POLCOMP CIA. LTDA.
POLITICA DE PROTECCIÓN DE DATOS PERSONALES

Contenido

1. INTRODUCCIÓN 3
2. OBJETIVO 3
3. ALCANCE 4
4. TÉRMINOS Y DEFINICIONES 5
5. FUNCIONES Y RESPONSABILIDADES PARA LA POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES 10
5.1. GERENCIA GENERAL Y ALTA DIRECCIÓN 10
5.2. DELEGADO DE PROTECCIÓN DE DATOS PERSONALES 10
5.3. DEPARTAMENTO LEGAL 11
5.4. DEPARTAMENTO DE SISTEMAS Y TECNOLOGÍA DE LA INFORMACIÓN 11
5.5. OPERACIONES Y GESTIÓN DE COBRANZA 12
5.6. TALENTO HUMANO 12
5.7. COMPRAS, PROVEEDORES Y ENCARGADOS 12
5.8. TRABAJADORES Y COLABORADORES 13
6. POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES 13
6.1. USO DE DATOS 14
6.1.1. USO DE DATOS DE CLIENTES, TITULARES DE OBLIGACIONES Y GARANTES 14
6.1.2. USO DE DATOS DE PROVEEDORES Y REPRESENTANTES 14
6.1.3. USO DE DATOS DE TRABAJADORES, CANDIDATOS Y EXTRABAJADORES 15
6.2. DATOS PERSONALES TRATADOS POR LA COMPAÑÍA 15
6.3. TIPOS DE DATOS PERSONALES TRATADOS POR LA COMPAÑÍA 16
6.4. CONSERVACIÓN, BLOQUEO, ELIMINACIÓN, ANONIMIZACIÓN Y SEUDONIMIZACIÓN 17
6.5. TRANSFERENCIAS Y COMUNICACIONES DE DATOS PERSONALES 17
6.6. PROTECCIÓN Y SEGURIDAD DE LOS DATOS PERSONALES 18
6.7. DERECHOS DEL TITULAR DE DATOS PERSONALES 19
6.8. CONSECUENCIAS DE PROPORCIONAR O DENEGAR DATOS PERSONALES 20
6.9. DATOS ERRÓNEOS, INEXACTOS O DESACTUALIZADOS 20
6.10. CULTURA, CAPACITACIÓN Y CONCIENTIZACIÓN 20
6.11. REVOCACIÓN DEL CONSENTIMIENTO 21

6.12. TRATAMIENTO DE DATOS DE NIÑAS, NIÑOS Y ADOLESCENTES 21

6.13. BASES DE LEGITIMACIÓN Y ANÁLISIS DE INTERÉS LEGÍTIMO..... 22

6.14. GESTIÓN DE COBRANZA, PROTOCOLO DE ESCALAMIENTO Y CONTACTO CON TERCEROS 23

6.15. FUENTES EXTERNAS, PROVEEDORES DE DATOS Y ENRIQUECIMIENTO 24

6.16. CONTRATOS, ENCARGADOS Y SUBENCARGADOS..... 25

6.17. GESTIÓN DE RIESGOS Y EVALUACIÓN DE IMPACTO 25

6.18. TRATAMIENTO DE DATOS PERSONALES A GRAN ESCALA..... 26

6.19. TRATAMIENTO DE DATOS BIOMÉTRICOS 26

6.20. INTELIGENCIA ARTIFICIAL, PERFILAMIENTO Y DECISIONES AUTOMATIZADAS 28

6.21. GESTIÓN Y NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD..... 29

6.22. TRAZABILIDAD, CONTROL DE COMUNICACIONES Y AUDITORÍA..... 29

6.23. INCUMPLIMIENTOS Y MEDIDAS DISCIPLINARIAS..... 30

7. ACTUALIZACIONES DE LA POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES 30

8. BASE LEGAL..... 31

9. APROBACIÓN 33

1. INTRODUCCIÓN

POLCOMP CÍA. LTDA. reconoce que la protección de datos personales es un derecho constitucional, una obligación jurídica exigible y un componente esencial de su gobierno corporativo, de la gestión de cobranza, de la seguridad de la información y de la relación con clientes, titulares de obligaciones, trabajadores, proveedores, visitantes y demás personas naturales cuyos datos sean tratados por la Compañía.

La presente Política establece las reglas obligatorias que deberán cumplirse durante todo el ciclo de vida de los datos personales, desde su obtención hasta su bloqueo, eliminación o anonimización. Su aplicación comprende los tratamientos automatizados, parcialmente automatizados y no automatizados, así como los efectuados mediante plataformas, bases de datos, archivos físicos, sistemas de comunicación, servicios en la nube, herramientas de inteligencia artificial y proveedores externos.

La Compañía aplicará la Ley Orgánica de Protección de Datos Personales, su Reglamento General y las resoluciones, normas, guías y criterios oficiales de la Superintendencia de Protección de Datos Personales que resulten vigentes y aplicables. Ninguna instrucción comercial, operativa, contractual o jerárquica podrá justificar un tratamiento ilícito, excesivo, opaco o contrario a los derechos de los titulares.

La responsabilidad proactiva exige que POLCOMP no solo cumpla la normativa, sino que pueda demostrarlo mediante registros, análisis de riesgos, evaluaciones de impacto, contratos, trazabilidad, auditorías, controles técnicos, capacitaciones y evidencias de las decisiones adoptadas.

2. OBJETIVO

La presente Política tiene por objeto establecer los principios, responsabilidades, controles y prohibiciones que permitan garantizar un tratamiento lícito, leal,

transparente, seguro, pertinente, proporcional y verificable de los datos personales tratados por POLCOMP CÍA. LTDA.

