

Política regional de protección de datos personales

WE MAKE IT EASY

1. objeto y alcance

Las sociedades identificadas en esta política, que operan bajo la marca B-TECH, protegen los datos personales de clientes, prospectos, trabajadores, candidatos, proveedores, visitantes y usuarios de sus canales digitales. La política comprende recolección, uso, consulta, almacenamiento, comunicación, conservación y eliminación, en soportes físicos o electrónicos.

B-TECH es una marca comercial y no reemplaza la identidad de la sociedad responsable. La entidad que decide la finalidad y los medios del tratamiento responde por él. El aviso específico, formulario o contrato identificará esa entidad. La sociedad contratante no será necesariamente responsable de todos los tratamientos; se determinará el rol real en cada operación. Cuando varias sociedades decidan conjuntamente, documentarán responsabilidades y explicarán al titular cómo ejercer sus derechos.

La legislación aplicable se determina por el ámbito material y territorial de cada norma, el establecimiento y las circunstancias del tratamiento. No depende únicamente de la nacionalidad o residencia del titular. Las reglas de esta política no desplazan normas imperativas ni regímenes sectoriales. Si concurren varias leyes, se atenderán conjuntamente sus obligaciones y se aplicará el plazo más breve que resulte exigible al caso.

Los canales electrónicos comprenden el sitio web, formularios, correo, chat o asistentes virtuales, portales de soporte, redes sociales oficiales, plataformas de eventos y colaboración y, si se habilitan, mensajería empresarial y aplicaciones. Solo se usarán los canales realmente disponibles e identificados por B-TECH. La incorporación de una funcionalidad nueva exige evaluar sus datos, finalidad, proveedor y riesgos y presentar el aviso correspondiente antes de activar el tratamiento.

2. sociedades y canales de atención

Ecuador

Goldconstruc S.A. RUC 0992686324001. Domicilio: Japón E5-25 y Av. Amazonas, Edificio Ferlosant, piso 3, Quito.

Colombia

Goldconstruc SAS. NIT 901607381-6. Domicilio: Carrera 7 # 32-29, oficina 1903, Bogotá D. C.

Perú

Bridgetech SRL. RUC 20611149132. Domicilio: Av. Reducto Nro. 975 URB., Lima. Completar distrito, urbanización y oficina antes de publicar.

Panamá

Goldconstruc Centroamérica SA. RUC 155724808-2-2022 DV 7. Domicilio: Bella Vista, Samuel Lewis, Edificio PH SL 55, apto. 17, oficinas de PGS Integrated Legal Services, Ciudad de Panamá.

Argentina

Bridgetech SRL. CUIT 30719247403. Domicilio: República Árabe Siria 3124, Buenos Aires.

Canal regional de privacidad: datospersonales@b-tech.ai. Sitio web: <https://www.b-tech.ai/>. También se reciben solicitudes escritas en los domicilios indicados. El equipo encargado del canal identifica la sociedad competente y coordina la respuesta sin exigir al titular que conozca la estructura del grupo. Su gestión no sustituye al delegado u oficial de protección de datos cuando su designación sea obligatoria. Sus datos de contacto se incorporarán al aviso aplicable una vez designado.

3. Conceptos y principios

Dato personal es la información que identifica o permite identificar a una persona. Titular es la persona a quien se refiere. Responsable es quien determina las finalidades y medios; encargado es quien trata datos por su cuenta e instrucciones. El consentimiento es una manifestación libre, específica, informada e inequívoca, expresada de forma verificable y con los requisitos adicionales de cada país.

Son datos sensibles o de protección especial aquellos definidos por cada legislación, incluidos datos de salud, origen étnico, convicciones, afiliación sindical y determinados datos biométricos. Las categorías no son idénticas en todos los países. La seudonimización reduce la identificación directa, pero mantiene la condición de dato personal si la persona puede ser identificada; solo la anonimización efectiva excluye esa condición.

Una comunicación a otro responsable y un tratamiento por un encargado tienen requisitos distintos. Los términos transferencia y transmisión se aplican en su sentido local, especialmente en Colombia; no se trasladan automáticamente a otras jurisdicciones. El acceso remoto desde otro país también se evalúa como posible flujo internacional.

Se aplican licitud, lealtad, transparencia, finalidad determinada, proporcionalidad, minimización, exactitud, conservación limitada, seguridad, confidencialidad y responsabilidad demostrada, con protección desde el diseño y por defecto. La información disponible públicamente no es una autorización

universal para reutilizarla.

