



AVISO DE PRIVACIDAD DE SEGUNDA CAPA

**FRANQUICIAS ALIMENTICIAS FRANCEB CIA. LTDA.
LCR PRODUCTOS & SERVICIOS CIA. LTDA.**

Versión 1.0

El auténtico sabor del mar
DIRECTO A TU MESA

Aviso de privacidad de segunda capa

Este aviso informa de manera completa y transparente cómo FRANQUICIAS ALIMENTICIAS FRANCEB CIA. LTDA. (FRANCEB) y LCR PRODUCTOS & SERVICIOS CIA. LTDA. (LCR), cada una como responsable dentro del ámbito de sus respectivas competencias, tratan datos personales vinculados con la operación de la marca “Los Cebiches de la Rumiñahui”. El aviso desarrolla los contenidos exigidos por el artículo 12 de la Ley Orgánica de Protección de Datos Personales (LOPD) y se complementa con las políticas generales de protección de datos de cada responsable, la Política de Cookies, los Términos y Condiciones, el Procedimiento para el Ejercicio de Derechos y el Formulario ARSO+.

Regla de responsabilidad por ámbito

FRANCEB concentra principalmente los tratamientos relativos a comercialización, canales de venta, sitio web, comercio electrónico, call center, aplicaciones de delivery, marketing, administración de franquicias y proveedores del franquiciador. LCR concentra principalmente los tratamientos relativos a producción, bodega, fábrica, administración operativa, recursos humanos, nómina, salud ocupacional, ERP, seguridad física, CCTV y control de accesos. Cuando un tratamiento involucre a ambas entidades, cada una responderá por las operaciones que determine o ejecute dentro de su ámbito, y el DPD coordinará la atención de los titulares cuando resulte necesario.

1. Fines del tratamiento

1.1. Pedidos, ventas y atención comercial. FRANCEB trata datos para gestionar compras presenciales y digitales, tomar y administrar pedidos, identificar al cliente o destinatario, asignar locales, coordinar entrega o retiro, gestionar cambios, anulaciones, devoluciones, reclamos, garantías, incidencias y atención postventa.

1.2. Sitio web y comercio electrónico. FRANCEB trata datos para crear y administrar cuentas de usuario, facilitar futuros pedidos, gestionar direcciones, historial de compras, carrito, recuperación de cuenta, seguridad de sesión, soporte, conciliación del pedido y mejora funcional del canal web.

1.3. Call center, WhatsApp, mensajería y redes sociales. FRANCEB trata datos para atender llamadas, mensajes y consultas, tomar pedidos, brindar soporte, gestionar reclamos, mantener trazabilidad de la atención, escalar incidentes y solicitudes de derechos, y grabar o monitorear llamadas cuando corresponda para calidad, seguridad y defensa.

1.4. Facturación, pagos y obligaciones tributarias. FRANCEB y LCR, en el ámbito que corresponda, tratan datos para emitir comprobantes electrónicos, validar y conciliar pagos, gestionar retenciones, soportes contables, impuestos, reportes fiscales, requerimientos de autoridad y defensa de reclamaciones. Los datos de tarjetas son procesados por pasarelas autorizadas y no se solicitan ni almacenan CVV, PIN o claves bancarias por canales generales.

1.5. Aplicaciones de delivery. FRANCEB trata datos recibidos desde Uber Eats, Rappi, PedidosYa u otras plataformas autorizadas para recibir, preparar, coordinar, facturar, entregar, conciliar, atender novedades y reclamos, y analizar el desempeño del canal.

1.6. Marketing, fidelización y comunicaciones comerciales. FRANCEB trata datos para administrar campañas, email marketing, telemarketing, promociones, programas de fidelización, segmentación comercial, seguimiento de clientes, medición de campañas, eventos, activaciones, encuestas, gestión de leads, redes sociales y remarketing cuando exista base jurídica válida.

