POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES Y AVISO DE PRIVACIDAD

Cómo protegemos y usamos los datos personales en todo el Grupo

Guatemala · El Salvador · Honduras · Nicaragua · Costa Rica · Panamá · República Dominicana · Colombia

Código SI-PO-08 · Versión 1.0 · 7 de octubre de 2026
Política regional única · Documento público · Sitio web → Privacidad
Aprobada por el Director General (CEO)

Contenido

Control del documento 3
1. Compromiso 4
2. Objetivo, alcance y definiciones 4
3. Responsables del tratamiento y contacto 5
4. Marco legal por país 5
5. Principios 6
6. Datos que tratamos, para qué y con qué base 7
7. Bases legales, consentimiento, datos sensibles y menores 8
8. Derechos de los titulares 8
9. Comunicación de datos, proveedores y transferencias internacionales 9
10. Seguridad e incidentes 10
11. Privacidad desde el diseño y registro de bases de datos 11
12. Conservación y eliminación 11
13. Sitio web, MyRAP, videovigilancia y Canal de Ética 11
14. Capacitación, responsabilidades y consecuencias 12
15. Seguimiento y reporte 13
16. Documentos relacionados 13
17. Vigencia, publicación y cambios 13
Anexo A. Formulario para ejercer derechos 14
Anexo B. Textos cortos para la web y formularios 14
Anexo C. Sociedades responsables 15
Anexo D. Reglas para Colombia 16
Anexo E. Calendario de conservación 17

Control del documento

Código	Versión	Fecha de emisión	Vigencia	Próxima revisión
SI-PO-08	1.0	07/10/2026	Desde la firma del Director General	Octubre de 2027

Versión	Fecha	Descripción del cambio
—	—	Avisos y políticas de privacidad que existían en el sitio web o en cada sociedad. Quedan sustituidos.
1.0	07/10/2026	Primera emisión como política regional única de tratamiento de datos personales y aviso de privacidad del Grupo Rent a Pallet para los ocho países. Integra la política de seguridad de la información (SI-PO-01 a SI-PO-06) y el Programa Regional de Integridad, Ética y Cumplimiento (PG-CU-00). Incluye bases legales, derechos y plazos, incidentes, proveedores, transferencias, conservación y un anexo para Colombia.

Clasificación: documento público. **Dueño:** Tecnología de la Información (TI), con la Coordinación de Gobierno Corporativo y Legal. **Oficial de Protección de Datos Personales:** Oficial de Cumplimiento Regional, con el apoyo de TI; mientras se incorpora, la Coordinación de Gobierno Corporativo. **Validación legal previa:** asesores legales de cada país, en especial Colombia, Costa Rica, Panamá y El Salvador.

Aprobaciones

Elaboró	Revisó	Aprobó
Catalina Nicholls Coordinadora de Gobierno Corporativo Fecha: ____/____/_____	**Milton Villegas** Gerente del Departamento de Tecnología (TI) Fecha: ____/____/_____	**Carlos Luis Monge** Director General (CEO) Fecha: ____/____/_____

1. Compromiso

> **En el Grupo Rent a Pallet respetamos la privacidad de las personas.** Tratamos sus datos personales **solo para fines legítimos, informados y necesarios**, los protegemos con medidas de seguridad adecuadas y garantizamos que cada persona pueda **conocer, actualizar, corregir, suprimir u oponerse** al tratamiento de sus datos en cualquiera de los ocho países donde operamos. **No vendemos datos personales.**

Esta política fija un estándar único para los ocho países. Desarrolla el Código de Ética y Conducta, se complementa con la Política de Cookies y los Términos y Condiciones del sitio web, y se aplica junto con las demás políticas de integridad del Grupo. **Cuando la ley de un país sea más protectora para la persona, se aplica la ley.**

2. Objetivo, alcance y definiciones

Esta política establece cómo el Grupo recolecta, usa, almacena, comparte, conserva y elimina los datos personales, y cómo las personas pueden ejercer sus derechos. Sirve además como **aviso de privacidad** del sitio web corporativo y de los canales digitales del Grupo.

- **Cumplir** las leyes de protección de datos de los países donde operamos, con un estándar común.
- **Proteger** los datos de colaboradores, candidatos, clientes, proveedores, inversionistas, visitantes y demás personas.
- **Atender** con rapidez y claridad las solicitudes de las personas sobre sus datos.
- **Responder** de forma ordenada ante incidentes de seguridad y poder demostrar que se cumple lo que se promete.