4. Datos y fuentes

Según la relación y la necesidad, podrán tratarse nombre, identificación, datos de contacto, cargo y empresa; antecedentes profesionales; información contractual, de facturación y pago; solicitudes y registros de soporte; información laboral, nómina y seguridad social; registros de acceso e imágenes de videovigilancia cuando existan; dirección IP, dispositivos, registros de seguridad y preferencias digitales cuando estén habilitados legítimamente.

Los datos proceden del titular, su representante, la organización con la que se relaciona, interacciones con B-TECH y fuentes externas cuya utilización sea lícita. Antes de incorporar datos obtenidos de terceros se verificará su procedencia, la base legal y el deber de información. Cada aviso indicará los campos obligatorios, los voluntarios y las consecuencias concretas de no proporcionar los necesarios. No se solicitarán datos sensibles o financieros innecesarios.

Personas de contacto y datos de terceros

La política protege a las personas naturales que representan o trabajan para clientes y proveedores, aunque la relación comercial sea con una persona jurídica. Los asistentes a eventos, participantes de capacitaciones y usuarios de soporte pueden ser titulares sin haber contratado directamente con B-TECH. La categoría comercial no determina por sí sola la base legal de cada tratamiento.

Si un contacto entrega datos de otras personas, se le solicitará limitar la información a lo necesario y acreditar que su entrega es legítima cuando corresponda. La declaración del remitente no sustituye las verificaciones, avisos o autorizaciones que deba realizar B-TECH. No se incorporará una referencia de tercero automáticamente a campañas comerciales.

5. Finalidades y legitimación

Cada tratamiento tendrá una finalidad específica y una base legal documentada conforme al país. El consentimiento no se presume por navegar, guardar silencio o aceptar esta política. La existencia de un contrato no permite cualquier tratamiento; las excepciones legales deben verificarse de forma individual. El interés legítimo solo se empleará donde sea reconocido y tras la evaluación exigible, sin importarlo como excepción general a países que no lo contemplen de la misma forma.

Clientes y proveedores

Gestionar solicitudes de servicio, evaluación de proveedores, contratación,

ejecución, soporte, facturación, cobro, pagos y cumplimiento de obligaciones fiscales o regulatorias. Se tratarán los datos necesarios con consentimiento o con la excepción legal correspondiente. Los avisos distinguirán estas finalidades de las campañas comerciales opcionales.

Trabajadores y candidatos

Gestionar selección, contratación, nómina, seguridad social, formación, prevención de riesgos y obligaciones laborales. Las referencias y verificaciones se limitarán a lo pertinente y permitido. Conservar currículos para futuras vacantes, divulgar fotografías o utilizar datos en programas opcionales requiere una legitimación diferenciada; no se condicionará el empleo a usos innecesarios.

Prospectos y comunicaciones comerciales

Atender solicitudes de información y, cuando exista legitimación específica, enviar novedades, invitaciones y campañas relacionadas con los intereses informados. El marketing, la nutrición de contactos, la segmentación y el remarketing son finalidades opcionales que deben explicarse separadamente. Cada comunicación identificará a la sociedad remitente y permitirá darse de baja por un mecanismo sencillo y gratuito. La baja se aplicará a las campañas y se conservará solo la información mínima necesaria para respetarla.

Seguridad y canales digitales

Proteger instalaciones y sistemas, prevenir fraude, atender consultas y gestionar formularios y conversaciones de soporte. La videovigilancia se informará con señalización previa y aviso accesible; se evitarán zonas íntimas y captaciones excesivas. Las grabaciones, analítica, cookies y chatots se comunicarán en el punto de interacción con su finalidad y conservación.

Eventos y actividades de formación

Gestionar inscripciones, asistencia, comunicaciones logísticas, certificados y atención de participantes en eventos o capacitaciones. El aviso del evento distinguirá estos usos de las futuras campañas. El uso publicitario de imágenes, voz, testimonios o grabaciones identificables contará con información y legitimación específicas sobre medios y finalidad; asistir al evento no equivale a aceptar su difusión. Si existe una alternativa razonable para participar sin aparecer en contenidos publicitarios, se comunicará al asistente.