1.7. Cookies, analítica y geolocalización. FRANCEB trata datos técnicos y de navegación para operar el sitio, mantener seguridad, recordar preferencias, medir uso y conversión, mejorar la experiencia y, cuando el titular lo active, utilizar ubicación para localizar sucursales, calcular rutas o verificar cobertura. Las cookies no necesarias y las tecnologías de seguimiento o publicidad se sujetan a la Política de Cookies y a las preferencias del titular.

1.8. Franquicias. FRANCEB trata datos de candidatos a franquiciado, franquiciados, representantes, contactos y personal vinculado para gestionar solicitudes, evaluación, negociación, contratación, administración de la relación, auditorías de calidad, supervisión operativa, cumplimiento de lineamientos, soporte, campañas y defensa contractual.

1.9. Proveedores y contratistas. FRANCEB y LCR tratan datos para selección, registro, contratación, debida diligencia, evaluación, pagos, gestión de riesgos, administración contractual, soporte, compras, cadena de suministro, control de servicios y cumplimiento.

1.10. Producción, bodega, fábrica y ERP. LCR trata datos necesarios para órdenes internas, producción, trazabilidad de productos, inventario, entradas y salidas, administración de bodega y fábrica, control de calidad, continuidad operativa, soporte de ERP y coordinación con áreas autorizadas.

1.11. Administración, contabilidad y control interno. LCR y, respecto de su estructura propia, FRANCEB tratan datos para gestión administrativa, contable, financiera, tributaria, conciliaciones bancarias, auditoría, control interno, archivo de soportes, indicadores, reportes, defensa y atención de requerimientos de autoridades.

1.12. Tecnología, ciberseguridad y continuidad. FRANCEB y LCR tratan datos para administrar usuarios, perfiles, permisos, dispositivos, redes, sistemas, bases de datos, respaldos, recuperación, continuidad, logs, monitoreo de seguridad, detección de amenazas, gestión de vulnerabilidades, incidentes, bajas de accesos y evidencia de cumplimiento.

1.13. Talento humano y nómina. LCR y FRANCEB respecto de su propio personal tratan datos para reclutamiento, selección, contratación, expediente laboral, nómina, IESS, beneficios, décimos, utilidades, vacaciones, permisos, licencias, capacitación, evaluaciones de desempeño, disciplina, incentivos, bonos, comisiones, seguros, terminación, liquidaciones, finiquitos, obligaciones tributarias, control de asistencia y gestión documental laboral.

1.14. Salud ocupacional y seguridad y salud en el trabajo. LCR y FRANCEB respecto de su personal propio tratan datos de salud estrictamente necesarios para vigilancia de la salud, exámenes ocupacionales, aptitud, accidentes laborales, incapacidades, enfermedades profesionales, ergonomía, prevención, programas de bienestar y cumplimiento de obligaciones de seguridad y salud en el trabajo.

1.15. Videovigilancia, control de acceso y seguridad física. LCR y, cuando corresponda, FRANCEB tratan imágenes, video, registros de acceso y datos asociados para proteger personas, bienes e instalaciones, controlar ingresos y salidas, prevenir e investigar incidentes, conservar evidencias y atender requerimientos de autoridades o aseguradoras.

1.16. Ejercicio de derechos, privacidad y cumplimiento. FRANCEB y LCR tratan datos para recibir, registrar, verificar identidad o representación, tramitar y responder solicitudes de derechos, bajas y oposiciones, gestionar incidentes de privacidad, mantener bitácoras, demostrar cumplimiento, atender auditorías y cooperar con la Superintendencia de Protección de Datos Personales.

2. Base legal para el tratamiento

2.1. Ejecución de medidas precontractuales y obligaciones contractuales. Se aplica, según corresponda, a pedidos, compras, entregas, cuentas de usuario, reclamos vinculados al servicio, contratación de franquicias y proveedores, procesos precontractuales, relaciones laborales y demás operaciones necesarias para iniciar o ejecutar una relación jurídica, de conformidad con el artículo 7 numeral 5 de la LOPDP.