2.1 Alcance

- **Sociedades:** todas las sociedades del Grupo listadas en el Anexo C, incluida la sociedad emisora Costa Rican Pallet & Pooling Co., Corp., las sociedades operativas de Costa Rica, Guatemala, El Salvador, Honduras, Nicaragua, Panamá, República Dominicana y Colombia, y las sociedades de American Pallet & Logistics.
- **Personas cuyos datos tratamos (titulares):** clientes y sus contactos, proveedores y contratistas, colaboradores y excolaboradores y sus familiares o beneficiarios, candidatos a empleo, accionistas, inversionistas y tenedores de bonos, miembros de la Junta Directiva y de los comités, visitantes de plantas y oficinas, usuarios del sitio web y de MyRAP, personas que reportan por el Canal de Ética y miembros de comunidades.
- **Datos cubiertos:** los de toda persona natural, en cualquier medio, físico o digital.
- **Obligados:** directores, colaboradores y terceros que traten datos por cuenta del Grupo, como los proveedores de servicios.

2.2 Definiciones clave

Término	Significado
Dato personal	Cualquier información que identifique o permita identificar a una persona natural: nombre, documento, teléfono, correo, dirección IP, imagen, entre otros.
Dato sensible	Dato que, si se usa mal, puede discriminar o afectar la intimidad: salud, origen étnico, creencias, afiliación sindical, vida sexual y datos biométricos.
Titular	La persona a quien pertenecen los datos.
Responsable	La sociedad del Grupo que decide para qué y cómo se tratan los datos.

Término	Significado
Encargado	La persona o empresa que trata datos por cuenta del responsable, como un proveedor de nube, nómina o sitio web.
Tratamiento	Cualquier operación con datos: recolectar, almacenar, usar, consultar, compartir, transferir o eliminar.
Consentimiento o autorización	Manifestación libre, informada, específica e inequívoca de la persona para un tratamiento concreto. Puede retirarse.
Transferencia internacional	Envío o acceso a datos desde un país hacia otro, incluido el almacenamiento en la nube fuera del país.
Incidente de seguridad	Pérdida, robo, acceso, uso, alteración o divulgación no autorizados de datos personales.
Evaluación de impacto	Análisis previo de los riesgos que un nuevo proyecto o sistema puede causar a la privacidad de las personas.

3. Responsables del tratamiento y contacto

Cada sociedad del Grupo es **responsable** de los datos personales que recolecta en su país. La coordinación regional y la atención de solicitudes se centralizan así:

Concepto	Información
Responsable regional	Costa Rican Pallet & Pooling Co., Corp. · Ave. Roberto Motta, Costa del Este, Parque Lefevre, Ciudad de Panamá
Correo para ejercer derechos y consultas	**datospersonales@rentapallet.com**
Formulario en línea	www.rentapallet.com → Privacidad → Ejercer mis derechos
Oficial de protección de datos	Oficial de Cumplimiento Regional, con el apoyo de Tecnología. Mientras se incorpora, la Coordinación de Gobierno Corporativo.
Responsables locales	La sociedad del Grupo de cada país (listado en el Anexo C).
Incidentes o conducta indebida	Canal de Ética: etica@rentapallet.com · tools.rentapallet.com/etica
Sitio web	www.rentapallet.com

4. Marco legal por país

El Grupo aplica la ley de protección de datos de cada país y, donde no existe una ley general, los estándares de esta política. **Cuando dos normas difieran, se aplica la más protectora para el titular.**

País	Norma principal	Autoridad	Observación
Colombia	Ley 1581 de 2012, Decreto 1377 de 2013 (compilado en el Decreto 1074 de 2015) y Ley 1266 de 2008 (hábeas data financiero)	Superintendencia de Industria y Comercio (SIC)	Exige autorización previa y expresa, política publicada, Registro Nacional de Bases de Datos cuando aplique y reporte de incidentes a la SIC. Ver Anexo D.
Costa Rica	Ley 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales y su Reglamento (Decreto Ejecutivo 37554-JP)	Agencia de Protección de Datos de los Habitantes (PRODHAB)	Consentimiento informado y por escrito, físico o electrónico; inscripción de bases de datos cuando la ley lo exige; transferencias con autorización expresa del titular.

País	Norma principal	Autoridad	Observación
Panamá	Ley 81 de 2019 y Decreto Ejecutivo 285 de 2021	ANTAI	Consentimiento previo, informado e inequívoco; derechos ARCO y portabilidad.
El Salvador	Ley para la Protección de Datos Personales, Decreto 144 de 2024	Agencia de Ciberseguridad del Estado (ACE)	Aviso de privacidad previo; derechos ARCO-POL; transferencias con autorización y contrato. La ACE emite lineamientos para el delegado de protección de datos.
Nicaragua	Ley 787 de 2012, Ley de Protección de Datos Personales	Dirección de Protección de Datos Personales	Consentimiento previo e informado del titular; derechos de acceso, rectificación, cancelación y oposición. Aplica esta política como estándar mínimo.
República Dominicana	Ley 172-13 de protección integral de los datos personales	Tribunales (acción de hábeas data)	Consentimiento del titular; derechos de acceso, rectificación y supresión, exigibles mediante la acción de hábeas data. Aplica esta política como estándar mínimo.
Guatemala	Sin ley general vigente. Constitución (arts. 24 y 31) y Ley de Acceso a la Información Pública (Decreto 57-2008)	—	Hay una iniciativa de ley en el Congreso (iniciativa 6464), pendiente de dictamen. Mientras tanto, aplica esta política como estándar mínimo.
Honduras	Sin ley general vigente. Constitución (hábeas data) y Ley de Transparencia y Acceso a la Información Pública	IAIP en el ámbito público	Aplica esta política como estándar mínimo.

