
5. ÁREA RESPONSABLE DE LA ATENCIÓN DE PETICIONES, CONSULTAS Y RECLAMOS 5
6. MARCO NORMATIVO Y ÁMBITO DE APLICACIÓN 5
6.1. Ámbito de aplicación 6
7. PRINCIPIOS RECTORES 6
7.1. Reglas de gestión que complementan los principios 7
8. DATOS QUE TRATA LA COMPAÑÍA Y BASES DE DATOS 8
9. FINALIDADES DEL TRATAMIENTO, POR GRUPO DE TITULARES 8
9.1. Trabajadores, extrabajadores, aprendices y candidatos 8
9.2. Clientes y clientes potenciales 9
9.3. Proveedores, contratistas y sus colaboradores 9
9.4. Visitantes y personas que ingresan a las instalaciones 10
9.5. Titulares vinculados a clientes corporativos (Tratamiento por cuenta del cliente) 10
9.6. Finalidades transversales a todos los grupos de Titulares 11
10. AUTORIZACIÓN DEL TITULAR 11
10.1. Casos en que no se requiere autorización 12
10.2. Cambio de finalidad y modificación de la política 12
11. CONSULTA DE LISTAS RESTRICTIVAS Y DEBIDA DILIGENCIA LA/FT/FPADM Y C/ST 12
11.1. Base de legitimación 12
11.2. Reglas de manejo 13
12. TRATAMIENTO DE DATOS SENSIBLES 13
12.1. Datos biométricos y control de acceso 13
12.2. Datos de salud 14
13. TRATAMIENTO DE DATOS DE NIÑAS, NIÑOS Y ADOLESCENTES 15
14. NEWREST COMO RESPONSABLE Y COMO ENCARGADA DEL TRATAMIENTO 15
14.1. Deberes de la Compañía como Responsable 16
14.2. Deberes de la Compañía como Encargada 17
14.3. Separación de las bases de datos 17
14.4. Relación con Encargados de la Compañía 17
15. TRANSFERENCIAS Y TRANSMISIONES DE DATOS PERSONALES 18
15.1. Transferencias nacionales e internacionales 18
15.2. Transmisiones y contrato de transmisión 19
16. DERECHOS DE LOS TITULARES 19
17. PROCEDIMIENTO PARA EL EJERCICIO DE LOS DERECHOS 20
17.1. Presentación de la solicitud 20
17.2. Consultas — artículo 14 de la Ley 1581 de 2012 20
17.3. Reclamos — artículo 15 de la Ley 1581 de 2012 20
17.4. Contenido de la respuesta 21
17.5. Revocatoria de la autorización y supresión del dato 21
17.6. Requisito de procedibilidad 22
18. MEDIDAS DE SEGURIDAD 22

19. REGISTRO NACIONAL DE BASES DE DATOS 23
20. INCIDENTES DE SEGURIDAD 24
21. AVISO DE PRIVACIDAD 24
22. VIGENCIA DE LA POLÍTICA Y PERÍODO DE VIGENCIA DE LAS BASES DE DATOS 25
22.1. Vigencia de la política 25
22.2. Período de vigencia de las bases de datos 25
23. GOBIERNO DEL PROGRAMA Y RESPONSABILIDAD DEMOSTRADA 27
24. MODIFICACIONES Y DIVULGACIÓN 27

0. DEFINICIONES

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (art. 3 lit. a, Ley 1581 de 2012).
Aviso de privacidad: Comunicación verbal o escrita dirigida al Titular, generada por el Responsable, para informarle sobre la existencia de las políticas de Tratamiento que le serán aplicables, la forma de acceder a ellas y las finalidades del Tratamiento (art. 2.2.2.25.1.3 del Decreto 1074 de 2015).
Base de datos: Conjunto organizado de datos personales que sea objeto de Tratamiento (art. 3 lit. b, Ley 1581 de 2012).
Dato personal: Conjunto organizado de datos personales que sea objeto de Tratamiento (art. 3 lit. b, Ley 1581 de 2012).
Dato sensible: Aquel que afecta la intimidad del Titular o cuyo uso indebido puede generar su discriminación: origen racial o étnico, orientación política, convicciones religiosas o filosóficas, pertenencia a sindicatos u organizaciones sociales o de derechos humanos, datos relativos a la salud, a la vida sexual y los datos biométricos (art. 5, Ley 1581 de 2012).
Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realiza el Tratamiento de datos personales por cuenta del Responsable del Tratamiento (art. 3 lit. d, Ley 1581 de 2012).
Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decide sobre la base de datos y/o el Tratamiento de los datos (art. 3 lit. e, Ley 1581 de 2012).
RNBD: Registro Nacional de Bases de Datos administrado por la Superintendencia de Industria y Comercio.
SIC: Superintendencia de Industria y Comercio, autoridad de protección de datos personales en Colombia.
Titular: Persona natural cuyos datos personales sean objeto de Tratamiento (art. 3 lit. f, Ley 1581 de 2012).
Transferencia: Envío de datos personales, por el Responsable o el Encargado ubicado en Colombia, a un receptor que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país (art. 2.2.2.25.1.3 del Decreto 1074 de 2015).
Transmisión: Comunicación de datos personales, dentro o fuera del territorio colombiano, que tiene por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable (art. 2.2.2.25.1.3 del Decreto 1074 de 2015).
Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión (art. 3 lit. g, Ley 1581 de 2012).

1. OBJETIVO

Establecer las condiciones bajo las cuales **Newrest Services Colombia S.A.S., Newrest Catering Colombia S.A.S. y Newrest Inflight Colombia S.A.S. ZF** realizan el Tratamiento de los datos personales de las personas naturales con quienes se relacionan; informar las finalidades de ese Tratamiento, los derechos que asisten a los Titulares y los procedimientos para ejercerlos; y dar cumplimiento a la Ley Estatutaria 1581 de 2012, al Capítulo 25 del Título 2 de la Parte 2 del Libro 2 del Decreto 1074 de 2015 y a las instrucciones de la Superintendencia de Industria y Comercio.

2. ALCANCE

Toda operación de recolección, almacenamiento, uso, circulación o supresión de datos personales (incluidas la transmisión y la transferencia, nacionales e internacionales) contenidos en bases de datos o archivos, físicos o digitales, que sean objeto de Tratamiento por las tres sociedades identificadas en el numeral 4, sea que actúen como Responsables o como Encargadas del Tratamiento. Vincula a los administradores, trabajadores, aprendices y contratistas de la Compañía, y a los terceros que traten datos personales por cuenta de ella en virtud de un contrato de transmisión.

3. CONTENIDO MÍNIMO LEGAL Y SU UBICACIÓN EN ESTE DOCUMENTO

El artículo 2.2.2.25.3.1 del Decreto 1074 de 2015 (que compiló el artículo 13 del Decreto 1377 de 2013) fija seis contenidos que toda política de Tratamiento debe incluir. La tabla siguiente indica dónde se satisface cada uno, de modo que su verificación pueda hacerse numeral por numeral.

Núm.	Contenido exigido por el art. 2.2.2.25.3.1	Sección de esta política
1	Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del Responsable	4
2	Tratamiento al cual serán sometidos los datos y finalidad del mismo	8 y 9
3	Derechos que le asisten al Titular	16
4	Persona o área responsable de la atención de peticiones, consultas y reclamos	5
5	Procedimiento para que los Titulares ejerzan sus derechos y revoquen la autorización	17
6	Fecha de entrada en vigencia de la política y período de vigencia de la base de datos	22

Esta política consta en medio electrónico y en medio físico, está redactada en lenguaje claro y sencillo y se pone en conocimiento de los Titulares por los canales señalados en la sección 24.

4. IDENTIFICACIÓN DE LOS RESPONSABLES DEL TRATAMIENTO

Las tres sociedades que se identifican a continuación (en adelante, conjunta o indistintamente, **NEWREST** o **la Compañía**) son personas jurídicas distintas y, en consecuencia, **cada una es Responsable del Tratamiento de sus propias bases de datos**, con obligaciones propias de registro, de atención de derechos y de reporte. Adoptan esta política de manera

común, sin que ello confunda ni traslade entre ellas la responsabilidad que a cada cual corresponde.