- Garantizar el ejercicio efectivo de los derechos reconocidos a los titulares por la normativa ecuatoriana.
- Definir responsabilidades concretas para Gerencia, Delegado de Protección de Datos, Legal, Tecnología, Talento Humano, Operaciones, Cobranza, Compras, proveedores y trabajadores.
- Prevenir el contacto indebido con familiares, empleadores, referencias personales, compañeros de trabajo u otros terceros no obligados.
- Asegurar que cada tratamiento tenga finalidad determinada, base de legitimación identificada, origen lícito, plazo de conservación y medidas de seguridad documentadas.
- Integrar la protección de datos desde el diseño y por defecto en procesos, sistemas, contratos, servicios, canales de comunicación y herramientas de inteligencia artificial.

El cumplimiento de esta Política es inmediato y obligatorio. No se entenderá condicionado a una implementación progresiva ni a la disponibilidad futura de recursos.

3. ALCANCE

Esta Política es aplicable a todos los datos personales tratados por POLCOMP, con independencia del soporte, ubicación, formato, origen, canal o tecnología utilizada. Comprende repositorios físicos y digitales, sistemas institucionales, bases de datos, archivos, grabaciones, respaldos, correos electrónicos, telefonía, mensajería, videovigilancia, aplicaciones, servicios en la nube e integraciones con terceros.

Es obligatoria para accionistas, administradores, representantes, trabajadores, pasantes, consultores, gestores de cobranza, proveedores, encargados, subencargados y cualquier persona que acceda a datos personales por cuenta o bajo autorización de la Compañía.

La Política se aplicará cuando POLCOMP actúe como responsable, corresponsable o encargado del tratamiento. Cuando la Compañía adquiera cartera, actúe como cesionaria y decida los fines y medios de la gestión, asumirá la calidad de responsable del tratamiento respecto de sus propias actividades, sin trasladar a la entidad cedente o al proveedor la responsabilidad por sus decisiones, comunicaciones y controles.

4. TÉRMINOS Y DEFINICIONES

Definición	Concepto
Autorización o consentimiento	Manifestación de voluntad libre, específica, informada e inequívoca mediante la cual el titular acepta el tratamiento para una o varias finalidades determinadas. Debe poder demostrarse y retirarse con facilidad.
Base de datos	Conjunto estructurado de datos personales, cualquiera sea su forma, soporte, localización o modalidad de acceso.
Dato personal	Dato que identifica o hace identificable a una persona natural, directa o indirectamente.
Dato sensible	Dato relativo a la esfera íntima del titular cuyo tratamiento indebido puede originar

	discriminación o afectar derechos y libertades fundamentales.
Dato biométrico	Dato personal único obtenido de características físicas, fisiológicas o conductuales que permite o confirma la identificación de una persona, como huellas dactilares, geometría facial o patrones de voz.
Dato crediticio	Dato relacionado con el comportamiento económico, financiero o de cumplimiento de obligaciones de una persona natural. Su uso deberá limitarse a finalidades lícitas y no podrá divulgarse a terceros no autorizados.
Dato de fuente accesible al público	Dato disponible legítimamente al público. Su carácter público no elimina su condición de dato personal ni autoriza su uso indiscriminado; debe existir finalidad, base de legitimación, necesidad y proporcionalidad.
Responsable del tratamiento	Persona natural o jurídica que decide los fines y medios del tratamiento.
Encargado del tratamiento	Persona natural o jurídica que trata datos personales por cuenta del responsable y

	conforme a sus instrucciones documentadas.
Titular	Persona natural a quien corresponden los datos personales.
Tratamiento	Cualquier operación realizada sobre datos personales, automatizada o no, como recolección, registro, consulta, uso, comunicación, cotejo, almacenamiento, modificación, bloqueo, eliminación o destrucción.
Comunicación o transferencia	Entrega, acceso o puesta a disposición de datos personales a un destinatario distinto del titular, conforme al régimen jurídico aplicable.
Transferencia internacional	Comunicación o acceso a datos personales que involucra un destinatario o tratamiento fuera del territorio ecuatoriano, sujeta a las garantías previstas por la normativa vigente.
Anonimización	Proceso aplicado para impedir de forma irreversible la identificación o reidentificación razonable del titular.
Seudonimización	Tratamiento que impide atribuir los datos a una persona sin utilizar información

	adicional, la cual debe conservarse separada y protegida.
Bloqueo	Medida que restringe el acceso y uso de datos cuya finalidad concluyó, pero que deben conservarse únicamente para atender responsabilidades, reclamos o mandatos legales.
Eliminación	Supresión segura y verificable de datos personales en los soportes y sistemas donde se encuentren, conforme a las reglas de conservación y respaldo.
Delegado de Protección de Datos	Persona natural que asesora, supervisa el cumplimiento, coopera con la SPDP y actúa como punto de contacto con la autoridad y los titulares, con independencia funcional.
Destinatario	Persona natural o jurídica a quien se comunican datos personales, sea o no tercero.
Elaboración de perfiles	Tratamiento automatizado destinado a evaluar o predecir aspectos personales, económicos, laborales, conductuales o de localización de una persona.

Evaluación de impacto o EIPD	Proceso previo y documentado para identificar y reducir riesgos altos para los derechos y libertades de los titulares.
Análisis de interés legítimo o LIA	Evaluación documentada que identifica el interés perseguido, verifica necesidad y subsidiariedad, y pondera dicho interés frente a los derechos y expectativas razonables del titular.
Vulneración o incidente de seguridad	Evento que compromete o puede comprometer la confidencialidad, integridad, disponibilidad o resiliencia de datos personales.
Tratamiento a gran escala	Tratamiento que cumple los criterios, umbrales o supuestos directos establecidos por la normativa ecuatoriana vigente.
Sistema de inteligencia artificial	Sistema computacional que genera predicciones, recomendaciones, contenidos o decisiones y que puede involucrar tratamiento de datos personales.
Privacidad desde el diseño y por defecto	Integración de medidas de protección de datos desde la concepción de un tratamiento y configuración

	predeterminada del mínimo dato, acceso, plazo y alcance necesarios.