Como referencia de buena práctica, el Grupo toma los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (RIPD), el Reglamento General de Protección de Datos de la Unión Europea (RGPD), aplicados de forma voluntaria, y las normas ISO/IEC 27001 (seguridad de la información), ISO/IEC 27701 (gestión de la privacidad) e ISO 37301 (cumplimiento).

5. Principios

Principio	Qué significa
Legalidad y lealtad	Los datos se recolectan sin engaño y conforme a la ley, con una base legal y diciéndole a la persona qué hacemos.
Finalidad	Se usan solo para los fines informados al titular y compatibles con ellos.
Consentimiento	Se obtiene la autorización del titular cuando la ley lo exige.
Minimización	Solo se piden los datos necesarios.
Exactitud	Los datos se mantienen veraces, correctos y actualizados.
Conservación limitada	No se guardan más tiempo del necesario o del que exija la ley (Anexo E).
Seguridad y confidencialidad	Se protegen con medidas técnicas, administrativas y físicas (SI-PO-01 a SI-PO-06) y solo acceden las personas autorizadas.
Transparencia	Se informa de forma clara y sencilla.

Principio	Qué significa
Responsabilidad demostrada	El Grupo documenta lo que hace para poder probar que cumple.
Privacidad desde el diseño	La protección de datos se considera desde que se piensa un proceso o sistema.

6. Datos que tratamos, para qué y con qué base

Titular	Datos	Finalidades	Base legal
Clientes y sus contactos	Nombre, cargo, empresa, correo, teléfono, dirección de entrega, usuario de MyRAP, datos de facturación y pago	Prestar el servicio de pooling y arrendamiento de tarimas; recolección y conteo; facturación electrónica y cobranza; atención al cliente; encuestas de satisfacción; conocimiento del cliente (PO-CU-01)	Contrato, ley e interés legítimo. Consentimiento para comunicaciones comerciales
Proveedores y contratistas	Nombre, identificación, representantes y beneficiarios finales, datos bancarios, certificaciones, antecedentes en listas restrictivas	Selección, contratación y pago; debida diligencia de integridad (PO-CU-04); trazabilidad de la madera; seguridad y salud de contratistas	Contrato y ley
Colaboradores y excolaboradores	Identificación, contacto, datos laborales, salariales y bancarios, seguridad social, formación, evaluaciones, salud ocupacional, familiares y beneficiarios	Gestión de la relación laboral, nómina y prestaciones; seguridad y salud en el trabajo; capacitación; cumplimiento legal; declaraciones de conflictos de interés (GC-DP-03)	Contrato laboral, ley y, para datos sensibles, consentimiento
Candidatos	Contacto, hoja de vida, estudios, referencias, resultados de pruebas	Evaluar candidaturas en los procesos de selección y la bolsa de empleo	Consentimiento y medidas previas a la contratación
Accionistas, inversionistas, tenedores de bonos, Junta Directiva y comités	Identificación, contacto, participación, declaraciones de conflictos de interés, datos de conocimiento del cliente y de participación en sesiones	Relación con inversionistas; obligaciones del emisor ante la SMV, Latinex y agentes de la emisión; obligaciones societarias y de gobierno corporativo; prevención de LA/FT	Ley y contrato
Visitantes de plantas y oficinas	Nombre, identificación, empresa, imagen de videovigilancia, registro de ingreso	Seguridad de personas y activos; control de acceso; protección del pool de tarimas	Interés legítimo
Usuarios del sitio web	Datos de formularios de contacto, dirección IP, identificadores de cookies técnicas y de analítica	Atender solicitudes; funcionamiento y mejora del sitio (capítulo 13 y Política de Cookies)	Consentimiento (cookies no esenciales) e interés legítimo
Personas que reportan por el Canal de Ética	Solo los datos que decidan entregar; puede ser anónimo. Datos de las personas mencionadas	Recibir, investigar y resolver reportes con confidencialidad, con las garantías de la GC-DP-05 y la PO-CU-08	Ley, interés legítimo y consentimiento
Comunidades	Nombre y contacto de quienes presentan quejas o participan en consultas	Mecanismo de quejas y relacionamiento comunitario (P-SGAS-02, P-SGAS-04)	Consentimiento e interés legítimo

Lo que no hacemos. No vendemos ni alquilamos datos personales. No los usamos para fines distintos a los informados sin una nueva base legal. No tomamos decisiones que produzcan efectos jurídicos sobre una persona basadas únicamente en tratamientos automatizados, sin intervención humana.