Dato	Newrest Services Colombia S.A.S.	Newrest Catering Colombia S.A.S.	Newrest Inflight Colombia S.A.S. ZF
NIT	890.929.877-1	808.001.297-6	900.960.881-5
Domicilio	Bogotá D.C., Colombia	Bogotá D.C., Colombia	Bogotá D.C., Colombia
Dirección	Torre REM, Carrera 14 # 99-33, pisos 6 y 7	Torre REM, Carrera 14 # 99-33, pisos 6 y 7	Carrera 106 # 15ª – 25 interior 10 manzana 4
Correo electrónico	protecciondatos@newrest.eu | politica.datosco@newrest.eu	protecciondatos@newrest.eu | politica.datosco@newrest.eu	protecciondatos@newrest.eu | politica.datosco@newrest.eu
Teléfono	(+57) 601 514 0088	(+57) 601 514 0088	(+57) 601 514 0088
Actividad	Catering industrial y de remotos, y servicios de alimentación en plantas de clientes corporativos	Catering industrial y de remotos, y servicios de alimentación en plantas de clientes corporativos	Catering aéreo en régimen de zona franca

NEWREST hace parte del grupo empresarial encabezado por **Newrest Group Holding S.A.**, con domicilio en Francia. Esta política desarrolla, para el ordenamiento colombiano, los compromisos de la Política de Protección de Datos Personales del grupo (PPDP, versión 2023) y se articula con la Política de Seguridad de los Sistemas de Información (P.S.S.I., versión 2024). Cuando el estándar del grupo y la ley colombiana difieran, **prevalece la ley colombiana**; cuando el estándar del grupo sea más exigente sin contrariarla, se aplica el del grupo

5. ÁREA RESPONSABLE DE LA ATENCIÓN DE PETICIONES, CONSULTAS Y RECLAMOS

En cumplimiento del artículo 2.2.2.25.4.4 del Decreto 1074 de 2015 (antes art. 23 del Decreto 1377 de 2013), la Compañía designa como área que asume la función de protección de datos personales a la **Dirección Legal**, en cabeza del **Oficial de Cumplimiento**. A ella corresponde dar trámite a las peticiones, consultas y reclamos de los Titulares, mantener actualizado el RNBD, conservar la evidencia del programa y servir de punto de contacto con la Superintendencia de Industria y Comercio.

Canal	Datos
Correo electrónico	protecciondatos@newrest.eu | politica.datosco@newrest.eu
Dirección física	Torre REM, Carrera 14 # 99-33, pisos 6 y 7, Bogotá D.C., Colombia — Atención: Oficial de Cumplimiento
Teléfono	(+57) 601 514 0088
Canales internos	Los trabajadores y extrabajadores pueden además dirigirse al proceso de Gestión Humana, y los proveedores al proceso de Compras. En ambos casos la solicitud se remite a la Dirección Legal dentro de los dos (2) días hábiles siguientes y los términos de respuesta son los de la sección 17.

6. MARCO NORMATIVO Y ÁMBITO DE APLICACIÓN

Esta política se sujeta, entre otras, a las siguientes normas:

- **Constitución Política, artículos 15 y 20** — habeas data, intimidad, buen nombre e información veraz e imparcial.

- **Ley Estatutaria 1581 de 2012** (17 de octubre de 2012) — régimen general de protección de datos personales.
- **Decreto 1074 de 2015** — Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, Libro 2, Parte 2, Título 2, **Capítulo 25** (que compiló el Decreto 1377 de 2013) y **Capítulo 26** (que compiló el Decreto 886 de 2014, sobre el RNBD), este último modificado por el Decreto 090 de 2018.
- **Ley Estatutaria 1266 de 2008**, modificada por la Ley 2157 de 2021 — habeas data financiero y crediticio, aplicable a los reportes de cartera y a la consulta de centrales de información.
- **Ley 1762 de 2015** y la Circular Básica Jurídica de la Superintendencia de Sociedades — deberes de prevención del lavado de activos, la financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva (LA/FT/FPADM).
- **Circular Única de la SIC, Título V**, y en particular las circulares externas 005 de 2017 (transferencias internacionales), 003 de 2018 (RNBD, reportes de reclamos e incidentes), 006 de 2022 (marketing), 002 de 2024 (inteligencia artificial) y 003 de 2024 (instrucciones a los administradores societarios).
- **Resolución 2346 de 2007** del entonces Ministerio de la Protección Social, modificada por la Resolución 1918 de 2009, y **Decreto 1072 de 2015** — evaluaciones médicas ocupacionales, custodia de la historia clínica ocupacional y conservación de documentos del Sistema de Gestión de Seguridad y Salud en el Trabajo.

6.1. Ámbito de aplicación

Esta política aplica a los datos personales registrados en cualquier base de datos, física o digital, que los haga susceptibles de Tratamiento por la Compañía, y al Tratamiento que realicen los terceros con quienes la Compañía suscriba contratos de transmisión. Aplica igualmente al Tratamiento que la Compañía realiza en calidad de Encargada por cuenta de sus clientes corporativos, en los términos de la sección 14.

Conforme al artículo 2 de la Ley 1581 de 2012, quedan fuera de su ámbito, sin perjuicio de los principios constitucionales y del deber de reserva, las bases de datos de ámbito exclusivamente personal o doméstico, las que tengan por finalidad la seguridad y defensa nacional o la prevención, detección, monitoreo y control del lavado de activos y la financiación del terrorismo, las de inteligencia y contrainteligencia, las de información periodística, las reguladas por la Ley 1266 de 2008 y las reguladas por la Ley 79 de 1993.

7. PRINCIPIOS RECTORES

Todo Tratamiento que realice la Compañía se sujeta, de manera armónica e integral, a los ocho principios del artículo 4 de la Ley 1581 de 2012. No son jerárquicos ni alternativos: el incumplimiento de cualquiera de ellos vicia el Tratamiento.

Lit.	Principio	Contenido
a)	**Legalidad**	El Tratamiento es una actividad reglada que debe sujetarse a lo establecido en la ley y en las demás disposiciones que la desarrollen.

b)	**Finalidad**	El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley, la cual debe ser informada al Titular. Prohíbe el uso ulterior incompatible con la finalidad informada.
c)	**Libertad**	El Tratamiento sólo puede ejercerse con el consentimiento previo, expreso e informado del Titular. Los datos no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.
d)	**Veracidad o calidad**	La información debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
e)	**Transparencia**	Debe garantizarse al Titular el derecho a obtener, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.
f)	**Acceso y circulación restringida**	El Tratamiento se sujeta a los límites que derivan de la naturaleza de los datos. Salvo la información pública, los datos no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o a terceros autorizados.
g)	**Seguridad**	La información se maneja con las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
h)	**Confidencialidad**	Todas las personas que intervengan en el Tratamiento de datos que no tengan el carácter de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento.

7.1. Reglas de gestión que complementan los principios

Las siguientes son reglas propias de la Compañía, adoptadas en desarrollo del principio de responsabilidad demostrada de los artículos 2.2.2.25.6.1 y 2.2.2.25.6.2 del Decreto 1074 de 2015. No sustituyen los principios legales: los operacionalizan.

Regla	Contenido
Separabilidad de las bases de datos	La Compañía mantiene separadas, lógica y físicamente, las bases de datos en las que tiene la calidad de Encargada de aquellas en las que es Responsable. Los perfiles de acceso, los plazos de retención y los procedimientos de supresión se administran de forma independiente para unas y otras.
Limitación temporal del Tratamiento	Los datos se tratan durante el tiempo razonable y necesario para las finalidades que justificaron su recolección. Cumplida la finalidad se suprimen, salvo disposición legal o contractual en contrario (art. 2.2.2.25.2.8). Los plazos están en la sección 22.2.
Minimización en la recolección	Sólo se recolectan los datos pertinentes y adecuados a la finalidad informada (art. 2.2.2.25.2.1). Está prohibido pedir datos «por si acaso» o conservar hojas de vida de candidatos no seleccionados sin base ni plazo.
Protección posterior a la terminación del vínculo	Todo dato que no sea público continúa tratándose como confidencial una vez terminado el vínculo que dio origen al Tratamiento, y hasta su supresión efectiva.