2.2. Cumplimiento de obligaciones legales. Se aplica a facturación, contabilidad, tributación, SRI, IESS, Ministerio del Trabajo, seguridad social, obligaciones laborales, seguridad y salud en el trabajo, defensa del consumidor, conservación legal, atención de autoridades, gestión de derechos y otras obligaciones previstas en la normativa, de conformidad con el artículo 7 numeral 2 de la LOPDP.

2.3. Interés legítimo. FRANCEB y LCR fundamenta los tratamientos bajo la base de legitimación contenida en el artículo 7 numeral 8 de la LOPDP únicamente cuando el interés sea real, lícito, concreto, necesario y proporcional, y siempre que no prevalezcan los intereses, derechos o libertades fundamentales del titular. Cuando corresponda se documentará una evaluación de interés legítimo (LIA), se aplicarán medidas de minimización, transparencia, oposición y revisión periódica.

2.3.1. Seguridad física y CCTV. La videovigilancia, el control de acceso, la prevención e investigación de incidentes y la protección de personas, activos e instalaciones se sustentan principalmente en el interés legítimo de seguridad, sin perjuicio de obligaciones legales aplicables. La videovigilancia se implementará con señalización, acceso restringido, conservación limitada y controles de proporcionalidad.

2.3.2. Seguridad digital, prevención de fraude y trazabilidad. Los logs, alertas, controles de acceso, monitoreo de sistemas, conciliación antifraude, gestión de incidentes, respaldos y continuidad pueden sustentarse en interés legítimo de protección de información, activos, sistemas, clientes y operación.

2.3.3. Calidad del servicio y grabación de llamadas. La grabación y monitoreo de llamadas, la trazabilidad de reclamos y la evaluación de calidad pueden sustentarse en interés legítimo de control de calidad, seguridad, evidencia y mejora del servicio, junto con la ejecución contractual cuando la llamada esté vinculada con un pedido o servicio.

2.3.4. Marketing directo y fidelización. Cuando exista una relación previa, una expectativa razonable del titular y una finalidad compatible, FRANCEB podrá usar interés legítimo para seguimiento comercial, fidelización, segmentación limitada y comunicaciones relacionadas con productos o servicios propios, previa ponderación y

con un mecanismo sencillo e inmediato de oposición o baja. El interés legítimo no se utilizará para eludir el consentimiento cuando la normativa, la tecnología o la naturaleza del tratamiento lo requieran.

2.3.5. Control interno, auditoría y mejora operativa. La auditoría, gestión de desempeño, evaluación de proveedores, administración de riesgos, analítica operativa limitada, capacitación en seguridad, supervisión de red y continuidad pueden sustentarse en interés legítimo cuando resulten necesarios y proporcionados.

2.4. Consentimiento. Se utilizará para tratamientos opcionales que no puedan sustentarse válidamente en otra base, incluyendo determinadas campañas a prospectos sin relación previa, usos promocionales de imagen, cookies no necesarias, publicidad comportamental, remarketing mediante tecnologías opcionales y otras finalidades que requieran una manifestación libre, específica, informada e inequívoca.

2.5. Intereses vitales. En situaciones de emergencia que comprometan la vida, salud o integridad del titular o de otra persona natural, el tratamiento podrá sustentarse en el artículo 7 numeral 6 de la LOPDP, dentro de los límites estrictamente necesarios.

2.6. Fuentes accesibles al público. Los datos disponibles legítimamente en fuentes públicas podrán tratarse de forma proporcional y compatible con la finalidad de publicación, especialmente para verificación, debida diligencia o selección, conforme al artículo 7 numeral 7 de la LOPDP.