7. Bases legales, consentimiento, datos sensibles y menores

Base legal	Cuándo se usa
Consentimiento	Cuando no existe otra base: conservar una hoja de vida para futuras vacantes, enviar comunicaciones comerciales o activar cookies no esenciales.
Contrato o medidas previas	Para alquilar tarimas, contratar a un colaborador o a un proveedor.
Obligación legal	Nómina, impuestos, prevención de lavado de activos, mercado de valores, seguridad y salud, y requerimientos de autoridades.
Interés legítimo	Seguridad de las instalaciones y activos, prevención de fraude y gestión del Canal de Ética, siempre que se documente que no afecta de forma desproporcionada a la persona y que no prevalezcan sus derechos. Solo donde la ley local lo reconozca.
Interés vital	Emergencias que ponen en riesgo la vida o la salud de una persona.

7.1 Consentimiento

Debe ser previo, libre, informado, específico y fácil de retirar. No se condiciona un servicio a un consentimiento que no sea necesario. Se guarda la prueba: quién, cuándo, qué versión del aviso y para qué finalidad. En Colombia aplican las reglas de autorización del Anexo D.

7.2 Datos sensibles

Son sensibles, entre otros, los datos de salud, biométricos (huella o rostro para control de acceso), origen étnico, afiliación sindical y vida sexual. Solo se tratan cuando son indispensables, con **autorización expresa** cuando la ley lo exige, como la salud ocupacional o la afiliación a la seguridad social, y con medidas de seguridad reforzadas. El titular no está obligado a entregarlos. Se limita el acceso a las personas que los necesitan.

7.3 Menores de edad

El Grupo no recolecta intencionalmente datos de menores de edad, salvo los de beneficiarios de colaboradores para prestaciones legales, con autorización de su representante legal y respetando su interés superior.

8. Derechos de los titulares

Toda persona puede ejercer, de forma **gratuita**, los siguientes derechos:

Derecho	En qué consiste
Acceso	Saber si tratamos sus datos, cuáles, para qué y con quién se han compartido, y recibir una copia.
Rectificación	Corregir o actualizar datos inexactos o incompletos.
Cancelación o supresión	Pedir que se eliminen cuando ya no sean necesarios, cuando retire su consentimiento o se traten sin base legal, salvo obligación legal de conservarlos.
Oposición	Oponerse a ciertos tratamientos, como el envío de comunicaciones comerciales.
Revocación o retiro del consentimiento	Retirar la autorización en cualquier momento, con la misma facilidad con que se dio y sin efecto retroactivo.

Derecho	En qué consiste
Portabilidad	Recibir sus datos en un formato estructurado y de uso común, donde la ley lo reconoce.
Limitación y olvido	Pedir que se limite el tratamiento mientras se resuelve una reclamación, donde la ley lo reconoce (por ejemplo, El Salvador).
No ser objeto de decisiones automatizadas	Pedir intervención humana en decisiones que lo afecten y que se tomen solo por medios automáticos.
Queja ante la autoridad	Acudir a la autoridad de protección de datos de su país (capítulo 4).

8.1 Cómo ejercerlos

Paso	Qué se hace	Plazo
1. Solicitud	La persona escribe a **datospersonales@rentapallet.com**, usa el formulario del sitio web o el formato del Anexo A, indicando nombre, documento de identidad, país, derecho que ejerce, descripción y medio de respuesta. Si actúa un representante, adjunta el documento que lo acredite. Cualquier colaborador que reciba una solicitud la remite al Oficial el mismo día.	Inmediato
2. Acuse y verificación	Se acusa recibo y se confirma la identidad de la persona, sin pedir más datos de los necesarios.	5 días hábiles
3. Análisis	El Oficial de Protección de Datos, con Legal y el área dueña de los datos, decide si procede.	Dentro del plazo de respuesta
4. Respuesta	Se responde por escrito. Si se niega, se explican los motivos y se informa del derecho a reclamar ante la autoridad. Si se necesita más tiempo, se informa el motivo y la nueva fecha.	Consultas: 10 días hábiles, prorrogables por 5. Reclamos: 15 días hábiles, prorrogables por 8
5. Registro	Se guarda el registro de la solicitud, la decisión y la fecha.	Siempre

Se aplica el plazo menor cuando la ley del país del titular lo fije. Si la persona no está conforme con la respuesta, puede acudir a la autoridad de su país (capítulo 4) o al Canal de Ética. En Colombia aplican, además, las reglas del Anexo D.

9. Comunicación de datos, proveedores y transferencias internacionales

9.1 A quién comunicamos datos

Destinatario	Finalidad y garantías
Sociedades del Grupo en los ocho países	Gestión regional centralizada (nómina, finanzas, tecnología, cumplimiento), bajo esta misma política y un acuerdo de tratamiento de datos entre las sociedades.
Proveedores tecnológicos (nube, ERP SAP, facturación electrónica, correo y colaboración, Smart Tools)	Actúan como **encargados** del tratamiento, con contrato de encargo (sección 9.2) y seguridad con terceros (SI-PO-06).
Auditores, asesores legales, aseguradoras y bancos	Cumplimiento de obligaciones, auditorías y seguros, con deber de confidencialidad.
Autoridades	Cuando lo exija la ley o una orden competente.
Agentes de la emisión, reguladores del mercado de valores e inversionistas institucionales	Obligaciones del emisor y debida diligencia, limitadas a lo necesario.