Privacidad desde el diseño y por defecto	Todo proyecto, sistema o cambio de proceso que implique Tratamiento de datos personales se consulta con la Dirección Legal antes de su implementación, para verificar la base de legitimación, la finalidad autorizada, el plazo de retención y las medidas de seguridad.
Responsabilidad demostrada	La Compañía conserva la evidencia que acredita el cumplimiento: autorizaciones, contratos de transmisión, inventario de bases, radicados del RNBD, registro de consultas y reclamos, actas de capacitación y de aprobación, y reportes a la SIC.

8. DATOS QUE TRATA LA COMPAÑÍA Y BASES DE DATOS

La Compañía trata datos de identificación, de contacto, de ubicación, socioeconómicos, de historia laboral y académica, de afiliación al Sistema de Seguridad Social Integral, financieros y de facturación, de acceso a sistemas de información, y las imágenes captadas por los sistemas de videovigilancia. Trata además, con las restricciones de la sección 12, datos sensibles: datos de salud en el marco del Sistema de Gestión de Seguridad y Salud en el Trabajo, datos biométricos para control de acceso, y las restricciones alimentarias que el Titular declare voluntariamente.

9. FINALIDADES DEL TRATAMIENTO, POR GRUPO DE TITULARES

Las finalidades se enuncian de manera específica y agrupadas por grupo de Titulares, de modo que cada persona pueda identificar para qué se tratan sus datos. La Compañía no trata datos personales para finalidades distintas de las aquí informadas o de las que el Titular acepte expresamente al momento de la recolección.

9.1. Trabajadores, extrabajadores, aprendices y candidatos

- **Adelantar procesos de selección:** recepción y evaluación de hojas de vida, verificación de referencias laborales y de títulos académicos, pruebas técnicas y psicotécnicas, y estudios de seguridad.
- **Formalizar la vinculación:** elaboración y suscripción del contrato, afiliación al Sistema de Seguridad Social Integral y a la caja de compensación familiar, y expedición del carné.
- **Liquidar y pagar la nómina,** las prestaciones sociales, las vacaciones, los aportes parafiscales y las retenciones de ley, y expedir los certificados correspondientes.
- **Administrar el Sistema de Gestión de Seguridad y Salud en el Trabajo:** programación de evaluaciones médicas ocupacionales y recepción del concepto de aptitud, gestión de incapacidades, investigación de accidentes e incidentes de trabajo, seguimiento de casos de enfermedad laboral y ejecución de los programas de medicina preventiva y de vigilancia epidemiológica.
- **Controlar el ingreso, la permanencia y la salida de las instalaciones de la Compañía** y de las plantas o unidades de clientes en las que presta el servicio, incluido el registro biométrico cuando el Titular lo haya autorizado de forma separada, en los términos de la sección 12.1.

- **Gestionar la formación y la capacitación, las evaluaciones de desempeño,** los planes de carrera y los programas de bienestar, incluidos los que se extienden al grupo familiar del trabajador.
- **Expedir certificaciones laborales** y suministrar referencias laborales cuando el extrabajador lo solicite o lo haya autorizado.
- **Adelantar procesos disciplinarios** e investigaciones internas por conductas que puedan constituir incumplimiento del reglamento interno de trabajo, del Código de Conducta o de las políticas de la Compañía.
- **Atender requerimientos de autoridades judiciales y administrativas**, y ejercer o defender los derechos de la Compañía en procesos judiciales, administrativos o arbitrales.
- **Reportar a la casa matriz y a las entidades del grupo la información de personal** necesaria para la consolidación de indicadores y la gestión corporativa, en los términos de la sección 15.
- Conservar la hoja de vida del candidato no seleccionado en el banco de talento, **únicamente cuando el candidato lo haya autorizado de forma expresa** y por el plazo señalado en la sección 22.2. A falta de esa autorización, la hoja de vida se devuelve o se destruye con constancia.

9.2. Clientes y clientes potenciales

Cuando el cliente es persona jurídica, los datos de su representante legal y de sus contactos son datos personales de personas naturales y se tratan bajo esta política.

- **Atender solicitudes de información y de cotización**, elaborar propuestas comerciales y participar en procesos de selección, licitación o contratación.
- **Celebrar, ejecutar, modificar y liquidar los contratos** de prestación de servicios de catering aéreo, catering industrial y de remotos, y servicios de alimentación en plantas.
- **Programar y ejecutar la operación diaria del servicio** menús, ciclos, novedades y órdenes
- **Facturar los servicios prestados,** gestionar la cartera, realizar conciliaciones y cumplir las obligaciones tributarias y de registro contable asociadas.
- **Atender peticiones, quejas, reclamos y sugerencias**, y medir la satisfacción con el servicio prestado.
- Enviar comunicaciones comerciales, invitaciones a eventos e información sobre nuevos servicios, **únicamente cuando el Titular lo haya autorizado**; esa autorización es revocable en cualquier momento y por el mismo canal por el que se realizó el contacto, sin que su revocatoria afecte la ejecución del contrato.
- **Adelantar la debida diligencia de conocimiento de la cliente prevista** en la sección

9.3. Proveedores, contratistas y sus colaboradores

- **Adelantar los procesos de selección**, evaluación, homologación, reevaluación y desarrollo de proveedores.
- **Celebrar y ejecutar contratos**, órdenes de compra y órdenes de servicio.
- **Gestionar la cuenta por pagar**: radicación y validación de facturas, causación, conciliación de cartera y pago.
- **Verificar el cumplimiento de las obligaciones del proveedor** en materia de afiliación y aportes a seguridad social, seguridad y salud en el trabajo, inocuidad alimentaria y licencias o habilitaciones exigidas por la ley.
- **Controlar el ingreso y la permanencia de contratistas** y de su personal en las instalaciones de la Compañía y en las unidades de servicio.
- **Adelantar la debida diligencia** de conocimiento del proveedor prevista en la sección 11.
- **Atender requerimientos de autoridades** y ejercer o defender los derechos de la Compañía en sede judicial, administrativa o arbitral.

9.4. Visitantes y personas que ingresan a las instalaciones

- **Registrar el ingreso y la salida**, identificar a quien ingresa y controlar su permanencia, con el fin de garantizar la seguridad de las personas, de los bienes y de las áreas, y la inocuidad de los procesos de alimentos.
- **Captar imágenes mediante los sistemas de videovigilancia instalados en accesos**, corredores, áreas de producción y zonas de almacenamiento, con finalidad de seguridad e inocuidad. No hay cámaras en baños, vestieres, casilleros ni áreas de descanso, y las grabaciones no se utilizan para control de productividad ni con fines disciplinarios sin una base de legitimación distinta e informada.
- **Gestionar la participación de invitados y asistentes en eventos**, capacitaciones y visitas institucionales.

En cada acceso y en cada zona videovigilada se instala el aviso de privacidad de que trata la sección 21.

9.5. Titulares vinculados a clientes corporativos (Tratamiento por cuenta del cliente)

Respecto de los trabajadores, contratistas y visitantes de los clientes corporativos en cuyas plantas o sedes la Compañía presta el servicio de alimentación, **NEWREST actúa como Encargada del Tratamiento** y no como Responsable, en los términos de la sección 14. Las finalidades son las que el cliente, en su calidad de Responsable, instruye por escrito, y comprenden ordinariamente:

- Cargar y mantener actualizados en el sistema de control de comedor los datos de identificación que el cliente entrega (nombre, número de documento y dependencia), cuya actualización es permanente por efecto de la rotación de personal del cliente.
- Verificar el derecho del Titular al servicio de alimentación y habilitar su acceso.
- Contabilizar los servicios efectivamente prestados, para efectos de la facturación al cliente.

- Gestionar el enrolamiento en el sistema de control de acceso al comedor en la modalidad definida para cada planta, con sujeción a la sección 12.1.
- Recoger y procesar encuestas de satisfacción y peticiones, quejas, reclamos y sugerencias presentadas por los canales dispuestos, incluidos los códigos QR, que recogen nombre, área y de forma opcional correo electrónico.
- Registrar las alergias alimentarias y demás restricciones médicas que el Titular declare de forma voluntaria y expresa, con el único fin de evitar su exposición al alérgeno en el servicio.

La Compañía **no utiliza estos datos para finalidades propias**, no los incorpora a sus bases comerciales ni de mercadeo y no los comparte con terceros, salvo instrucción escrita del cliente o requerimiento de autoridad competente.