5. FUNCIONES Y RESPONSABILIDADES PARA LA POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

5.1. GERENCIA GENERAL Y ALTA DIRECCIÓN

- Aprobar esta Política y las actualizaciones que correspondan; asignar recursos humanos, tecnológicos y presupuestarios suficientes.
- Exigir reportes periódicos de cumplimiento y ordenar acciones correctivas ante hallazgos, incidentes o desviaciones.
- Garantizar la independencia funcional del Delegado de Protección de Datos y evitar instrucciones sobre el resultado de sus análisis.
- No aceptar como riesgo residual una práctica manifiestamente ilícita, desproporcionada o contraria a los derechos de los titulares.
- Aprobar los tratamientos de alto riesgo, las EIPD y los planes de remediación que requieran decisión de la alta dirección.

5.2. DELEGADO DE PROTECCIÓN DE DATOS PERSONALES

- Informar y asesorar a POLCOMP sobre sus obligaciones legales y reglamentarias.
- Supervisar la Política, el Registro de Actividades de Tratamiento, las EIPD, los análisis de interés legítimo, los incidentes, las transferencias, los contratos con encargados y los tratamientos mediante inteligencia artificial.
- Emitir recomendaciones independientes y mantener evidencia de su seguimiento. Cuando una recomendación no sea aceptada, la decisión deberá quedar motivada y documentada por el responsable competente.

- Atender y canalizar consultas de titulares y actuar como punto de contacto con la SPDP.
- Supervisar la capacitación y auditoría, sin asumir funciones operativas incompatibles que generen conflicto de interés.

5.3. DEPARTAMENTO LEGAL

- Validar bases de legitimación, deberes de información, contratos, cesiones, encargos, transferencias, respuestas a autoridades y ejercicio de derechos.
- Verificar que los contratos que involucren datos personales incluyan las cláusulas obligatorias y que los proveedores se obliguen a cumplir instrucciones, confidencialidad, seguridad, cooperación y eliminación.
- Coordinar con el DPD la revisión de coherencia entre Política, RAT, EIPD, procedimientos, manuales, avisos y contestaciones.

5.4. DEPARTAMENTO DE SISTEMAS Y TECNOLOGÍA DE LA INFORMACIÓN

- Implementar controles de identidad, acceso, mínimo privilegio, segregación de funciones, cifrado, respaldo, registro, monitoreo, bloqueo y eliminación.
- Mantener trazabilidad de consultas, exportaciones, modificaciones, comunicaciones, accesos y eliminaciones de datos personales.
- Gestionar vulnerabilidades, parches, continuidad, recuperación y pruebas de restauración.
- Reportar inmediatamente al DPD y a Legal cualquier incidente real o sospechado, preservar evidencia y ejecutar medidas de contención.

5.5.OPERACIONES Y GESTIÓN DE COBRANZA

- Utilizar exclusivamente fuentes, guiones, canales y finalidades aprobados.
- Registrar cada intento de contacto, la fuente del dato, destinatario, canal, fecha, resultado y acciones posteriores.
- Detener y escalar la gestión cuando exista duda sobre la identidad del receptor, dato desactualizado, solicitud de no contacto, riesgo de revelar información a terceros o situación no prevista.
- No improvisar mensajes, amenazas, consecuencias jurídicas, ni utilizar cuentas o dispositivos personales.

5.6.TALENTO HUMANO

- Aplicar minimización, confidencialidad y acceso restringido a expedientes laborales, datos de salud y demás categorías especiales.
- Implementar programas formales de capacitación con registro de asistencia, evaluación y evidencia.
- Aplicar medidas disciplinarias proporcionales cuando se incumpla esta Política, sin perjuicio de corregir las causas de proceso o tecnología.
- Adoptar mecanismos no biométricos para el control de asistencia, conforme a la sección específica de esta Política.

5.7.COMPRAS, PROVEEDORES Y ENCARGADOS

- Realizar debida diligencia de privacidad y seguridad antes de contratar o habilitar accesos.

- No permitir tratamiento de datos sin contrato o adenda vigente, instrucciones documentadas y validación técnica.
- Controlar subencargados, ubicación de servicios, transferencias, incidentes y devolución o eliminación al finalizar la relación.

5.8. TRABAJADORES Y COLABORADORES

- Cumplir esta Política, los procedimientos, guiones, controles de acceso y obligaciones de confidencialidad.
- Acceder únicamente a los datos necesarios para sus funciones y no utilizarlos para fines personales o no autorizados.
- Reportar de inmediato errores de envío, accesos indebidos, pérdida de dispositivos, uso no autorizado o cualquier incidente.
- Participar en las capacitaciones y evaluaciones obligatorias.

6. POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

POLCOMP CÍA. LTDA., RUC 0993368991001, con domicilio en Av. Independencia y Antonio Ricaurte y teléfono 072805471, tratará datos personales conforme a los principios y obligaciones establecidos en la normativa ecuatoriana.

La Compañía cuenta con un Delegado de Protección de Datos registrado ante la SPDP. El canal oficial para consultas y ejercicio de derechos es delegadoproteciondatos@polcom.com.ec. Este canal deberá mantenerse activo, visible y unificado en la Política, avisos, procedimientos, contratos y comunicaciones institucionales.