Las comunicaciones necesarias para cotizaciones solicitadas, contratos, soporte, seguridad o logística se diferencian de la publicidad. La baja comercial no bloqueará avisos indispensables y legítimos para la relación vigente. Esos mensajes operativos no se utilizarán para introducir promociones que carezcan de legitimación.

6. Información y consentimiento

Antes de recoger datos se facilitará un aviso comprensible que identifique al responsable, contacto, datos y fuentes, finalidades y base legal, destinatarios, flujos internacionales, conservación y derechos. También se informarán las decisiones automatizadas y el contacto del delegado u oficial cuando corresponda. Si los datos se obtienen indirectamente se cumplirá el deber de información en la oportunidad exigida por la ley aplicable.

El consentimiento se obtiene mediante una acción afirmativa verificable, sin casillas premarcadas ni autorizaciones indiscriminadas. Puede documentarse en formularios, contratos, plataformas o grabaciones cuando el medio cumpla la norma local. Se conservará evidencia del aviso presentado, su versión, la fecha y la acción del titular. Los usos opcionales tendrán opciones separadas y la negativa no impedirá prestar servicios que no necesiten esos datos.

El titular puede retirar el consentimiento mediante el canal de privacidad o el mecanismo habilitado. La retirada no afecta la licitud previa, pero obliga a cesar el uso basado en ella, salvo que exista otra base legal válida que se explique. Una nueva finalidad incompatible requiere nueva información y, cuando corresponda, una nueva autorización; actualizar la política no la reemplaza.

Avisos en el punto de interacción

Los formularios, flujos de registro y canales de atención presentarán información breve y un enlace visible al aviso completo antes de enviar los datos. El aviso detallará el responsable y la finalidad concreta del canal. En chat y mensajería se advertirá si interviene un asistente automatizado, si se conserva la conversación y cómo solicitar atención humana; también se indicará qué información no debe compartirse por ese medio.

Necesidad de los datos y consecuencias de la negativa

Si falta un dato realmente necesario, B-TECH explicará qué solicitud o prestación no puede completar y por qué. Por ejemplo, la ausencia de un medio de contacto puede impedir responder una cotización y la falta de datos fiscales necesarios puede impedir emitir una factura conforme a la ley. Rechazar publicidad, cookies opcionales o una publicación de imagen no impedirá acceder a un servicio que pueda prestarse sin esos usos. Se ofrecerán medios alternativos razonables cuando proceda.

Se facilitará corregir información inexacta. Las obligaciones del titular de comunicar datos veraces no liberan a B-TECH de verificar calidad y proporcionalidad ni trasladan al titular toda responsabilidad por el tratamiento.

Evidencia de actuaciones electrónicas

La contratación, firma y aceptación por medios electrónicos se gestionarán bajo la legislación aplicable y los mecanismos de identidad e integridad pertinentes. Una clave, una sesión autenticada o el acceso al sitio no prueban por sí solos consentimiento para todas las finalidades. Se distinguirá la aceptación contractual, la constancia de haber recibido el aviso y las autorizaciones opcionales. No se impondrá una renuncia anticipada a derechos mediante términos digitales.

En Colombia, la autorización podrá constar por escrito, oralmente o mediante una conducta inequívoca admitida por la ley que permita concluir razonablemente que fue otorgada; el silencio no constituye autorización. B-TECH conservará una prueba consultable, vinculada a la persona, al texto informado, las finalidades y el momento de obtención. Los usos nuevos que requieran autorización se someterán a una solicitud adicional antes de iniciarse; no se entenderán aceptados por actualizar esta política.

7. Datos sensibles y de menores

Los datos sensibles se tratarán solo si se cumplen las condiciones específicas de la legislación aplicable. El consentimiento, cuando sea admisible, será explícito y separado; en Perú se observará el requisito escrito aplicable. En Argentina no se considerará suficiente el consentimiento para cualquier uso de datos sensibles: se verificarán las restricciones y habilitaciones del artículo 7 de la Ley 25.326. En Colombia se informará el carácter facultativo de responder preguntas sensibles y se evitará condicionar actividades a su entrega.

B-TECH no dirige campañas a menores. Si un tratamiento legítimo requiere sus datos, se documentará previamente el interés superior, la necesidad, las reglas locales de capacidad y representación y, cuando proceda, la autorización del representante y la participación del menor según su madurez. No se usará una edad de consentimiento única para toda la región. En Colombia se observarán las restricciones del artículo 7 de la Ley 1581 y su interpretación constitucional. Las medidas reforzadas incluyen acceso limitado, avisos comprensibles y ausencia de usos publicitarios incompatibles.