9.6. Finalidades transversales a todos los grupos de Titulares

- Cumplir las obligaciones legales, tributarias, contables, comerciales, laborales y de seguridad social a cargo de la Compañía, y atender los requerimientos de autoridades judiciales y administrativas competentes.
- Ejercer o defender los derechos de la Compañía en procesos judiciales, administrativos o arbitrales.
- Adelantar la gestión documental, la generación de copias de respaldo, la recuperación ante desastres y las demás actividades necesarias para la seguridad y la continuidad de la información.
- Atender auditorías internas y externas, incluidas las del grupo empresarial y las de certificación de sistemas de gestión.
- Adelantar campañas de actualización de datos y comunicar a los Titulares los cambios sustanciales de esta política, así como solicitar nuevas autorizaciones cuando el cambio se refiera a la finalidad.

10. AUTORIZACIÓN DEL TITULAR

Salvo en los casos exceptuados por la ley, todo Tratamiento requiere la **autorización previa, expresa e informada** del Titular, obtenida a más tardar en el momento de la recolección y por un medio que pueda ser objeto de consulta posterior (arts. 9 y 12 de la Ley 1581 de 2012 y arts. 2.2.2.25.2.2 a 2.2.2.25.2.5 del Decreto 1074 de 2015).

Antes de que el Titular autorice, la Compañía le informa: el Tratamiento al que serán sometidos sus datos y la finalidad; el **carácter facultativo** de la respuesta cuando se trate de datos sensibles o de datos de niñas, niños y adolescentes; los derechos que le asisten como Titular; y la identificación, dirección física o electrónica y teléfono del Responsable.

La autorización puede constar por escrito, de forma oral o mediante conductas inequívocas del Titular que permitan concluir de forma razonable que la otorgó. **En ningún caso el silencio se asimila a una conducta inequívoca.** No constituyen conducta inequívoca las casillas premarcadas, la continuación de la navegación en un sitio web, la falta de respuesta a un correo ni la aceptación de términos generales que no mencionen el Tratamiento.

La Compañía **conserva prueba de la autorización otorgada** por cada Titular, de manera indexada y recuperable, por todo el tiempo en que se traten los datos y mientras perduren las obligaciones derivadas del Tratamiento. La imposibilidad de producir esa prueba ante la autoridad equivale, en la práctica, a no contar con autorización.

10.1. Casos en que no se requiere autorización

Conforme al artículo 10 de la Ley 1581 de 2012, no se requiere autorización cuando se trate de:

a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales, o por orden judicial.

b) Datos de naturaleza pública.

c) Casos de urgencia médica o sanitaria.

d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.

e) Datos relacionados con el Registro Civil de las personas.

10.2. Cambio de finalidad y modificación de la política

Cuando la Compañía pretenda tratar datos para una finalidad distinta de la informada, **solicitará una nueva autorización** antes de iniciar ese Tratamiento. Los cambios sustanciales de esta política se comunican a los Titulares de manera oportuna y **antes de implementar la nueva versión**, por los canales de la sección 24.

11. CONSULTA DE LISTAS RESTRICTIVAS Y DEBIDA DILIGENCIA LA/FT/FPADM Y C/ST

En cumplimiento de sus deberes legales de prevención y control del lavado de activos, la financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva (LA/FT/FPADM) y de la Corrupción y Soborno Transnacional (C/ST), la Compañía consulta y verifica información de sus contrapartes (clientes, proveedores, contratistas, socios, administradores, empleados y candidatos) en listas restrictivas vinculantes y en fuentes oficiales de acceso público.

11.1. Base de legitimación

Esta actividad **no se sujeta a autorización revocable del Titular**. Su fundamento es el siguiente:

a) **Artículo 10, literal b), de la Ley 1581 de 2012** — se trata de datos de naturaleza pública: las listas vinculantes del Consejo de Seguridad de las Naciones Unidas, la lista OFAC/SDN y demás sanciones publicadas en registros oficiales, así como los antecedentes judiciales, fiscales y disciplinarios consultables en portales oficiales.

b) **Artículo 10, literal a), de la misma ley** — información requerida por entidad pública o administrativa en ejercicio de sus funciones legales, o por orden judicial.

c) **Ley 1762 de 2015** — las entidades obligadas a reportar a la Unidad de Información y Análisis Financiero (UIAF) pueden recolectar, procesar y almacenar información personal

sin autorización previa del Titular, siempre que respeten sus derechos fundamentales, mantengan la confidencialidad, restrinjan el acceso a personal autorizado y utilicen la información exclusivamente para fines de prevención de LA/FT.

d) Artículo 2, numeral 2, de la Ley 1581 de 2012 — las bases de datos cuya finalidad sea la prevención, detección, monitoreo y control del lavado de activos y la financiación del terrorismo están excluidas del ámbito del régimen general, sin perjuicio de los principios constitucionales y del deber de reserva.

11.2. Reglas de manejo

- El acceso a los resultados de la debida diligencia queda restringido a la Oficial de Cumplimiento y a quienes esta autorice por escrito.
- **Queda prohibida la reutilización** de esta información para finalidades comerciales, de mercadeo, de evaluación de desempeño o para cualquier otra ajena a la prevención de LA/FT/FPADM.
- La consulta y el reporte de información a centrales de información crediticia se rigen por la **Ley 1266 de 2008**, modificada por la Ley 2157 de 2021, régimen propio que exige autorización del Titular y comunicación previa con veinte (20) días de antelación antes de reportar información negativa.
- La documentación de debida diligencia se conserva por el plazo señalado en la sección 22.2.

12. TRATAMIENTO DE DATOS SENSIBLES

El Tratamiento de datos sensibles está **prohibido**, salvo en los casos del artículo 6 de la Ley 1581 de 2012. Cuando la Compañía requiera tratarlos con fundamento en la autorización explícita del Titular, las tres reglas del artículo 2.2.2.25.2.3 del Decreto 1074 de 2015 (antes art. 6 del Decreto 1377 de 2013):

1. Informa al Titular, de manera explícita y previa, que **no está obligado a autorizar** el Tratamiento de sus datos sensibles.
2. Le informa **cuáles de los datos que se le solicitan son sensibles** y la finalidad específica de su Tratamiento.
3. **No condiciona ninguna actividad** de contratación, vinculación, acceso a instalaciones, prestación del servicio o cualquier otra a que el Titular suministre datos sensibles.

La autorización para datos sensibles se obtiene de forma **separada e independiente** de la autorización general, mediante casilla o manifestación propia, y se conserva como prueba autónoma.

12.1. Datos biométricos y control de acceso

Los datos biométricos son datos sensibles por mandato del artículo 5 de la Ley 1581 de 2012. La Compañía utiliza sistemas de control de acceso con verificación biométrica (facial y/o

dactilar, según la instalación) para el control de ingreso a sus sedes y para el control del servicio de alimentación en plantas de clientes.

Ese Tratamiento se sujeta, de manera acumulativa, a las siguientes condiciones:

1. **Carácter facultativo y alternativa real.** El registro biométrico es **opcional**. En toda instalación en que opere un lector biométrico debe existir y estar disponible una **alternativa de identificación no biométrica y no gravosa** (digitación del número de documento, lectura del código de barras del documento de identidad, carné o registro con el personal de control), sin que su uso implique demora, señalamiento o restricción alguna para el Titular. **La biometría no puede ser en ningún caso la única vía de acceso.**
2. **Autorización explícita, separada y revocable.** Se obtiene antes del enrolamiento, en documento o formulario independiente, con la advertencia expresa de que el Titular no está obligado a autorizar y de que puede revocar la autorización en cualquier momento, caso en el cual se le habilita de inmediato la alternativa no biométrica y se suprime su plantilla.
3. **Almacenamiento.** Se almacena la **plantilla biométrica cifrada y no reversible**, no la imagen ni la huella en bruto. El proveedor del sistema es Encargado del Tratamiento y debe constar la ubicación de las plantillas.
4. **Finalidad estricta.** El registro biométrico se usa exclusivamente para el control de acceso o para el conteo de los servicios de alimentación. **No puede desviarse** a control de productividad, control de jornada con fines disciplinarios ni a ninguna otra finalidad, sin una base de legitimación distinta e informada.
5. **Supresión.** La plantilla se suprime dentro del plazo señalado en la sección 22.2, contado desde la desvinculación del Titular, la terminación del contrato con el cliente o la revocatoria de la autorización, lo que ocurra primero.