Toda actividad de tratamiento deberá estar identificada en el Registro de Actividades de Tratamiento y contar con finalidad, base jurídica, categorías de titulares y datos, fuente,

destinatarios, plazo de conservación, medidas de seguridad, responsables y evidencia de revisión.

6.1. USO DE DATOS

6.1.1. USO DE DATOS DE CLIENTES, TITULARES DE OBLIGACIONES Y GARANTES

- Gestionar obligaciones vigentes o vencidas, realizar contactos lícitos de cobranza, registrar gestiones, atender acuerdos y ejercer o defender derechos.
- Verificar identidad y datos de contacto mediante fuentes lícitas, documentadas y necesarias.
- Atender reclamos, solicitudes de derechos, requerimientos judiciales, administrativos o de autoridades competentes.
- Prevenir fraude, gestionar riesgos y cumplir obligaciones legales aplicables.
- Realizar comunicaciones comerciales únicamente cuando exista una base de legitimación específica y separada de la gestión de cobranza.

La relación contractual, cesión o titularidad de una obligación puede legitimar el tratamiento del deudor para la gestión de la cartera, pero no legitima automáticamente el tratamiento de familiares, empleadores, referencias o terceros. El tratamiento de estas personas requerirá una base propia y la aplicación de las reglas de la sección sobre contacto con terceros.

6.1.2. USO DE DATOS DE PROVEEDORES Y REPRESENTANTES

- Evaluar, seleccionar, contratar y controlar proveedores y sus representantes.
- Gestionar pagos, facturación, obligaciones tributarias, continuidad, seguridad, calidad y cumplimiento contractual.

- Aplicar controles de prevención de fraude y demás obligaciones legales pertinentes.
- Mantener comunicaciones estrictamente necesarias para la relación comercial.

6.1.3. USO DE DATOS DE TRABAJADORES, CANDIDATOS Y EXTRABAJADORES

- Gestionar selección, contratación, nómina, beneficios, seguridad social, formación, desempeño, seguridad y salud ocupacional y terminación de la relación laboral.
- Cumplir obligaciones laborales, tributarias, de seguridad social, prevención de riesgos y defensa de derechos.
- Controlar el acceso físico y lógico mediante mecanismos proporcionales y preferentemente no biométricos.
- Conservar expedientes durante los plazos legales y bloquearlos cuando la finalidad activa haya concluido.

Los datos de salud, discapacidad, biometría u otras categorías especiales solo podrán tratarse bajo una excepción legal aplicable, con necesidad acreditada, acceso restringido y medidas reforzadas.

6.2. DATOS PERSONALES TRATADOS POR LA COMPAÑÍA

POLCOMP podrá realizar operaciones de recolección, registro, organización, estructuración, consulta, uso, modificación, cotejo, comunicación, conservación, bloqueo, eliminación, destrucción, seudonimización o anonimización, siempre que sean necesarias para una finalidad legítima y estén documentadas en el RAT.

Se prohíbe obtener, enriquecer, combinar o reutilizar datos por el solo hecho de que sean técnicamente accesibles. Cada operación deberá superar los criterios de finalidad, necesidad, pertinencia, minimización y proporcionalidad.

6.3. TIPOS DE DATOS PERSONALES TRATADOS POR LA COMPAÑÍA

- Datos de identificación e identidad: nombres, apellidos, número de identificación, firma y datos de verificación.
- Datos de contacto y comunicaciones: dirección, teléfono, correo electrónico, registros de llamadas, mensajes y gestiones.
- Datos económicos, financieros y crediticios: obligaciones, pagos, saldos, productos, garantías y comportamiento de cumplimiento.
- Datos laborales y profesionales: cargo, historial, remuneración, desempeño, formación y referencias laborales.
- Datos tributarios, comerciales y de proveedores.
- Datos de navegación, acceso, tráfico, metadatos, registros de seguridad e identificadores técnicos.
- Datos de salud y otras categorías especiales únicamente cuando exista habilitación legal y necesidad documentada.
- Datos biométricos solo en los casos excepcionales permitidos por esta Política; nunca como mecanismo ordinario de control de asistencia.

Las categorías concretas tratadas por cada proceso deberán constar en el RAT y en los avisos de privacidad correspondientes. No se utilizarán categorías genéricas para justificar tratamientos excesivos.

6.4. CONSERVACIÓN, BLOQUEO, ELIMINACIÓN, ANONIMIZACIÓN Y SEUDONIMIZACIÓN

- Cada actividad tendrá un plazo o criterio de conservación aprobado y registrado.
- La conservación no dependerá únicamente de la autorización del titular, sino de la finalidad, obligaciones legales, plazos de prescripción, defensa de reclamaciones y demás bases aplicables.
- Al concluir la finalidad, los datos se eliminarán o anonimizarán; si deben conservarse para responsabilidades o mandato legal, se bloquearán y no podrán utilizarse para finalidades incompatibles.
- La eliminación será segura y verificable e incluirá, según corresponda, bases activas, archivos físicos, exportaciones, repositorios, dispositivos y el ciclo de respaldos.
- La seudonimización reduce riesgos, pero los datos seudonimizados continúan siendo datos personales.
- La anonimización deberá ser irreversible y superar una evaluación razonable de reidentificación.

6.5. TRANSFERENCIAS Y COMUNICACIONES DE DATOS PERSONALES

- Antes de comunicar o transferir datos, se documentará finalidad, base jurídica, destinatario, categorías, necesidad, proporcionalidad, garantías y medidas de seguridad.
- Las transferencias internacionales y accesos transfronterizos se sujetarán a la LOPDP, su Reglamento y la Resolución SPDP-SPD-2026-0004-R vigente.