9.2 Proveedores que tratan datos (contrato de encargo)

Antes de contratar a un proveedor que trate datos personales por cuenta del Grupo (nube, nómina, sitio web, comunicaciones, cobranza) se evalúa su seguridad y se firma un contrato de encargo que incluye, como mínimo:

- Tratar los datos solo según las instrucciones del Grupo y para la finalidad pactada.
- Confidencialidad y medidas de seguridad equivalentes a esta política.
- Autorización previa del Grupo para subcontratar, y las mismas obligaciones para el subcontratista.
- Aviso de cualquier incidente en un máximo de 24 horas y apoyo para atenderlo.
- Devolución o eliminación segura de los datos al terminar el contrato, y derecho del Grupo a auditar.

Los proveedores también se sujetan a la Política de Integridad para Socios, Proveedores, Contratistas y Clientes (PO-CU-04).

9.3 Transferencias internacionales

Los datos pueden circular entre las sociedades del Grupo en los ocho países y con proveedores ubicados en otros países, por ejemplo servicios de nube. En particular, las plataformas My RAP y Smart Tools (incluido el Canal de Ética) se alojan en Amazon Web Services en los Estados Unidos, y el correo y la colaboración se gestionan con Microsoft 365. Toda transferencia se hace solo con una base legal y con garantías: un destino con nivel adecuado de protección, cláusulas contractuales que obliguen al receptor a proteger los datos, o la autorización del titular cuando la ley lo exige. En **Costa Rica**, la transferencia de datos a otro país requiere la autorización expresa, informada e inequívoca del titular. En **Colombia** aplica el Anexo D. Las transferencias entre sociedades del Grupo se rigen por un acuerdo de tratamiento de datos entre ellas, y Legal mantiene un registro de los flujos de datos hacia otros países.

10. Seguridad e incidentes

10.1 Medidas de seguridad

El Grupo aplica medidas proporcionales al riesgo, alineadas con ISO/IEC 27001 y con sus políticas de seguridad de la información: clasificación (SI-PO-02), uso aceptable (SI-PO-03), control de acceso (SI-PO-04), copias de seguridad (SI-PO-05) y seguridad con terceros (SI-PO-06). TI las mantiene y las revisa cada año. Solo el personal autorizado accede a los datos, con el mínimo privilegio necesario.

Tipo	Medidas
Técnicas	Acceso por roles y con el mínimo privilegio; contraseñas seguras y doble factor de autenticación; cifrado de los datos en tránsito y, cuando sea posible, en reposo; copias de respaldo; actualizaciones de seguridad; antivirus y registro de accesos.
Organizativas	Cláusulas de confidencialidad para colaboradores y proveedores; clasificación de la información; escritorio limpio; entrega y baja de accesos al ingresar y al salir un colaborador; capacitación (sección 14.1).
Físicas	Control de acceso a oficinas, plantas y archivos; archivos físicos bajo llave; destrucción segura de documentos.

10.2 Incidentes de seguridad

Todo incidente que afecte datos personales se atiende con este procedimiento. **Cualquier persona que sospeche de un incidente debe reportarlo de inmediato** a TI y al Oficial de Protección de Datos, o por el Canal de Ética.

Fase	Qué se hace	Responsable	Plazo
1. Reporte	Se avisa y se registra qué pasó, cuándo y qué datos están involucrados.	Quien lo detecta	24 horas

Fase	Qué se hace	Responsable	Plazo
2. Contención	Se detiene la fuga, se aíslan sistemas, se recupera lo posible y se preserva la evidencia.	TI	Inmediata
3. Evaluación	Se mide el riesgo para las personas: tipo de datos, cantidad y probabilidad de daño.	Oficial, TI y Legal	72 horas
4. Notificación	Se informa a la autoridad y a las personas afectadas cuando la ley lo exija o el riesgo sea alto, en los plazos de la ley local.	Legal y Oficial	Según la ley local; si no la fija, 72 horas
5. Corrección	Se eliminan las causas y se refuerzan las medidas.	TI y área dueña	30 días
6. Registro y aprendizaje	Se guarda el expediente del incidente, aunque no deba notificarse. Se informa al Comité de Riesgos y, si es material, al Comité de Auditoría.	Oficial	Al cierre

En Colombia, el reporte a la SIC se rige por el Anexo D.