Cuando la Compañía opera el sistema de control de comedor por cuenta de un cliente corporativo, estas condiciones se incorporan en el contrato o cláusula de transmisión con el cliente, y la autorización del Titular la recauda quien el contrato indique, conservando ambas partes la prueba.

12.2. Datos de salud

La Compañía trata datos de salud en el marco del Sistema de Gestión de Seguridad y Salud en el Trabajo y para la gestión de incapacidades, accidentes y enfermedad laboral. Se observan las siguientes reglas:

- **La Compañía no recibe, no conserva ni anexa a la hoja de vida copia de la historia clínica ocupacional.** Su custodia corresponde al prestador de servicios de salud ocupacional, conforme a los artículos 16 y 17 de la Resolución 2346 de 2007, modificada por la Resolución 1918 de 2009. Del examen médico ocupacional la Compañía sólo recibe el **concepto de aptitud** con las recomendaciones o restricciones para el ejercicio de la labor. **La autorización del trabajador no sanea la recepción del diagnóstico**, porque la prohibición es sectorial y está dirigida al empleador.
- Las incapacidades, los diagnósticos y los soportes de casos médicos y de enfermedad laboral se custodian con acceso restringido al personal del proceso de Seguridad y Salud

en el Trabajo y de Gestión Humana estrictamente necesario, bajo control de acceso individual y trazabilidad.

- Las pruebas de embarazo y de VIH sólo se practican con el consentimiento del trabajador y en los supuestos en que la ley lo permita. Está prohibido indagar por el estado de embarazo en los procesos de selección.
- Las **alergias alimentarias y demás restricciones médicas** declaradas por el Titular son dato sensible de salud. Se recogen únicamente cuando el Titular las declara de forma voluntaria y expresa, con advertencia del carácter facultativo, y se usan con el único fin de evitar su exposición al alérgeno. **No puede negarse el servicio de alimentación a quien no declare esta información.**

13. TRATAMIENTO DE DATOS DE NIÑAS, NIÑOS Y ADOLESCENTES

El artículo 7 de la Ley 1581 de 2012 **proscribe** el Tratamiento de datos personales de niñas, niños y adolescentes, salvo aquellos datos que sean de naturaleza pública. Se trata de una prohibición con excepción estrecha, y no de una autorización condicionada.

Cuando excepcionalmente proceda (aprendices y trabajadores menores de edad en los supuestos autorizados por la ley laboral, hijos beneficiarios en seguridad social, hijos de trabajadores en programas de bienestar, o menores que ingresen a instalaciones o eventos), el Tratamiento cumple de manera **acumulativa** los tres requisitos del artículo 2.2.2.25.2.9 del Decreto 1074 de 2015 (antes art. 12 del Decreto 1377 de 2013):

1. Que el Tratamiento **responda y respete el interés superior** de la niña, el niño o el adolescente.
2. Que se asegure el **respeto de sus derechos fundamentales**.
3. Que el **representante legal del menor** otorgue la autorización, **previo ejercicio del derecho del menor a ser escuchado**, valorando su opinión en función de su madurez, autonomía y capacidad para entender el asunto.

La Compañía deja **constancia documental del ejercicio del derecho del menor a ser escuchado**, y no sólo de la firma del representante legal del menor. Ese registro es parte de la prueba de la autorización.

Los datos biométricos de menores de edad **no se recolectan**. Cuando un menor deba ingresar a una instalación sujeta a control de acceso, se utiliza la alternativa no biométrica y el registro se limita a los datos pertinentes y adecuados al control de ingreso, con supresión en el plazo de la sección 22.2. El representante legal puede ejercer en nombre del menor los derechos de conocer, actualizar, rectificar y suprimir, y revocar la autorización otorgada.

14. NEWREST COMO RESPONSABLE Y COMO ENCARGADA DEL TRATAMIENTO

La calidad en que actúa la Compañía no depende de su voluntad ni de la denominación que las partes den al contrato, sino de **quién decide sobre la base de datos y sobre el Tratamiento**. De esa calificación dependen los deberes aplicables y el instrumento que legitima el flujo de datos.

Criterio	NEWREST como RESPONSABLE	NEWREST como ENCARGADA

Cuándo	Cuando decide sobre la base de datos y sobre las finalidades del Tratamiento: datos de sus trabajadores, candidatos, clientes, prospectos, proveedores, contratistas y visitantes.	Cuando trata datos por cuenta de un tercero y bajo sus instrucciones: los datos de trabajadores, contratistas y visitantes de los clientes corporativos cargados en el sistema de control de comedor y en los canales de PQRS y satisfacción asociados al servicio.
Deberes	Los del artículo 17 de la Ley 1581 de 2012.	Los del artículo 18 de la Ley 1581 de 2012.
Instrumento	Autorización del Titular, salvo excepción legal.	Contrato o cláusula de transmisión con el cliente Responsable, conforme al artículo 2.2.2.25.5.2 del Decreto 1074 de 2015 (antes art. 25 del Decreto 1377 de 2013).
Registro en el RNBD	Inscribe la base a su nombre.	No inscribe la base como propia; la registra en su inventario interno bajo la calidad de Encargada, y figura como Encargada en el registro del cliente.

14.1. Deberes de la Compañía como Responsable

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de habeas data.

b) Solicitar y conservar copia de la respectiva autorización otorgada por el Titular.

c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten.

d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

e) Garantizar que la información que se suministre al Encargado sea veraz, completa, exacta, actualizada, comprobable y comprensible.

f) Actualizar la información, comunicando oportunamente al Encargado todas las novedades, y adoptar las medidas necesarias para que la información se mantenga actualizada.

g) Rectificar la información cuando sea incorrecta y comunicarlo al Encargado.

h) Suministrar al Encargado únicamente datos cuyo Tratamiento esté previamente autorizado.

i) Exigir al Encargado, en todo momento, el respeto de las condiciones de seguridad y privacidad de la información del Titular.

j) Tramitar las consultas y reclamos en los términos de la Ley 1581 de 2012.

k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y, en especial, para la atención de consultas y reclamos.

l) Informar al Encargado cuando determinada información se encuentre en discusión por parte del Titular.

m) Informar, a solicitud del Titular, sobre el uso dado a sus datos.

n) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

14.2. Deberes de la Compañía como Encargada

a) Garantizar al Titular el pleno y efectivo ejercicio del derecho de habeas data.

b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

c) Realizar oportunamente la actualización, rectificación o supresión de los datos.

d) Actualizar la información reportada por el Responsable **dentro de los cinco (5) días hábiles** contados a partir de su recibo.

e) Tramitar las consultas y reclamos formulados por los Titulares.

f) Adoptar un manual interno de políticas y procedimientos.

g) Registrar en la base de datos la leyenda **«reclamo en trámite»** en la forma en que se regula en la sección 17.3.

h) Insertar en la base de datos la leyenda «información en discusión judicial» cuando la autoridad competente lo notifique.

i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.

j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.

k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

14.3. Separación de las bases de datos

La Compañía **mantiene separadas** las bases de datos en las que es Encargada de aquellas en las que es Responsable. Esa separación es lógica y física: perfiles de acceso distintos, repositorios distintos, administradores distintos y plazos de retención distintos. Está prohibido incorporar a las bases propias de la Compañía (comerciales, de mercadeo, de gestión humana o de cualquier otra naturaleza) datos recibidos de un cliente corporativo en calidad de Encargada, así como utilizarlos para finalidades propias.

Al terminar el contrato con el cliente corporativo, la Compañía **devuelve o suprime** los datos tratados por su cuenta, según la instrucción escrita del cliente, y expide la constancia correspondiente en el plazo de la sección 22.2.

14.4. Relación con Encargados de la Compañía

Cuando un tercero trata datos personales por cuenta de la Compañía (proveedores de nómina, de tecnología, de servicios en la nube, de seguridad física, de salud ocupacional o de control de acceso), la Compañía suscribe con él un contrato o cláusula de transmisión con el contenido de la sección 15.2, adelanta la debida diligencia previa de sus garantías de seguridad y se reserva el derecho de auditar su cumplimiento.

15. TRANSFERENCIAS Y TRANSMISIONES DE DATOS PERSONALES

La distinción entre transferencia y transmisión es determinante y con frecuencia se invierte. Depende de si el receptor **decide** sobre los datos o los trata **por cuenta** de quien se los entrega.