- La contratación de servicios en la nube deberá analizar ubicación, subencargados, acceso remoto, soporte, jurisdicción, seguridad y mecanismo jurídico aplicable.
- Queda prohibido compartir bases por correo personal, enlaces públicos, mensajería no autorizada, dispositivos no controlados o repositorios sin contrato y validación.
- POLCOMP mantendrá un inventario actualizado de comunicaciones, transferencias y accesos de terceros.

6.6. PROTECCIÓN Y SEGURIDAD DE LOS DATOS PERSONALES

- Inventario y clasificación de activos de información y responsables definidos.
- Autenticación robusta, cuentas individuales, mínimo privilegio, segregación de funciones, baja inmediata y revisión periódica de accesos.
- Cifrado en tránsito y, según el riesgo, en reposo, con gestión segura de claves.
- Registros protegidos de acceso, consulta, modificación, exportación, contacto, bloqueo y eliminación.
- Gestión de vulnerabilidades, parches, endurecimiento, monitoreo, prevención de fuga y pruebas de seguridad.
- Copias de seguridad cifradas, segregadas y sometidas a pruebas de restauración.
- Separación de ambientes y uso preferente de datos sintéticos o anonimizados en desarrollo y pruebas.
- Controles de impresión, escritorio limpio, destrucción segura y seguridad física.
- Continuidad del negocio y recuperación ante desastres.

Los controles serán definidos con base en el análisis de riesgos y deberán revisarse cuando cambie la tecnología, finalidad, volumen, proveedor, amenaza o contexto del tratamiento.

6.7. DERECHOS DEL TITULAR DE DATOS PERSONALES

- Información: Recibir información clara, accesible y completa sobre el tratamiento.
- Acceso: Conocer si POLCOMP trata sus datos y obtener la información y copia que corresponda.
- Rectificación y actualización: Corregir datos inexactos, incompletos, desactualizados o erróneos.
- Eliminación: Solicitar la supresión cuando se cumplan las condiciones legales.
- Oposición: Oponerse al tratamiento en los casos previstos por la ley, especialmente cuando se invoque interés legítimo.
- Portabilidad: Recibir o transmitir datos en formato estructurado, de uso común y lectura mecánica cuando proceda.
- Suspensión o limitación: Solicitar la restricción temporal del tratamiento en los casos aplicables.
- Revocatoria: Retirar el consentimiento sin afectar la licitud del tratamiento previo.
- Decisiones automatizadas: Solicitar información, intervención humana, explicación o impugnación cuando corresponda.

Las solicitudes serán gratuitas, accesibles, trazables y atendidas dentro del plazo legal. La verificación de identidad será proporcional al riesgo y no podrá convertirse en una barrera. No se exigirá obligatoriamente un formulario cuando la solicitud contenga información suficiente para identificar al titular y el derecho ejercido.

Cada solicitud tendrá expediente, fecha de recepción, análisis de procedencia, acciones ejecutadas, evidencia técnica y comunicación final motivada. Los encargados y áreas internas deberán cooperar dentro del plazo asignado.

6.8. CONSECUENCIAS DE PROPORCIONAR O DENEGAR DATOS PERSONALES

Cuando un dato sea necesario para ejecutar un contrato, cumplir una obligación legal o prestar un servicio solicitado, la negativa puede impedir o limitar dicho proceso. POLCOMP informará de manera clara cuáles datos son obligatorios y cuáles opcionales.
La negativa a consentir una finalidad opcional, como publicidad no necesaria, no podrá utilizarse para negar un servicio que no dependa de esa finalidad ni para generar consecuencias adversas injustificadas.

6.9. DATOS ERRÓNEOS, INEXACTOS O DESACTUALIZADOS

El titular deberá proporcionar datos veraces cuando los entregue directamente. Sin perjuicio de ello, POLCOMP mantiene la obligación de adoptar medidas razonables de calidad, verificación, actualización y corrección, especialmente antes de realizar comunicaciones de cobranza o afectar derechos.
Cuando una persona manifieste que un número, correo o dirección no corresponde al titular buscado, el dato deberá marcarse, bloquearse para futuras gestiones y ser sometido a verificación. No se continuará utilizando hasta confirmar su exactitud y licitud.

6.10. CULTURA, CAPACITACIÓN Y CONCIENTIZACIÓN

- Todo el personal recibirá capacitación inicial y periódica, diferenciada según sus funciones.

- El equipo de cobranza recibirá formación específica sobre identificación del titular, límites del contacto con terceros, guiones, canales, trazabilidad, incidentes y consecuencias disciplinarias.
- Cada capacitación contará con contenido aprobado, registro de asistencia, evaluación individual, evidencia y acciones de refuerzo cuando corresponda.
- Las directrices verbales no sustituirán procedimientos, manuales, guiones o registros documentados.

6.11. REVOCACIÓN DEL CONSENTIMIENTO

El titular podrá revocar su consentimiento mediante el canal oficial del DPD u otros canales habilitados, de forma gratuita y con una facilidad equivalente a la utilizada para otorgarlo. No será obligatorio solicitar previamente un formulario cuando la voluntad sea clara y pueda verificarse la identidad de manera proporcional.

La revocatoria no tendrá efectos retroactivos y no afectará tratamientos sustentados en otra base de legitimación. POLCOMP deberá identificar qué actividades cesan, cuáles se mantienen y por qué, comunicándolo al titular.

6.12. TRATAMIENTO DE DATOS DE NIÑAS, NIÑOS Y ADOLESCENTES

El tratamiento de datos de niñas, niños y adolescentes será excepcional, respetará su interés superior, capacidad progresiva y derechos, y contará con la habilitación exigida por la normativa. Se aplicarán medidas reforzadas de seguridad, transparencia y minimización.