Antes de utilizar biometría se evaluarán necesidad, proporcionalidad, riesgos y alternativas menos intrusivas. Se cumplirán las normas especiales del país; esta política no autoriza por sí sola reconocimiento facial ni controles biométricos.

8. Proveedores y servicios por cuenta de clientes

Se podrá acudir a proveedores de infraestructura, correo, gestión comercial, soporte y servicios profesionales únicamente con los datos necesarios y bajo legitimación válida. Cada aviso precisará destinatarios o categorías y, cuando sea obligatorio, su identidad. Compartir datos con otra sociedad de B-TECH o un

aliado exige la misma revisión jurídica que compartirlos con cualquier tercero.

Los contratos con encargados establecerán objeto, duración, finalidad, instrucciones, categorías de datos y titulares, confidencialidad, seguridad, subcontratación, asistencia en derechos e incidentes, auditoría y devolución o eliminación al terminar. No basta un acuerdo de confidencialidad. Se controlarán subencargados, ubicaciones y accesos, y se verificarán las garantías antes de habilitarlos.

Cuando B-TECH implemente, migre, aloje, administre o soporte sistemas de un cliente, tratará los datos de ese cliente según su rol real y contrato. Si actúa como encargado, seguirá instrucciones documentadas y no reutilizará expedientes, documentos, registros o datos de usuarios para marketing, pruebas o entrenamiento de modelos. Las solicitudes de titulares se remitirán y asistirán oportunamente al cliente responsable, sin desconocer obligaciones legales directas. Los ambientes de pruebas utilizarán datos sintéticos o anonimizados siempre que resulte posible.

Destinatarios y requerimientos de autoridades

Los avisos identificarán, según el tratamiento real, proveedores de alojamiento y respaldo, correo y colaboración, CRM y automatización comercial, analítica, mensajería, soporte, seguridad y asesores legales o contables. En eventos conjuntos se indicará qué organizadores reciben datos y con qué rol. Si un fabricante o aliado actúa como responsable independiente para sus propios fines, se informará esa circunstancia y se verificará la legitimación de la comunicación; no se lo calificará automáticamente como encargado.

Antes de atender un requerimiento de autoridad, B-TECH verificará competencia, fundamento, alcance y autenticidad; entregará solo lo exigible mediante un canal seguro y conservará evidencia. Informará al titular cuando corresponda y no exista prohibición legal. Una política interna o una petición informal no constituyen por sí solas una obligación legal de revelar datos.

B-TECH evaluará a los encargados antes de contratarlos y verificará durante la relación, de acuerdo con el riesgo, sus medidas, subcontrataciones y cumplimiento. Solicitará evidencias pertinentes y acordará revisiones o auditorías proporcionadas. Las rectificaciones, supresiones y restricciones procedentes se comunicarán a los encargados y destinatarios conforme a la ley; se conservará evidencia de ejecución. La confidencialidad del personal y proveedores continuará después de terminar su vinculación.

9. Transferencias internacionales

Antes de un flujo internacional se documentarán país de origen y destino, importador, finalidad, rol, datos y mecanismo jurídico admisible. Se verificará el nivel de protección y se adoptarán las garantías, contratos, autorizaciones o excepciones que permita la ley aplicable. El consentimiento general de esta política no legitima todas las transferencias.

Las garantías se revisarán también para respaldos, soporte remoto, subencargados y accesos entre filiales. Los avisos específicos identificarán los destinos y mecanismos con el detalle legalmente requerido. No se afirmará que un país es adecuado sin comprobar la decisión vigente de la autoridad competente. Las disposiciones nacionales de la sección 15 complementan esta regla.

10. Cookies e inteligencia artificial

Las cookies estrictamente necesarias se identificarán y limitarán a su función. Como estándar interno de B-TECH, las cookies analíticas, de personalización opcional y publicitarias se bloquearán hasta obtener una elección afirmativa cuando traten datos personales. Se ofrecerán opciones claras para aceptar, rechazar y configurar, y para retirar la elección con facilidad equivalente. El aviso de cookies describirá finalidad, proveedor, duración y flujos internacionales. Cambiar la configuración del navegador no sustituye estos mecanismos.