11. Privacidad desde el diseño y registro de bases de datos

- **Evaluación de impacto.** Antes de lanzar un sistema, proyecto o proceso que trate datos sensibles, datos de muchas personas, videovigilancia, biometría o decisiones automatizadas, el área responsable hace una evaluación de impacto, que aprueban el Oficial de Protección de Datos y TI.
- **Registro de tratamientos.** El Oficial mantiene un registro de las bases de datos y actividades de tratamiento: responsable, finalidad, categorías de datos, destinatarios, transferencias, plazos y medidas de seguridad.
- **Registro ante autoridades.** Donde la ley lo exija, las bases de datos se inscriben ante la autoridad competente, por ejemplo en Costa Rica y en Colombia (Anexo D). Legal verifica los requisitos de cada país.

12. Conservación y eliminación

Los datos se conservan mientras dure la relación y, después, durante el plazo que exijan la ley o la defensa de los derechos del Grupo, según el calendario del Anexo E. Al vencer el plazo se eliminan de forma segura o se anonimizan. Si hay un litigio, una investigación o un requerimiento de autoridad, se bloquea la eliminación hasta que termine. Cada año las áreas revisan el calendario y eliminan lo que ya no se necesita.

Como referencia, los registros de prevención de lavado de activos y del Canal de Ética se conservan **mínimo diez años** (PO-CU-01, PO-CU-08); las hojas de vida de candidatos no seleccionados, **un año**, salvo autorización para conservarlas más; y las grabaciones de videovigilancia, **hasta 30 días**, salvo que sean necesarias para una investigación.

13. Sitio web, MyRAP, videovigilancia y Canal de Ética

13.1 Sitio web y cookies

- El sitio web usa **cookies técnicas**, necesarias para su funcionamiento, y, con el consentimiento del usuario, **cookies de analítica** para medir el uso y mejorar los contenidos. El usuario puede aceptarlas, rechazarlas o configurarlas en el banner de cookies y en su navegador. El detalle está en la **Política de Cookies**.
- Los formularios del sitio muestran un **aviso corto de privacidad** y una casilla de aceptación (Anexo B). Los datos de los formularios se conservan según el Anexo E.
- El sitio puede contener enlaces a sitios de terceros, cuyas prácticas de privacidad no controla el Grupo.

13.2 MyRAP

MyRAP trata los datos de los usuarios de los clientes para operar la plataforma, con usuario y contraseña personales.

13.3 Videovigilancia

Las plantas y oficinas cuentan con cámaras para la seguridad de personas y activos, señalizadas con avisos visibles (Anexo B). No se instalan en baños, vestidores ni lugares de descanso. Las imágenes solo las ve el personal autorizado de Protección de Activos y Seguridad, y se conservan según el Anexo E.

13.4 Canal de Ética

Los datos que se entregan en el Canal de Ética se tratan con las garantías de **anonimato, confidencialidad y no represalias** de la GC-DP-05 y la PO-CU-08. El canal permite reportar sin datos de identificación y no registra la dirección IP ni la ubicación de quien reporta.

14. Capacitación, responsabilidades y consecuencias

14.1 Capacitación

- **Inducción:** todo colaborador nuevo recibe esta política dentro de sus primeros 30 días.
- **Anual:** capacitación para todo el personal.
- **Reforzada:** para quienes manejan más datos (Desarrollo Humano, Tecnología, Comercial, Servicio al Cliente y Compras) y para quienes atienden solicitudes de derechos e incidentes.
- **Registro:** se conserva la asistencia y se mide el avance (capítulo 15).

14.2 Responsabilidades

Responsable	Funciones
Junta Directiva y Comité de Auditoría	Supervisan el cumplimiento, reciben los informes y los incidentes graves, y atienden los casos que involucren a la alta dirección.
Director General y alta gerencia	Aprueban esta política, asignan los recursos y dan ejemplo.
Oficial de Protección de Datos (Oficial de Cumplimiento Regional)	Supervisa el cumplimiento, atiende las solicitudes de los titulares y la relación con las autoridades, mantiene el inventario de bases de datos y el registro de tratamientos e incidentes, aprueba las evaluaciones de impacto, capacita y reporta al Comité de Auditoría.
Gobierno Corporativo	Mantiene esta política, coordina su revisión anual y presenta los informes al Comité de Auditoría.
Legal	Valida la ley de cada país, los contratos de encargo, las transferencias, el registro ante autoridades y las notificaciones.
Tecnología de la Información (TI)	Diseña y mantiene las medidas de seguridad, gestiona los incidentes, los contratos con encargados tecnológicos y apoya las evaluaciones de impacto.
Desarrollo Humano Regional	Aplica esta política a los datos de candidatos y colaboradores, incluida la salud ocupacional, y gestiona las autorizaciones laborales.
Comercial, Servicio al Cliente y Compras	Aplican esta política a los datos de clientes y proveedores, y exigen el contrato de encargo.
Líderes de área	Garantizan que su equipo cumpla, reportan incidentes y solicitudes, y revisan la conservación.
Colaboradores y proveedores	Protegen los datos que manejan, reportan incidentes y solo los usan para su trabajo.