POLCOMP no realizará perfilamiento comercial, contacto de cobranza, presión, localización ni decisiones automatizadas sobre menores por obligaciones de terceros.

6.13. BASES DE LEGITIMACIÓN Y ANÁLISIS DE INTERÉS LEGÍTIMO

Cada finalidad deberá asociarse a una base de legitimación específica. Se prohíbe utilizar el consentimiento como autorización genérica para cubrir tratamientos que realmente se sustentan en contrato, obligación legal, orden de autoridad, interés público, intereses vitales o interés legítimo.

- Consentimiento válido para una o varias finalidades específicas.
- Cumplimiento de una obligación legal aplicable a POLCOMP.
- Ejecución de medidas precontractuales solicitadas por el titular o de un contrato en el que sea parte.
- Cumplimiento de una orden judicial o de autoridad competente.
- Protección de intereses vitales o ejercicio de funciones de interés público cuando legalmente corresponda.
- Interés legítimo del responsable o de un tercero, siempre que no prevalezcan los derechos del titular.

El interés legítimo no se presumirá. Antes de iniciar el tratamiento se documentará un LIA que identifique el interés real y actual, necesidad, subsidiariedad, expectativas razonables, categorías de datos, impacto, salvaguardas, mecanismo de oposición, conclusión y fecha de revisión.

El LIA deberá ser específico para el tratamiento evaluado. Un análisis orientado al deudor no legitima el tratamiento de un familiar, empleador, referencia o tercero, quienes son titulares independientes y requieren ponderación propia.

6.14. GESTIÓN DE COBRANZA, PROTOCOLO DE ESCALAMIENTO Y CONTACTO CON TERCEROS

Las gestiones de cobro se dirigirán exclusivamente al titular de la obligación o al garante legalmente constituido. Queda prohibido revelar a familiares, referencias, empleadores, compañeros de trabajo, vecinos u otros terceros la existencia, origen, monto, mora, banco cedente, producto, días de atraso, propuestas de pago, medidas judiciales o cualquier dato financiero del titular.

- El contacto excepcional con un tercero solo podrá utilizarse para localizar al titular, cuando exista base jurídica y LIA vigente, y luego de agotar los intentos directos definidos en el protocolo de escalamiento.
- La comunicación se limitará a identificar a POLCOMP y solicitar que el titular se comunique, sin mencionar deuda, cobranza, banco, producto, monto o consecuencias.
- En el primer contacto se facilitará un aviso breve con la identidad del responsable, finalidad de localización y canal del DPD para ejercer derechos.
- No se pedirá al tercero que presione, exhorte, convenza o participe en la regularización de la obligación.
- No se contactará a empleadores o compañeros a través de correos corporativos para gestionar deudas. Cuando un correo laboral pertenezca al propio titular, se aplicarán controles reforzados para evitar exposición a terceros.
- Si el tercero informa que el dato es incorrecto, solicita no ser contactado o existe riesgo de divulgación, el dato será bloqueado de inmediato y el caso se evaluará como posible incidente.

- Los guiones de localización y de cobro serán separados, versionados, aprobados por Operaciones, Legal y DPD, y técnicamente protegidos contra modificaciones no autorizadas.
- Queda prohibido utilizar lenguaje amenazante, humillante, engañoso o afirmar embargos, prohibiciones de salida, retenciones u otras consecuencias no determinadas por autoridad competente.

El sistema deberá conservar evidencia de los intentos previos al titular, la activación del escalamiento, el dato utilizado, su fuente, el contenido enviado, el gestor y el resultado. La falta de registro se considerará incumplimiento de esta Política.

6.15. FUENTES EXTERNAS, PROVEEDORES DE DATOS Y ENRIQUECIMIENTO

- Toda fuente externa deberá ser identificada en el RAT y evaluada antes de su uso.
- POLCOMP verificará la licitud de la obtención, la finalidad original, las categorías, actualidad, calidad, restricciones, deber de información y derecho de oposición.
- Los datos de fuentes públicas no podrán utilizarse de forma indiscriminada ni para finalidades incompatibles.
- Los proveedores de datos complementarios deberán actuar bajo contrato vigente, instrucciones documentadas, seguridad, trazabilidad, asistencia en derechos e incidentes, y obligación de eliminación o devolución.
- Las fuentes históricas deberán revisarse y regularizarse; cuando no pueda demostrarse su licitud, los datos serán suspendidos, bloqueados o eliminados.
- No se contratará ni mantendrá un proveedor cuya procedencia de datos, medidas de seguridad o subencargados no puedan verificarse.

6.16. CONTRATOS, ENCARGADOS Y SUBENCARGADOS

- Todo contrato celebrado en Ecuador que implique tratamiento de datos personales incorporará cláusulas específicas de protección de datos conforme a la Resolución SPDP-SPD-2025-0006-R.
- El contrato definirá objeto, duración, naturaleza, finalidad, categorías, titulares, instrucciones, confidencialidad, seguridad, subencargados, cooperación, auditoría, incidentes, devolución o eliminación y responsabilidad.
- El encargado no podrá usar los datos para fines propios, enriquecer bases, contactar titulares, crear perfiles, vender información o designar subencargados sin autorización.
- La firma contractual no sustituye el control; POLCOMP verificará periódicamente el cumplimiento real del proveedor.
- Los proveedores históricos sin contrato actualizado deberán ser regularizados, suspendidos o sustituidos según el riesgo.

6.17. GESTIÓN DE RIESGOS Y EVALUACIÓN DE IMPACTO

- Cada tratamiento será sometido a análisis de riesgos antes de su inicio y cuando cambien finalidad, tecnología, volumen, categorías, proveedor o contexto.
- Se realizará EIPD previa en tratamientos que puedan generar alto riesgo, incluyendo datos sensibles, biometría, monitoreo sistemático, geolocalización, perfilamiento significativo, inteligencia artificial, comunicaciones masivas o combinación de fuentes.