El uso de IA se limita a finalidades informadas y legítimas. Antes de cada uso se evaluarán riesgos, datos requeridos, proveedor, seguridad, transferencias, conservación y uso para entrenamiento. No se cargarán datos de clientes ni categorías sensibles en herramientas sin autorización contractual y controles válidos. La seudonimización no exime del cumplimiento.

Cuando una decisión automatizada pueda producir efectos jurídicos o afectar significativamente a una persona, se ofrecerán información comprensible, intervención humana efectiva y vías de impugnación en los casos exigidos por la ley. Un chatbot no deberá solicitar datos innecesarios ni ocultar tratamientos adicionales. Se realizarán evaluaciones de impacto y consultas previas cuando sean obligatorias. En Ecuador se aplicará la normativa de la SPDP sobre IA y sus reformas vigentes.

Permisos de dispositivos y plataformas externas

Si una funcionalidad utiliza cámara, micrófono, geolocalización o contactos del dispositivo, solicitará únicamente el permiso necesario, en el momento de uso, explicando finalidad y duración. Como estándar interno, no se accederá a la libreta completa de contactos ni a ubicación precisa para una atención ordinaria que pueda realizarse sin ello. El permiso técnico del dispositivo no reemplaza el consentimiento u otra legitimación jurídica exigida. La retirada se gestionará sin afectar funcionalidades independientes.

Las integraciones con plataformas externas se identificarán antes de redirigir o comunicar datos. Se explicará el responsable de cada tratamiento y dónde consultar su aviso. B-TECH mantiene sus obligaciones por lo que recoge y comunica; el aviso de un tercero no las elimina. Las consultas públicas en redes sociales se trasladarán a un canal privado seguro cuando requieran datos personales; no se expondrá en respuestas públicas información de clientes o de terceros.

Perfiles y funcionamiento de la IA

Si se habilita segmentación o puntuación de prospectos, se informará la finalidad, los datos utilizados y las opciones de oposición o retiro que correspondan. No se reutilizarán datos de soporte, trabajadores o expedientes de clientes para crear audiencias comerciales sin una legitimación propia. La finalidad y base legal de la IA se evaluarán por operación; alojarla dentro de Ecuador no convierte automáticamente en interés legítimo una actividad que exigiría consentimiento.

Para decisiones automatizadas alcanzadas por la ley, la información incluirá la intervención del sistema, los factores principales, el origen y tipos de datos y las consecuencias previsibles, con detalle suficiente para ejercer derechos. La revisión humana será realizada por una persona con capacidad de reconsiderar el resultado. Si B-TECH provee IA como encargado, facilitará al cliente la información de funcionamiento, limitaciones, riesgos y controles necesaria para cumplir sus obligaciones, preservando las reservas legales legítimas.

En Colombia, antes de usar datos personales en sistemas de IA, B-TECH evaluará la necesidad, proporcionalidad, calidad de los datos y riesgos para los titulares y aplicará medidas preventivas desde el diseño. Documentará la evaluación de impacto cuando corresponda, controles de seguridad, transparencia y mecanismos de intervención humana. Una autorización para prestar soporte no habilita por sí sola entrenar modelos para usos propios o de un tercero.

11. Seguridad e incidentes

B-TECH implementará medidas proporcionales al riesgo, incluidos controles de acceso por funciones, autenticación reforzada cuando corresponda, cifrado adecuado, registros de actividad, respaldos verificados, gestión de vulnerabilidades, capacitación y compromisos de confidencialidad. Se revisarán periódicamente y se documentará su eficacia. Esta política no declara una certificación ISO ni garantiza ausencia de incidentes.

Todo incidente se escalará sin demora al equipo de seguridad y privacidad,

preservando evidencia y la fecha de conocimiento. Se evaluarán los datos, personas, países y riesgos afectados; se contendrá el incidente y se documentarán las decisiones de notificar o no. Las comunicaciones a autoridades, titulares y clientes se harán según los destinatarios, supuestos y plazos de cada jurisdicción, sin esperar a cerrar la investigación. Los contratos podrán fijar avisos al cliente más breves que los máximos legales.

Se recomienda a los usuarios utilizar canales oficiales y proteger sus credenciales, códigos temporales y dispositivos; no deberán enviar contraseñas ni secretos de acceso por formularios o conversaciones de atención. B-TECH habilitará un medio para reportar accesos sospechosos. Estas recomendaciones complementan las medidas de B-TECH y no reducen su responsabilidad legal.