14.3 Consecuencias

Usar datos personales de forma indebida, acceder a ellos sin autorización, ocultar un incidente o tomar represalias contra quien reporte es una falta grave, sancionada conforme al Código de Ética y Conducta, a las Sanciones por Incumplimiento (GC-DP-06) y a la ley, y puede constituir un delito. A proveedores y contratistas se aplican medidas contractuales, incluida la terminación. Cualquier persona puede reportar por el Canal de Ética, sin represalias. La Auditoría Interna incluye esta política en su plan basado en riesgos (PO-GC-03).

15. Seguimiento y reporte

El Oficial informa al Comité de Auditoría cada semestre sobre las solicitudes de derechos recibidas y su tiempo de respuesta, los incidentes de seguridad y su notificación, el personal capacitado, los proveedores con contrato de encargo y las evaluaciones de impacto realizadas. El Comité presenta un informe anual a la Junta Directiva. Cada año se evalúa si las medidas son eficaces.

16. Documentos relacionados

- Código de Ética y Conducta (GC-CE-01) y Sanciones por Incumplimiento (GC-DP-06).
- Programa Regional de Integridad, Ética y Cumplimiento (PG-CU-00).
- Políticas de seguridad de la información (SI-PO-01 a SI-PO-06).
- Política de Cookies y Términos y Condiciones de Uso del sitio web.
- Política de Integridad para Socios, Proveedores, Contratistas y Clientes (PO-CU-04), conocimiento del cliente (PO-CU-01) y las políticas antifraude y de prevención de lavado de activos, por la debida diligencia y la conservación.
- Canal de Ética: GC-DP-05 y PO-CU-08, y declaración de empleados y directivos (GC-DP-03).
- Política de Dignidad y Respeto en el Trabajo y Política de Diversidad, Equidad e Inclusión, por el manejo confidencial de denuncias y los datos sensibles de discapacidad y género.
- Mecanismo de quejas y relacionamiento comunitario (P-SGAS-02, P-SGAS-04).
- Plan de Auditoría Interna basado en riesgos (PO-GC-03).

17. Vigencia, publicación y cambios

- **Vigencia:** desde su firma por el Director General. Deja sin efecto los avisos y políticas de privacidad anteriores que le sean contrarios.
- **Publicación:** en el sitio web, en español y en inglés, en PDF abierto, a no más de tres clics de la portada y con enlace permanente en el pie de todas las páginas.
- **Revisión:** al menos una vez al año, ante cambios legales o después de un incidente grave.
- **Cambios:** los cambios sustanciales se publican en el sitio web con su fecha de vigencia y, cuando la ley lo exige, se comunican a los titulares.

Fecha de última actualización: 07/10/2026

Anexo A. Formulario para ejercer derechos

Este formato es opcional: la solicitud también puede hacerse por correo a **datospersonales@rentapallet.com** o por el formulario del sitio web. El servicio es gratuito. La información que usted entregue se usa solo para atender su solicitud.

Campo	Respuesta
Nombre completo	
Tipo y número de documento	
País y sociedad del Grupo con la que se relaciona	
Relación con el Grupo (cliente, proveedor, colaborador, candidato, inversionista, visitante, otro)	
Derecho que ejerce	Acceso [ ] Rectificación [ ] Supresión [ ] Oposición [ ] Revocación [ ] Portabilidad [ ] Limitación [ ] Intervención humana [ ]
Descripción de la solicitud	
Medio de respuesta (correo / dirección)	
Documentos adjuntos (identificación, poder si actúa por otro)	
Firma y fecha	
Uso interno: fecha de recepción, folio y recibida por	
Uso interno: decisión, fecha de respuesta y responsable	

Anexo B. Textos cortos para la web y formularios

B.1 Aviso corto para formularios

> Al enviar este formulario, autorizo a la sociedad del Grupo Rent a Pallet de mi país a tratar mis datos personales para atender mi solicitud y, si lo acepto, para enviarme información comercial, conforme a su **Política de Tratamiento de Datos Personales y Aviso de Privacidad** (enlace). Puedo conocer, actualizar, corregir, suprimir mis datos o revocar esta autorización escribiendo a datospersonales@rentapallet.com.
>
> ☐ Acepto el tratamiento de mis datos para atender mi solicitud (obligatorio). ☐ Acepto recibir información comercial (opcional).

B.2 Banner de cookies

Usamos cookies propias necesarias para que el sitio funcione y, si usted lo acepta, cookies de analítica para mejorar nuestros contenidos. Puede aceptarlas, rechazarlas o configurarlas. Más información en nuestra **Política de Cookies** y en la **Política de Tratamiento de Datos Personales**. [Aceptar] [Rechazar] [Configurar]

B.3 Aviso de videovigilancia

ZONA VIDEOVIGILADA. Grupo Rent a Pallet trata imágenes con fines de seguridad de personas y activos. Para ejercer sus derechos: datospersonales@rentapallet.com.

B.4 Autorización para colaboradores y candidatos

Autorizo a [sociedad del Grupo] a tratar mis datos personales, incluidos los sensibles de salud ocupacional estrictamente necesarios, para la gestión de la relación laboral o del proceso de selección, conforme a la Política de Tratamiento de Datos Personales SI-PO-08, que he conocido. Declaro que fui informado de que no estoy obligado a entregar datos sensibles y de mis derechos de acceso, rectificación, supresión, oposición y revocación.