	TRANSFERENCIA	TRANSMISIÓN
Quién recibe	Otro Responsable, que trata los datos para fines propios.	Un Encargado, que trata los datos por cuenta del Responsable y bajo sus instrucciones.
¿Cambia quién decide?	Sí.	No.
Instrumento	Autorización expresa e inequívoca del Titular y, si es internacional, el régimen del artículo 26 de la Ley 1581 de 2012.	Contrato de transmisión del artículo 2.2.2.25.5.2 del Decreto 1074 de 2015. Las transmisiones internacionales entre Responsable y Encargado no requieren ser informadas al Titular ni contar con su consentimiento cuando existe ese contrato.

15.1. Transferencias nacionales e internacionales

La Compañía transfiere datos personales a terceros Responsables únicamente cuando cuenta con la autorización del Titular o cuando media un deber legal, un requerimiento de autoridad competente o la necesidad de ejercer o defender un derecho en un proceso judicial, administrativo o arbitral.

Tratándose de **transferencias internacionales**, el artículo 26 de la Ley 1581 de 2012 **prohíbe** la transferencia de datos personales a países que no proporcionen niveles adecuados de protección. Esa prohibición sólo cede en los casos que la propia norma enumera:

a) Información respecto de la cual el Titular haya otorgado su **autorización expresa e inequívoca** para la transferencia.

b) Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública.

c) Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.

d) Transferencias acordadas en el marco de tratados internacionales en los que Colombia sea parte, con fundamento en el principio de reciprocidad.

e) Transferencias necesarias para la **ejecución de un contrato** entre el Titular y el Responsable, o para el cumplimiento de medidas precontractuales, siempre que se cuente con la autorización del Titular.

f) Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

Antes de cada transferencia internacional, la Dirección Legal verifica si el país de destino figura en la lista de países con nivel adecuado de protección del Capítulo Tercero del Título V de la Circular Única de la SIC (lista que la SIC puede modificar y que debe consultarse en su versión consolidada vigente). Si el país no figura y no aplica ninguna de las causales anteriores, la transferencia **no se realiza** hasta obtener la declaración de conformidad de la SIC o suscribir con el destinatario un instrumento jurídico en el que este garantice el cumplimiento de los principios y obligaciones de la normativa colombiana, comunicándolo a la Delegatura para la Protección de Datos Personales.

15.2. Transmisiones y contrato de transmisión

Cuando la Compañía entrega datos personales a un tercero para que los trate **por su cuenta**, suscribe con él un contrato o cláusula de transmisión que contiene, como mínimo: los alcances del Tratamiento; las actividades que el Encargado realizará por cuenta de la Compañía; las obligaciones del Encargado frente al Titular y frente a la Compañía; y el compromiso del Encargado de dar aplicación a las obligaciones que corresponden al Responsable bajo esta política y de realizar el Tratamiento conforme a la finalidad autorizada por el Titular.

El contrato incorpora expresamente las tres obligaciones que la norma exige del Encargado:

1. Dar Tratamiento, a nombre del Responsable, a los datos personales conforme a los principios que los tutelan.
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.

Adicionalmente, y como práctica de la Compañía, el contrato incluye: prohibición de subcontratar el Tratamiento sin autorización previa y escrita; identificación de la ubicación de los datos y de los subencargados; **obligación de notificar a la Compañía cualquier incidente de seguridad dentro de las veinticuatro (24) a cuarenta y ocho (48) horas siguientes a su detección**, de modo que la Compañía alcance a cumplir su propio plazo de quince (15) días hábiles ante la SIC; deber de asistir en la atención de consultas y reclamos; derecho de auditoría; y devolución o destrucción certificada de la información al terminar la relación.

16. DERECHOS DE LOS TITULARES

Conforme al artículo 8 de la Ley 1581 de 2012, el Titular de los datos personales tiene los siguientes derechos:

a) Conocer, actualizar y rectificar sus datos personales frente a la Compañía, en su calidad de Responsable o de Encargada. Este derecho se puede ejercer, entre otros, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.

b) Solicitar **prueba de la autorización** otorgada, salvo cuando la ley exceptúe ese requisito conforme al artículo 10.

c) Ser informado, previa solicitud, respecto del **uso** que se ha dado a sus datos personales.

d) Presentar ante la Superintendencia de Industria y Comercio **quejas** por infracciones a la ley, una vez agotado el trámite de consulta o reclamo ante la Compañía.

e) **Revocar la autorización y/o solicitar la supresión** del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales, o cuando la Superintendencia haya determinado el incumplimiento.

f) **Acceder en forma gratuita** a sus datos personales que hayan sido objeto de Tratamiento.

El acceso es gratuito **al menos una vez cada mes calendario** y cada vez que haya modificaciones sustanciales de esta política (art. 2.2.2.25.4.2 del Decreto 1074 de 2015). Para consultas adicionales dentro del mismo mes sólo podrán cobrarse los gastos de envío, reproducción y certificación, cuyo costo real debe poder demostrarse.

Están legitimados para ejercer estos derechos el Titular, sus causahabientes, su representante o apoderado, y quien actúe por estipulación a favor de otro (art. 2.2.2.25.4.1). La Compañía verifica la identidad del solicitante y, cuando actúe por medio de representante o apoderado, la prueba de esa calidad.

Los plazos que se señalan en esta política y los que a continuación se detallan se cuentan en **días hábiles**, salvo que expresamente se indique otra cosa.

17. PROCEDIMIENTO PARA EL EJERCICIO DE LOS DERECHOS

17.1. Presentación de la solicitud

Las consultas y los reclamos se presentan por cualquiera de los canales de la sección 5. La solicitud debe contener: la identificación plena del Titular; la descripción clara de los hechos y del objeto de la petición; la dirección física o electrónica de notificación; y los documentos que se quieran hacer valer. Cuando la Compañía requiera un documento de soporte que no se haya adjuntado, lo solicitará conforme a la regla de subsanación de la sección 17.3.

17.2. Consultas — artículo 14 de la Ley 1581 de 2012

Etapa	Plazo
Atención de la consulta	Diez (10) días hábiles contados desde la fecha de recibo de la solicitud.
Prórroga	Cinco (5) días hábiles adicionales. Se informa al interesado antes del vencimiento de los diez días iniciales, expresando los motivos de la demora y señalando la fecha en que se atenderá la consulta. Avisar después de vencido el término no prorroga nada.
Término máximo total	Quince (15) días hábiles.

La información que se suministre debe ser de fácil lectura, sin barreras técnicas que impidan su acceso, y corresponder en un todo a la que repose en la base de datos.

17.3. Reclamos — artículo 15 de la Ley 1581 de 2012

Procede el reclamo cuando el Titular, sus causahabientes o su representante consideren que la información debe ser corregida, actualizada o suprimida, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la ley.

Etapa	Plazo
Reclamo incompleto — requerimiento de subsanación	Dentro de los cinco (5) días siguientes a la recepción del reclamo, la Compañía requiere al interesado para que subsane las fallas.
Desistimiento	Transcurridos dos (2) meses desde la fecha del requerimiento sin que el solicitante presente la información requerida, se entiende que ha desistido del reclamo.
Traslado por falta de competencia	Si la Compañía no es competente para resolver el reclamo, da traslado a quien corresponda en un término máximo de dos (2) días hábiles e informa de ello al interesado.
Leyenda «reclamo en trámite»	Una vez recibido el reclamo completo, la Compañía incluye en la base de datos, en un término no mayor a dos (2) días hábiles, la leyenda «reclamo en trámite» y el motivo del mismo. La leyenda se conserva hasta que el reclamo sea decidido.
Atención del reclamo	Quince (15) días hábiles contados desde el día siguiente a la fecha de su recibo completo.
Prórroga	Ocho (8) días hábiles adicionales, informando al interesado, antes del vencimiento del primer término, los motivos de la demora y la fecha en que se atenderá el reclamo.
Término máximo total	Veintitrés (23) días hábiles.

La inclusión de la leyenda «reclamo en trámite» es una obligación autónoma: exige intervenir el registro del Titular en el sistema y no se satisface con responderle. La Dirección Legal verifica su cumplimiento en cada caso y deja evidencia de la fecha de inclusión y de retiro.