12. Conservación y eliminación

Los datos se conservarán por el tiempo necesario para la finalidad y las obligaciones legales concretas. La sociedad responsable documentará un calendario por categoría, con duración o criterio objetivo, fundamento y revisión; el aviso específico comunicará al titular el plazo o criterio aplicable. No se conservarán indefinidamente bajo una referencia genérica a posibles necesidades futuras.

Al terminar la necesidad se eliminarán o anonimizarán de forma verificable. Si existe deber legal, litigio o conservación legítima, se restringirá su acceso y uso a esa finalidad. Los respaldos seguirán un ciclo definido y no reactivarán datos eliminados al restaurarse. La baja comercial no obliga a borrar facturas que deban conservarse ni permite continuar enviando campañas.

El calendario de conservación distinguirá expedientes contractuales, registros de soporte, conversaciones y grabaciones, contactos comerciales, evidencias de consentimiento y logs de seguridad. Cada categoría tendrá un plazo o criterio propio; las grabaciones de oficinas no adoptarán automáticamente el plazo de 90 días del banco. La conservación de evidencia de una autorización no habilita a mantener activos todos los datos utilizados en la campaña.

13. Ejercicio de derechos

El titular podrá solicitar información, acceso, rectificación, actualización, eliminación o cancelación y retirar el consentimiento. Podrá ejercer oposición, portabilidad, suspensión u otros derechos cuando los reconozca la ley aplicable y se cumplan sus condiciones. También podrá solicitar prueba de autorización en los casos previstos. La negativa será motivada, parcial si procede, e indicará la vía de reclamación.

Las solicitudes se envían a datospersonales@b-tech.ai o al domicilio de la sociedad responsable, indicando nombre, medio de respuesta y petición clara. Se verificará identidad o representación por medios proporcionales; no se exigirán copias documentales innecesarias ni formalidades que la ley no establezca. Solo se requerirá soporte adicional pertinente a la solicitud. Se entregará información de manera segura sin revelar datos de terceros.

La atención es gratuita con el alcance de la ley local. Se registrará la recepción y se aplicarán los términos de la sección 15. Las subsanaciones y prórrogas solo procederán si la legislación las admite y se comunicarán con motivo y fecha. No se aplicará una ampliación colombiana a una solicitud sujeta a otro país.

El titular puede precisar si su petición afecta un canal o finalidad concretos o todos los tratamientos alcanzados. B-TECH confirmará recepción y alcance cuando resulte necesario y coordinará la ejecución en los sistemas correspondientes. El retiro podrá efectuarse por mecanismos sencillos equivalentes al medio de obtención, además del correo de privacidad, sin exigir siempre una carta firmada. Una denegación se sustentará en una excepción legal identificada y en hechos verificables, no en referencias genéricas a intereses de la compañía o investigaciones internas.

14. Gobierno y vigencia

Cada sociedad asignará una función de privacidad, mantendrá inventarios y evidencias, revisará tratamientos y proveedores y realizará registros, evaluaciones y designaciones obligatorias según su actividad. La función regional coordina y no elimina la responsabilidad local. Si se designa un delegado u oficial obligatorio, se garantizarán sus requisitos de independencia, recursos y ausencia de conflictos.

La versión propuesta entrará en vigor en la fecha de aprobación y publicación que determine B-TECH: [completar]. No se atribuye efecto retroactivo al 1 de enero de 2026. Las modificaciones relevantes se comunicarán por medios adecuados y se mantendrá evidencia de las versiones. La política estará disponible permanentemente en el sitio web y por el canal de atención.

Los administradores y responsables internos asignarán recursos, funciones, formación y seguimiento para demostrar cumplimiento. Se revisarán los cambios de propósito, destinatarios y tecnología antes de su implementación. Las políticas complementarias, como cookies y uso de IA, serán coherentes con esta política; una actualización material se comunicará por un medio accesible y no ampliará retroactivamente una autorización.

15. Disposiciones nacionales

Ecuador

Se aplican la LOPDP, su Reglamento General expedido mediante Decreto Ejecutivo 904 y las resoluciones vigentes de la SPDP, incluidas las relativas a transferencias, delegado, interés legítimo, IA, biometría y vulneraciones, según corresponda. El catálogo de normas y la reforma de mayo de 2026 deben leerse conjuntamente.