Nombre: _____ Documento: _____ Firma: _____ Fecha: _____

Anexo C. Sociedades responsables

País	Sociedad	Autoridad
Panamá (emisor)	Costa Rican Pallet & Pooling Co., Corp. y sociedades tenedoras	ANTAI
Panamá	Rent a Pallet Panamá S.A.	ANTAI
Costa Rica	Rent a Pallet S.A.	PRODHAB
Guatemala	Logística RAP, S.A.	— (sin autoridad)
El Salvador	Rent a Pallet El Salvador, S.A. de C.V.	ACE
Honduras	Logística RAP, S.A.	— (sin autoridad)
Nicaragua	TRÉBOL, S.A.	Dirección de Protección de Datos Personales
República Dominicana	CRP&P Rent a Pallet S.A.S.	Tribunales (acción de hábeas data)
Colombia	Colombiana de Estibas S.A. (COLESTIBAS)	SIC
Costa Rica, Guatemala y El Salvador	Sociedades de American Pallet & Logistics	Según el país

Anexo D. Reglas para Colombia

Este anexo recoge las reglas de la normativa colombiana que aplican a Colombiana de Estibas S.A. (COLESTIBAS). Si contradicen el cuerpo de la política, prevalece la más protectora para el titular compatible con la ley colombiana.

Tema	Regla en Colombia
Marco	Ley 1581 de 2012 (régimen general), Decreto 1377 de 2013 (compilado en el Decreto 1074 de 2015) y Ley 1266 de 2008 (hábeas data financiero). Autoridad: Superintendencia de Industria y Comercio (SIC).
Responsable	Colombiana de Estibas S.A. (COLESTIBAS), NIT 830085346-9. Contacto: datospersonales@rentapallet.com.
Autorización	Previa, expresa e informada, con prueba de que se obtuvo. Se informa para qué se usarán los datos y cuáles son los derechos de la persona.
Datos sensibles	Su entrega es facultativa. Se necesita autorización explícita y se informa cuáles datos son sensibles.
Niños, niñas y adolescentes	Solo se tratan con respeto de su interés superior y con autorización de su representante legal.
Consultas	Respuesta en 10 días hábiles, prorrogables por 5 días hábiles con aviso de los motivos.
Reclamos	Respuesta en 15 días hábiles, prorrogables por 8 días hábiles. Si el reclamo está incompleto, se pide corregirlo dentro de los 5 días siguientes. Se marca la base de datos con la leyenda “reclamo en trámite” en un máximo de 2 días hábiles.
Área de atención	Oficial de Protección de Datos (Oficial de Cumplimiento Regional, Departamento de Gobierno Corporativo): datospersonales@rentapallet.com.
Política de tratamiento	Está disponible para los titulares y se les comunica al momento de recoger los datos.
Transferencias internacionales	Solo a países con nivel adecuado de protección, o con las excepciones que prevé la ley.
Registro Nacional de Bases de Datos (RNBD)	Obligatorio para sociedades con activos totales superiores a 100.000 UVT. Se actualiza cada año entre el 2 de enero y el 31 de marzo, dentro de los 10 primeros días hábiles del mes siguiente a un cambio sustancial, y los reclamos se reportan en los 15 primeros días hábiles de febrero y agosto.
Reporte de incidentes a la SIC	Dentro de los 15 días hábiles siguientes al momento en que se detecta el incidente y se pone en conocimiento del área encargada. Si la sociedad está obligada a registrar sus bases de datos, se reporta por el RNBD; si no, por el módulo “Reporte de incidentes de seguridad” de la SIC.

Anexo E. Calendario de conservación

Los plazos son mínimos y se cuentan desde el cierre de la relación o del proceso, salvo que se indique otra cosa. **Prevalece el plazo mayor que exija la ley de cada país.**

Categoría de datos	Plazo de conservación	Referencia
Candidatos no seleccionados	1 año	Desde el cierre del proceso, o hasta que la persona retire su consentimiento
Expediente de colaboradores	Duración de la relación + plazo legal de cada país	Ley laboral
Nómina y seguridad social	Plazo legal de cada país	Ley laboral y tributaria
Salud ocupacional	Según la ley de salud ocupacional de cada país	Ley de seguridad y salud en el trabajo
Clientes: contratos y facturación	10 años	Ley contable y tributaria
Proveedores y debida diligencia	10 años	Prevención de lavado de activos (PO-CU-01, PO-CU-04)
Canal de Ética	10 años	Desde el cierre del caso (PO-CU-08)
Videovigilancia	Hasta 30 días	Salvo que se necesite como evidencia de una investigación
Formularios del sitio web	12 meses	Desde la última interacción
Consentimientos y solicitudes de derechos	5 años	Para demostrar el cumplimiento