- La EIPD describirá tratamiento, necesidad, proporcionalidad, riesgos para los titulares, medidas de mitigación, riesgo residual, responsables, plazos y decisión de aprobación.
- La EIPD de cobranza deberá incorporar el LIA para contacto con terceros, el protocolo de escalamiento, las fuentes externas y la referencia al Manual de Gestión de Cobranza.
- Si el riesgo residual permanece alto o crítico y no puede mitigarse razonablemente, el tratamiento no se iniciará o se suspenderá hasta adoptar medidas suficientes y realizar la consulta previa que corresponda.

6.18. TRATAMIENTO DE DATOS PERSONALES A GRAN ESCALA

- Cada actividad se evaluará individualmente conforme a la Resolución SPDP-SPD-2026-0005-R y su modelo técnico.
- La evaluación considerará volumen, número de titulares, categorías, duración, frecuencia, alcance geográfico, combinación de fuentes y efectos sobre los derechos.
- Cuando el tratamiento alcance el umbral o encaje en un supuesto directo, se registrará expresamente, se aplicará gobierno reforzado y se evaluará la obligatoriedad de EIPD, DPD, auditoría y medidas adicionales.
- La calificación de gran escala no se presumirá por el tamaño general de la empresa ni se descartará por analizar actividades de forma agregada.

6.19. TRATAMIENTO DE DATOS BIOMÉTRICOS

Los datos biométricos son datos personales sensibles y su tratamiento está sometido a prohibición general, salvo que concurra una excepción legal y se cumplan de forma

acumulativa los principios de necesidad, pertinencia, minimización, proporcionalidad, seguridad y responsabilidad proactiva.

Para el control de asistencia laboral, POLCOMP no utilizará huellas dactilares, reconocimiento facial, voz u otros datos biométricos como mecanismo ordinario ni obligatorio. La Compañía adoptará métodos menos invasivos, tales como tarjetas, credenciales, códigos individuales, registro en sistemas institucionales u otros mecanismos proporcionales.

Cualquier propuesta excepcional de tratamiento biométrico para una finalidad distinta del control ordinario de asistencia deberá cumplir, antes de su implementación, todos los requisitos siguientes:

- Identificación de una excepción válida del artículo 26 de la LOPDP y documentación de la base de legitimación.
- Test de necesidad y proporcionalidad que demuestre que no existe un medio menos invasivo con eficacia equivalente.
- Análisis de riesgos cuyo resultado no mantenga un riesgo residual alto o crítico.
- EIPD previa, con medidas técnicas, organizativas y jurídicas específicas.
- Evaluación de tratamiento a gran escala cuando corresponda.
- Revisión y recomendación del DPD y aprobación formal de Gerencia, Legal y Tecnología.
- Cuando se invoque consentimiento, opción real, libre y equivalente entre varios mecanismos, sin consecuencias adversas para quien elija la alternativa no biométrica.
- Almacenamiento preferente de plantillas biométricas y no de imágenes crudas, cifrado, segregación, control de acceso, trazabilidad, plazos mínimos y eliminación verificable.

- Prohibición de reutilización para vigilancia, perfilamiento, disciplina, cobranza, análisis emocional, control de productividad u otras finalidades incompatibles.
- Contrato y evaluación de transferencias cuando intervengan proveedores, nube o soporte fuera del Ecuador.

El consentimiento por sí solo no legitimará un tratamiento biométrico desproporcionado ni liberará a POLCOMP de demostrar el cumplimiento de todos los requisitos anteriores.

6.20. INTELIGENCIA ARTIFICIAL, PERFILAMIENTO Y DECISIONES AUTOMATIZADAS

- Todo sistema de inteligencia artificial que trate datos personales deberá registrarse, contar con propietario, finalidad, base jurídica, evaluación de riesgos, control de proveedor, trazabilidad, supervisión humana y documentación suficiente.
- Queda prohibido ingresar bases de cobranza, datos financieros, sensibles, expedientes, credenciales o información confidencial en servicios públicos o no autorizados de inteligencia artificial.
- Antes de usar IA para priorización, scoring, transcripción, análisis de llamadas, generación de comunicaciones o recomendaciones, se evaluarán exactitud, sesgo, explicabilidad, seguridad, impacto y riesgo de decisiones injustas.
- Las decisiones que produzcan efectos jurídicos o significativamente similares no se basarán exclusivamente en tratamiento automatizado cuando el titular tenga derecho a intervención humana, explicación o impugnación.
- Los resultados de IA no se asumirán como verdaderos sin validación humana. El área usuaria mantiene la responsabilidad por la decisión final.

- POLCOMP cumplirá la Resolución SPDP-SPD-2026-0009-R y sus reformas vigentes.

6.21. GESTIÓN Y NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD

- Todo trabajador o proveedor reportará inmediatamente pérdidas, envíos erróneos, accesos no autorizados, malware, exposición, alteración, uso indebido o sospecha de vulneración.
- Tecnología contendrá el incidente y preservará evidencia; el DPD y Legal evaluarán naturaleza, categorías, volumen, titulares, consecuencias, probabilidad y medidas adoptadas.
- POLCOMP mantendrá un registro de todos los incidentes, incluso cuando se concluya que no corresponde notificar.
- Las notificaciones a la SPDP y a los titulares se efectuarán sin dilación indebida y dentro del plazo legal aplicable, con el contenido exigido. La investigación interna no podrá utilizarse para retrasar una notificación obligatoria.
- Las comunicaciones indebidas realizadas por trabajadores serán evaluadas tanto como incumplimiento disciplinario como posible vulneración de seguridad, y se activará el procedimiento correspondiente.