Se atienden acceso, rectificación, actualización, eliminación y oposición dentro del plazo legal de 15 días, con las condiciones de cada derecho; se garantizan asimismo portabilidad, suspensión y las garantías frente a decisiones automatizadas que correspondan. El titular puede acudir a la Superintendencia de Protección de Datos Personales, conforme al procedimiento aplicable.

Las transferencias se revisarán bajo la norma general vigente de la SPDP. Se evaluará y documentará si corresponde designar y registrar delegado y cumplir las obligaciones del registro nacional. Para vulneraciones se aplicará el artículo 43 reformado: notificación tan pronto como sea posible y como máximo en el término de cinco días a los destinatarios legales, salvo la excepción de riesgo improbable; el encargado avisará al responsable tan pronto sea posible y dentro del término máximo de dos días. El titular será informado sin dilación y dentro del término de tres días desde conocimiento del riesgo, sujeto a las excepciones legales. La notificación a la SPDP utilizará el SISDPDP conforme a la norma técnica vigente.

Para Ecuador, la finalidad solicitada por el titular puede apoyarse en medidas precontractuales o ejecución contractual cuando concurren los requisitos legales; facturación y reportes se vinculan a la obligación concreta aplicable; los usos opcionales requieren su propia legitimación. Si se propone interés legítimo, se documentarán interés, necesidad, ponderación y salvaguardas bajo la normativa vigente. No se justificará todo el marketing o la difusión de imágenes con esa base por analogía con una entidad financiera.

En Ecuador, el titular puede oponerse a la mercadotecnia directa y sus perfiles. La suspensión permite limitar usos, por ejemplo mientras se comprueba un dato impugnado; la portabilidad facilita recibir datos en formato interoperable o transmitirlos si procede. Las condiciones y exclusiones de estos derechos se revisarán individualmente. Respecto de decisiones única o parcialmente automatizadas comprendidas en la LOPDP, podrá solicitar explicación, presentar observaciones e impugnar. No se condicionará su ejercicio a una aceptación general del canal.

Colombia

Se aplican la Ley 1581 de 2012 y el Decreto 1074 de 2015, que compila la reglamentación pertinente, además de instrucciones de la SIC. Si se tratan datos sometidos a hábeas data financiero u otro régimen especial, se aplicará también su normativa específica. No se invocará interés legítimo como excepción general a la autorización.

Consultas: diez días hábiles desde recepción; ampliación motivada hasta cinco días hábiles adicionales. Reclamos: quince días hábiles desde el día siguiente de recepción; ampliación motivada hasta ocho días hábiles adicionales. Si está incompleto se requiere subsanación dentro de cinco días; tras dos meses sin respuesta se entiende desistido. El incompetente remite en dos días hábiles. Recibido el reclamo completo se incorpora la leyenda reclamo en trámite en dos días hábiles y se mantiene hasta decidir. Antes de quejarse ante la SIC debe agotarse la consulta o reclamo correspondiente.

Las transferencias internacionales cumplen el artículo 26 de la Ley 1581; las transmisiones a encargados se documentan con el contrato exigible. Se verificará la obligación de inscribir y actualizar el RNBD según los umbrales y condiciones vigentes. La ausencia de obligación de registro no elimina los deberes de seguridad, derechos y reporte de incidentes. Estos se reportarán a la SIC por el canal correspondiente dentro de los quince días hábiles siguientes a su detección y puesta en conocimiento del área encargada, conforme a las instrucciones vigentes.

En Colombia, los derechos podrán ejercerse por el titular, sus causahabientes, representante o apoderado con acreditación suficiente, y mediante estipulación a favor de otro o para otro conforme a la ley. Los representantes habilitados ejercerán los derechos de niños, niñas y adolescentes. Un interés comercial o una relación con el titular no autorizan por sí solos a acceder a sus datos.

El titular podrá solicitar prueba de su autorización, salvo excepción legal, información sobre el uso y acceso gratuito en las condiciones normativas. La revocatoria puede limitarse a finalidades opcionales; la conservación legal o contractual de un expediente no habilita a mantener publicidad. B-TECH identificará los datos y deberes concretos que justifiquen conservar información y restringirá los usos restantes.