17.4. Contenido de la respuesta

Toda respuesta debe ser **clara, precisa, congruente y consecuente** con lo solicitado, y dar cuenta del trámite surtido. Cuando la Compañía niegue total o parcialmente el acceso a un dato, debe **invocar la norma exacta** que establece la clasificación o la reserva de **ese dato en concreto**, analizado individualmente. No es admisible la negativa en bloque sobre un expediente o una hoja de vida, ni la invocación genérica de que «se trata de información sensible».

17.5. Revocatoria de la autorización y supresión del dato

El Titular puede revocar en cualquier momento la autorización otorgada y solicitar la supresión de sus datos, mediante reclamo presentado conforme a la sección 17.3. La revocatoria puede ser **total** (sobre la totalidad de las finalidades consentidas) o **parcial** (sobre finalidades determinadas).

Situación	Efecto
Revocatoria sobre finalidades accesorias (mercadeo, uso de imagen,	Procede. La Compañía cesa el Tratamiento para esa finalidad, habilita la alternativa que corresponda y deja constancia.

actividades de bienestar, registro biométrico, banco de talento).	
Revocatoria sobre finalidades necesarias para el cumplimiento de un deber legal o para la ejecución del contrato (nómina, seguridad social, facturación, obligaciones tributarias y contables).	No procede la supresión mientras subsista el deber. La Compañía explica al Titular cuál es el deber, su fundamento y el plazo al cabo del cual se suprimirán los datos.
Solicitud de supresión de datos conservados por deber legal (contable, laboral, de seguridad y salud en el trabajo o de prevención de LA/FT).	Los datos se conservan, se limita su uso exclusivamente a esa finalidad, se restringe el acceso y se informa al Titular el plazo de conservación.

17.6. Requisito de procedibilidad

Conforme al artículo 16 de la Ley 1581 de 2012, el Titular sólo puede elevar queja ante la Superintendencia de Industria y Comercio **una vez agotado el trámite** de consulta o reclamo ante la Compañía. La Dirección Legal conserva, respecto de cada solicitud, el acuse de recibo con fecha, la trazabilidad de los días hábiles transcurridos, la copia de la respuesta y la prueba de su envío.

18. MEDIDAS DE SEGURIDAD

En desarrollo del principio de seguridad y de los artículos 17 literal d), 18 literal b) de la Ley 1581 de 2012 y 2.2.2.25.3.7 del Decreto 1074 de 2015, la Compañía adopta medidas apropiadas, efectivas y proporcionales a la naturaleza de los datos, al tipo de Tratamiento y a los riesgos que este representa para los derechos de los Titulares. Estas medidas se articulan con la Política de Seguridad de los Sistemas de Información del grupo (P.S.S.I.) y se agrupan conforme a la taxonomía de la Circular Externa 002 de 2024 de la SIC.

Tipo	Medidas
Tecnológicas	Control de acceso por perfiles y por necesidad de conocer; autenticación individual; cifrado de los datos personales en transmisión y, cuando sea técnicamente viable, en almacenamiento; segmentación de los ambientes de los sistemas donde se almacena datos personales; registro y conservación de trazas de acceso; copias de respaldo y pruebas periódicas de restauración; gestión de vulnerabilidades y actualizaciones.
Humanas	Cláusula de confidencialidad en los contratos de trabajo y de prestación de servicios, que subsiste después de terminado el vínculo; inducción en protección de datos personales para todo ingreso nuevo; capacitación anual general y capacitación específica para los roles críticos (Gestión Humana, Selección, Compras, Tecnología, Comercial, Servicio al Cliente, Seguridad y Salud en el Trabajo y personal de control de acceso); régimen disciplinario aplicable al incumplimiento.
Administrativas	Inventario de bases de datos actualizado; procedimiento documentado de obtención y conservación de autorizaciones; procedimiento de atención de consultas y reclamos con registro de trazabilidad; política de retención y supresión; procedimiento de gestión de incidentes; auditoría anual del programa; reporte periódico a los administradores.
Físicas	Control de acceso a las áreas donde reposan archivos con información personal; custodia bajo llave de los expedientes laborales y de los

	soportes de salud ocupacional, con acceso restringido y registro de consulta; mesa limpia y pantalla limpia; destrucción segura de documentos con constancia.
Contractuales	Contratos o cláusulas de transmisión con todos los Encargados; cláusulas de confidencialidad con proveedores que no tratan datos pero pueden acceder a ellos; obligación de notificación de incidentes en plazo corto; derecho de auditoría; devolución o destrucción certificada al terminar la relación.

La Compañía reconoce como frentes de mejora prioritarios, identificados en su diagnóstico interno, el fortalecimiento del control de los archivos físicos donde reposa información personal, la eliminación de la recepción de información personal sin autorización ni finalidad definida, y la depuración de las hojas de vida de candidatos que no avanzaron en los procesos de selección. El plan de acción correspondiente es objeto de seguimiento por la Dirección Legal.

19. REGISTRO NACIONAL DE BASES DE DATOS

La Compañía inscribe sus bases de datos en el Registro Nacional de Bases de Datos administrado por la Superintendencia de Industria y Comercio, conforme al artículo 25 de la Ley 1581 de 2012, al Capítulo 26 del Decreto 1074 de 2015 y a la Circular Externa 003 de 2018. **Cada base de datos se inscribe de forma independiente**, y cada sociedad del grupo registra las suyas bajo su propio número de identificación tributaria.

Obligación	Oportunidad
Inscripción de bases de datos creadas con posterioridad al vencimiento de los plazos iniciales	Dentro de los dos (2) meses siguientes a su creación.
Actualización anual del registro	Entre el 2 de enero y el 31 de marzo de cada año. Debe verificarse cada año si la Superintendencia ha modificado esta ventana.
Reporte de cambios sustanciales (finalidad, encargado, canales de atención, clasificación de los datos, medidas de seguridad, política de Tratamiento, transferencias y transmisiones internacionales)	Dentro de los primeros diez (10) días hábiles del mes siguiente a aquel en que se produjo el cambio.
Reporte semestral de reclamos presentados por los Titulares	Dentro de los quince (15) primeros días hábiles de febrero (reclamos del segundo semestre del año anterior) y de agosto (reclamos del primer semestre del año en curso). El reporte se presenta aunque no se hayan recibido reclamos.
Reporte de incidentes de seguridad	Dentro de los quince (15) días hábiles siguientes a su detección.

Para que el reporte semestral sea posible y verificable, la Dirección Legal lleva un registro permanente de consultas y reclamos con fecha de recibo, tipo, fecha de respuesta y días hábiles transcurridos. Los números de radicado del RNBD y sus consecutivos se conservan como prueba del registro y de cada actualización.

20. INCIDENTES DE SEGURIDAD

Se entiende por incidente de seguridad toda violación de los códigos de seguridad, o toda pérdida, robo o acceso no autorizado, que afecte la confidencialidad, la integridad o la disponibilidad de los datos personales. Los artículos 17 literal n) y 18 literal k) de la Ley 1581 de 2012 imponen el deber de informarlos a la autoridad, tanto al Responsable como al Encargado.

El procedimiento comprende cinco fases: detección, identificación y clasificación, respuesta y contención, documentación y reporte, y evaluación y mejora.

- Todo trabajador o contratista que detecte o sospeche un incidente debe informarlo **el mismo día** a la Dirección Legal y a Tecnología, por el canal dispuesto para ello.
- La Compañía **reporta el incidente a la Superintendencia de Industria y Comercio dentro de los quince (15) días hábiles siguientes a su detección**, por el módulo de incidentes de la plataforma del RNBD. El plazo corre desde la detección y no desde la resolución del incidente ni desde la terminación del análisis forense. Se admite reporte preliminar.
- El reporte contiene el tipo de incidente, la fecha de ocurrencia, la fecha de conocimiento, la causal, el tipo de datos comprometidos, la **cantidad de Titulares afectados**, las bases de datos afectadas y las medidas de contención y remediación.
- Cuando el incidente afecte datos que la Compañía trata en calidad de **Encargada**, informa además al cliente Responsable dentro del plazo pactado en el contrato de transmisión, y en todo caso a la mayor brevedad.
- La comunicación a los Titulares afectados no está impuesta con carácter general por la ley colombiana, pero la Compañía la evalúa en cada caso como medida de mitigación y la realiza cuando el incidente pueda generarles un perjuicio.
- La Compañía conserva un registro interno de incidentes con la descripción de las circunstancias, las bases y clases de datos comprometidos, las categorías de Titulares afectados, la fecha y hora del incidente y de su descubrimiento, las indagaciones realizadas, las medidas correctivas, los responsables del manejo y la **prueba del reporte a la SIC** y de las comunicaciones efectuadas.