6.22. TRAZABILIDAD, CONTROL DE COMUNICACIONES Y AUDITORÍA

- El sistema deberá impedir que un gestor omita o altere el registro de los contactos realizados.
- Se conservarán evidencias de destinatario, fuente, canal, contenido, fecha, hora, gestor, intentos previos, resultado y bloqueo.

- El DPD supervisará auditorías periódicas de muestras de comunicaciones con titulares y terceros para verificar el cumplimiento de guiones y protocolos.
- Los hallazgos tendrán responsable, prioridad, plazo, evidencia de cierre y validación independiente.
- Las inconsistencias entre Política, RAT, EIPD, contratos, Manual de Cobranza, avisos, procedimientos y comunicaciones deberán corregirse antes de presentar información a la SPDP.

6.23. INCUMPLIMIENTOS Y MEDIDAS DISCIPLINARIAS

- El incumplimiento podrá generar medidas disciplinarias, restricción de acceso, terminación contractual y acciones legales, sin perjuicio de responsabilidades administrativas, civiles o penales.
- Se consideran faltas graves revelar datos de deuda a terceros, usar canales personales, exportar bases sin autorización, alterar registros, ocultar incidentes, desobedecer bloqueos, usar IA no autorizada o reutilizar datos para fines propios.
- La sanción individual no sustituye la obligación de corregir fallas de proceso, tecnología, supervisión o capacitación.
- Queda prohibida cualquier represalia contra quien reporte de buena fe un riesgo o vulneración.

7. ACTUALIZACIONES DE LA POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

Esta Política será revisada al menos una vez al año y siempre que exista cambio normativo, nuevo tratamiento, incidente relevante, resultado de auditoría, modificación

tecnológica, uso de inteligencia artificial, incorporación de proveedor crítico o cambio sustancial en las actividades de cobranza.

Las versiones serán controladas, aprobadas y conservadas. La versión vigente estará disponible en los canales institucionales y las versiones anteriores permanecerán archivadas para fines de trazabilidad.

La continuidad de una relación contractual o del uso de un servicio no se considerará aceptación válida de cambios que requieran consentimiento. Cuando una modificación afecte la información debida al titular o la base de legitimación, POLCOMP realizará la comunicación o recabará el consentimiento que corresponda.

8. BASE LEGAL

Normativa de aplicación directa:

- Constitución de la República del Ecuador, especialmente los artículos 66 numeral 19 y 92.
- Ley Orgánica de Protección de Datos Personales.
- Reglamento General a la Ley Orgánica de Protección de Datos Personales.
- Resolución SPDP-SPD-2025-0003-R: Guía de Gestión de Riesgos y Evaluación de Impacto del Tratamiento de Datos Personales.
- Resolución SPDP-SPD-2025-0006-R: cláusulas de protección de datos personales en contratos celebrados en Ecuador.
- Resolución SPDP-SPD-2025-0022-R: metodología para el cálculo de multas en el régimen sancionatorio.
- Resolución SPDP-SPD-2025-0028-R: Reglamento del Delegado de Protección de Datos Personales.
- Resolución SPDP-SPD-2025-0030-R: seudonimización, anonimización, bloqueo y eliminación.

- Resolución SPDP-SPD-2025-0032-R: adopción de la Guía Panhispánica de Lenguaje Claro y Accesible.
- Resolución SPDP-SPD-2025-0041-R: interés legítimo como base de legitimación.
- Resolución SPDP-SPD-2026-0004-R: transferencias o comunicaciones nacionales e internacionales.
- Resolución SPDP-SPD-2026-0005-R: tratamiento de datos personales a gran escala.
- Resolución SPDP-SPD-2026-0009-R: garantía del derecho de protección de datos en el uso de sistemas de inteligencia artificial, incluidas sus reformas vigentes.
- Oficios SPDP-IRD-2025-0031-O y SPDP-IRD-2025-0065-O, y demás criterios oficiales aplicables al uso de datos biométricos en el control de asistencia.
- Demás resoluciones, guías, circulares, consultas oficiales y normativa ecuatoriana vigente que resulte aplicable a POLCOMP.

Instrumentos de referencia institucional:

El PRI 2025, el Reglamento del Programa Profesionalizante de DPD, el Plan Anual de Auditorías de la SPDP, la conformación del Comité de Protección de Datos de la autoridad, el procedimiento de evaluación de la LOPDP, la normativa sobre actividades familiares o domésticas, las reformas al reglamento de consultas y PAA, la norma de denuncias del DPD, las reformas al estatuto orgánico y la política interna de IA de la SPDP se considerarán únicamente cuando su contenido sea aplicable o aporte criterios de buena práctica. No se presentarán como obligaciones directas de POLCOMP cuando regulen exclusivamente la organización o actuación interna de la SPDP.

La Resolución SPDP-SPD-2025-0024-R se considerará para hechos o periodos en que haya resultado aplicable, sin perjuicio de la aplicación preferente de la Resolución SPDP-SPD-2026-0004-R vigente para transferencias y comunicaciones.

9. APROBACIÓN

La presente versión 2.0 entrará en vigencia únicamente a partir de su aprobación formal por la Gerencia o el órgano societario competente. Su implementación deberá acompañarse de la actualización coherente del RAT, EIPD, LIA, contratos, avisos, procedimientos, guiones, controles tecnológicos y capacitaciones relacionadas.

Certifico que el presente instrumento fue leído, revisado y aprobado por la autoridad competente de POLCOMP CÍA. LTDA., el día 20 de julio de 2026.

_____

Jorge Paul Vicuña Carpio
0102017225
PRESIDENTE
POLCOMP CÍA. LTDA.