La información visible en internet no se tratará automáticamente como dato público. Se verificará su naturaleza jurídica y la finalidad permitida. Los datos privados, semiprivados y sensibles tendrán controles acordes; la autorización general no sustituye los requisitos especiales de los sensibles. Para menores se respetarán su interés superior y derechos fundamentales, se escuchará su opinión según madurez y se obtendrá la autorización del representante cuando

proceda.

Las transferencias internacionales se verificarán bajo el artículo 26 de la Ley 1581 y las instrucciones vigentes de la SIC: nivel adecuado reconocido, excepción legal aplicable o declaración de conformidad cuando corresponda. Un contrato o la pertenencia al mismo grupo no sustituyen esos requisitos. La transmisión a un encargado se documentará conforme a su régimen propio. La simple revisión privada de la ley extranjera no equivale a reconocer un nivel adecuado.

Perú

Se aplican la Ley 29733 y el Reglamento aprobado por Decreto Supremo 016-2024-JUS, que sustituye al reglamento anterior. Se identificará en cada aviso el banco de datos correspondiente y se efectuarán su inscripción y actualizaciones y las comunicaciones de flujos transfronterizos exigibles. Las transferencias requieren la protección y garantías admitidas por la normativa peruana.

Plazos: información, ocho días hábiles; acceso, veinte; rectificación, cancelación y oposición, diez, contados desde el día siguiente a la solicitud. Las ampliaciones solo se usarán bajo condiciones legales. Se reconoce la portabilidad dentro del alcance reglamentario del acceso. La autoridad competente es la Autoridad Nacional de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos.

Los incidentes comprendidos en el artículo 34.1 se notifican a la ANPD en un máximo de 48 horas desde conocimiento; los avisos al titular y al Centro Nacional de Seguridad Digital se realizan cuando corresponda. Se evaluará la designación del oficial de datos personales y el calendario transitorio aplicable a B-TECH, sin presumir su categoría por tamaño o ventas.

En comunicaciones comerciales a consumidores se aplicará también la Ley 32323 y el Código de Protección y Defensa del Consumidor: se exigirá consentimiento previo, expreso y por iniciativa del consumidor. No se utilizará la llamada inicial del reglamento como habilitación para eludir esta restricción posterior. La revocación se hará efectiva conforme al régimen aplicable.

Panamá

Se aplican la Ley 81 de 2019 y el Decreto Ejecutivo 285 de 2021. Se garantizan acceso, rectificación, cancelación, oposición y portabilidad conforme a sus condiciones. El acceso se atiende en diez días hábiles y la rectificación en cinco días hábiles. Para otros derechos se aplicará su término legal; como compromiso interno adicional se procurará resolverlos en cinco días hábiles, sin ampliar un plazo legal más breve.

El titular podrá acudir a la Autoridad Nacional de Transparencia y Acceso a la Información, por los canales publicados en antai.gob.pa. Las comunicaciones internacionales y las relaciones con custodios observarán las garantías de la ley y su reglamento. El plan de incidentes incorporará las notificaciones exigibles; no se trasladará automáticamente a Panamá el plazo europeo de 72 horas. Se evaluará la figura de oficial conforme a los supuestos aplicables.

Argentina

Se aplican la Ley 25.326, el Decreto 1558 de 2001 y las disposiciones vigentes de la AAIP. El acceso se contesta en diez días corridos; rectificación, actualización o supresión, en cinco días hábiles. El acceso gratuito puede ejercerse a intervalos no inferiores a seis meses, salvo interés legítimo acreditado conforme al artículo 14. Las condiciones de supresión respetan las obligaciones de conservación y los derechos de terceros.

La Agencia de Acceso a la Información Pública, como órgano de control de la Ley 25.326, atiende denuncias y reclamos por incumplimientos en protección de datos personales. El titular conserva la acción de hábeas data. En publicidad puede pedir retiro o bloqueo de sus datos; las comunicaciones incorporarán los avisos exigidos por las disposiciones aplicables.

Se cumplirán los registros exigibles y el artículo 12 sobre transferencias internacionales, con las decisiones de adecuación o garantías contractuales admitidas. Un acuerdo genérico de confidencialidad no reemplaza esas garantías. Los datos sensibles se sujetan a las restricciones legales específicas. El protocolo de incidentes verificará obligaciones sectoriales y contractuales; no presume un plazo general de 72 horas derivado de la Ley 25.326.