21. AVISO DE PRIVACIDAD

Cuando no sea posible poner a disposición del Titular esta política al momento de la recolección, la Compañía le informa mediante **aviso de privacidad**, de manera oportuna y a más tardar al momento de la recolección. El aviso no reemplaza la política: es el vehículo informativo de primer contacto en porterías, zonas videovigiladas, comedores, formularios, códigos QR y canales telefónicos.

Conforme al artículo 2.2.2.25.3.3 del Decreto 1074 de 2015, el aviso contiene como mínimo:

1. Nombre o razón social y datos de contacto del Responsable.
2. El Tratamiento al cual serán sometidos los datos y la finalidad del mismo.
3. Los derechos que le asisten al Titular.
4. Los mecanismos dispuestos para que el Titular conozca esta política y los cambios sustanciales que se produzcan en ella.

Cuando por el canal se recolecten **datos sensibles** o datos de niñas, niños y adolescentes, el aviso señala expresamente el **carácter facultativo** de la respuesta. La Compañía conserva el modelo de cada aviso mientras se traten datos conforme a él y perduren las obligaciones derivadas del Tratamiento.

22. VIGENCIA DE LA POLÍTICA Y PERÍODO DE VIGENCIA DE LAS BASES DE DATOS

22.1. Vigencia de la política

Esta política entra en vigencia el **25 de septiembre de 2026** y deroga la versión 06 del 21 de julio de 2025. Permanecerá vigente hasta que sea sustituida por una versión posterior debidamente aprobada y comunicada.

22.2. Período de vigencia de las bases de datos

En cumplimiento del numeral 6 del artículo 2.2.2.25.3.1 del Decreto 1074 de 2015, el período de vigencia de las bases de datos **no se define por la duración de la operación de la Compañía**, sino por plazos determinables a partir de la finalidad de cada Tratamiento y de los deberes legales de conservación. Vencido el plazo, los datos se suprimen, se anonimizan o pasan a archivo de acceso restringido, según corresponda, y se deja evidencia de la actuación.

Base de datos o conjunto de información	Período de vigencia	Fundamento del plazo
Candidatos no seleccionados	Seis (6) meses contados desde la terminación del proceso de selección. Si el candidato autorizó expresamente su inclusión en el banco de talento, dos (2) años desde la autorización, prorrogables sólo con nueva autorización.	Principio de finalidad y limitación temporal (arts. 4 lit. b de la Ley 1581 y 2.2.2.25.2.8 del Decreto 1074).
Trabajadores — datos de la relación laboral	Duración del vínculo y diez (10) años contados desde su terminación.	Art. 28 del Código de Comercio (conservación de libros y papeles del comerciante) y términos de prescripción de las acciones laborales.
Trabajadores — soportes de afiliación y	Conservación indefinida, con acceso restringido, mientras	Régimen del Sistema General de Pensiones y carga

aportes al Sistema de Seguridad Social Integral	subsista su valor probatorio para el reconocimiento de prestaciones pensionales.	probatoria del empleador sobre tiempos de servicio y aportes.
Seguridad y salud en el trabajo — conceptos de aptitud, incapacidades, casos médicos, enfermedad laboral y medicina preventiva	Veinte (20) años contados desde la terminación del vínculo laboral.	Decreto 1072 de 2015, normas de conservación de documentos del SG-SST, y Resolución 2346 de 2007 modificada por la Resolución 1918 de 2009.
Clientes y proveedores — datos contractuales, de facturación y contables	Duración de la relación y diez (10) años contados desde su terminación o desde el último asiento, acto o documento.	Art. 28 del Código de Comercio y normas tributarias sobre firmeza de las declaraciones.
Clientes potenciales y prospectos	Dos (2) años contados desde el último contacto efectivo, o hasta la revocatoria de la autorización, lo que ocurra primero.	Principio de finalidad y limitación temporal.
Debida diligencia LA/FT/FPADM y C/ST	Diez (10) años contados desde la terminación de la relación con la contraparte, término que se ampliará si la normativa aplicable en la materia exige un plazo mayor.	Deberes de conservación documental del SAGRILAFT y PTEE (Circular Básica Jurídica de la Superintendencia de Sociedades) y Ley 1762 de 2015.
Plantillas biométricas	Treinta (30) días calendario contados desde la desvinculación del Titular, la terminación del contrato con el cliente o la revocatoria de la autorización, lo que ocurra primero.	Principio de limitación temporal y régimen de datos sensibles (arts. 6 de la Ley 1581 y 2.2.2.25.2.3 del Decreto 1074).
Grabaciones de videovigilancia	Treinta (30) días calendario, salvo que exista un incidente documentado que justifique su conservación por más tiempo, caso en el cual se conservan hasta la conclusión de la actuación correspondiente.	Principio de finalidad, necesidad y limitación temporal.
Registros de visitantes	Un (1) año contado desde la fecha del ingreso.	Principio de finalidad y limitación temporal.
Sistema de control de comedor (Tratamiento como Encargada)	Vigencia del contrato con el cliente corporativo. Terminado el contrato, devolución o supresión certificada dentro de los treinta (30) días calendario siguientes, según la instrucción escrita del cliente.	Art. 2.2.2.25.5.2 del Decreto 1074 de 2015 y estipulación del contrato de transmisión.
Autorizaciones, avisos de privacidad y evidencia del programa	Mientras se traten datos conforme a ellos y perduren las obligaciones derivadas del Tratamiento.	Arts. 17 lit. b) de la Ley 1581 y 2.2.2.25.2.5 y 2.2.2.25.3.4 del Decreto 1074.

La supresión alcanza también a las **copias de respaldo** y a las copias que reposen en poder de los Encargados, conforme al procedimiento y a los plazos técnicos definidos en el manual interno. Los plazos de conservación que concurran sobre un mismo dato se resuelven aplicando el más largo, limitando el uso del dato a la finalidad que justifica esa conservación.

23. GOBIERNO DEL PROGRAMA Y RESPONSABILIDAD DEMOSTRADA

Conforme a los artículos 2.2.2.25.6.1 y 2.2.2.25.6.2 del Decreto 1074 de 2015 y a la Circular Externa 003 de 2024 de la Superintendencia de Industria y Comercio, la administración de cada sociedad establece y monitorea las políticas internas de protección de datos personales, aprueba el manual interno, designa el área responsable y exige reportes periódicos.

- Esta política y el manual interno MAN-ITC-100-CO se someten a aprobación del máximo órgano de administración de cada sociedad, y de esa aprobación se deja **acta**.
- La Dirección Legal presenta a los administradores, **al menos una vez al año**, un informe sobre el estado del programa, los reclamos recibidos y su oportunidad de respuesta, los incidentes, las capacitaciones realizadas y el avance del plan de acción.
- El programa se somete a **auditoría**, interna o externa, cuyos hallazgos se traducen en un plan de acción con responsables y fechas.
- Antes de iniciar un Tratamiento que pueda representar un riesgo alto para los derechos de los Titulares (en particular la ampliación del uso de biometría o la incorporación de herramientas de inteligencia artificial que procesen datos personales), se realiza una **evaluación de impacto de privacidad** con descripción detallada del Tratamiento, evaluación de riesgos y medidas de mitigación.

24. MODIFICACIONES Y DIVULGACIÓN

La Compañía puede modificar la política cuando lo exijan cambios normativos, cambios en su operación o los resultados de sus auditorías. Los cambios sustanciales se comunican a los Titulares de manera oportuna y **antes de implementar la nueva versión**, y cuando el cambio se refiera a la **finalidad** del Tratamiento se solicita una **nueva autorización**.

La política se divulga por la intranet, Calypso y los canales internos de la Compañía, se entrega con la documentación contractual a clientes, proveedores y trabajadores, y puede solicitarse en cualquier momento al correo protecciondatos@newrest.eu | politica.datosco@newrest.eu o en la dirección física señalada en la sección 5. Las versiones anteriores se conservan en el sistema documental con su fecha de vigencia.