2.7. Categorías especiales y datos sensibles. El tratamiento de datos de salud, biométricos y otros datos sensibles se realizará únicamente cuando concorra una excepción válida del artículo 26 de la LOPDP. En el ámbito laboral y de seguridad y protección social se aplicará, cuando corresponda, el artículo 26 literal b. En emergencias podrá aplicarse el artículo 26 literal c. Los datos de salud se tratarán además conforme a las reglas específicas aplicables en el artículo 26 literal g y 31 de la LOPDP. El consentimiento explícito se reservará para supuestos en los que sea jurídicamente procedente y verdaderamente libre. El interés legítimo, por sí solo, no habilita el tratamiento de datos sensibles si no concurre una excepción del artículo 26.

3. Tipos de tratamiento

3.1. Operaciones realizadas. Los datos podrán ser recolectados, registrados, organizados, clasificados, consultados, utilizados, actualizados, cotejados, combinados, estructurados, almacenados, respaldados, recuperados, transmitidos, comunicados, transferidos, pseudoanonimizados, anonimizados, bloqueados, limitados, archivados o eliminados, según la finalidad y la base jurídica aplicable.

3.2. Tratamientos de observación y monitoreo. Cuando corresponda podrán realizarse grabaciones de voz, videovigilancia, control de acceso, generación y revisión de logs, monitoreo de seguridad, medición de uso del sitio, analítica y trazabilidad de interacciones.

3.3. Segmentación y perfilamiento comercial limitado. FRANCEB podrá clasificar contactos o clientes por historial de interacción, preferencias, productos consultados, canal, local, comportamiento de compra o respuesta a campañas para personalizar comunicaciones y medir resultados. El uso de cookies no necesarias o publicidad comportamental se registrará por las preferencias del titular.

3.4. Categorías principales de datos. Según el tratamiento podrán utilizarse datos de identificación y contacto; datos de facturación y tributarios; datos de consumo, pedidos y transacciones; datos financieros parciales o tokenizados; datos técnicos, IP, dispositivo, cookies y logs; voz y comunicaciones; datos laborales, profesionales y académicos; datos familiares y de beneficiarios; datos de salud y seguridad ocupacional; imágenes de CCTV; registros de acceso; datos biométricos cuando exista un sistema válido y necesario; datos de franquiciados, proveedores, representantes y contactos administrativos.

4. Tiempo de conservación

Numeral	Tratamiento	Criterio general de conservación
4.1.	Facturación, comprobantes, ventas, pagos y soportes contables o tributarios	Hasta 7 años, salvo plazo superior exigible o necesidad de defensa.
4.2.	Conciliaciones y soportes de cobro	Hasta 7 años o el plazo exigible por regulación y defensa.
4.3.	Pedidos, entregas, reclamos, cambios y devoluciones	Durante la gestión y posteriormente por los plazos de consumo, contabilidad, prescripción y defensa aplicables.
4.4.	Grabaciones de llamadas	Hasta 1 año como criterio general, salvo reclamo, investigación, auditoría, defensa o requerimiento de autoridad.

Numeral	Tratamiento	Criterio general de conservación
4.5.	Marketing y campañas	Hasta oposición, baja o revocatoria y, como criterio general, hasta 2 años desde la última interacción, conservando evidencia mínima de la baja cuando sea necesario.
4.6.	Cookies y analítica	Según la Política de Cookies y la configuración de cada tecnología, normalmente entre 3 meses y 2 años.
4.7.	Candidatos no seleccionados	Entre 1 año, salvo consentimiento para mantener una bolsa de empleo o necesidad de defensa.
4.8.	Expediente laboral, nómina, IESS, SRI y beneficios	Durante la relación laboral y hasta 7 años posteriores, sin perjuicio de plazos laborales, tributarios o de defensa aplicables.
4.9.	Control de asistencia y marcaciones	Durante la relación laboral y hasta 3 años posteriores; hasta 7 años cuando el registro tenga efectos contables o tributarios.
4.10.	CCTV	30 días como criterio general, salvo incidente, investigación, requerimiento de autoridad o defensa.
4.11.	Salud ocupacional y exámenes	Hasta 15 años desde la última atención o el plazo sanitario o laboral aplicable.
4.12.	Franquicias y contratos comerciales	Durante la relación y hasta 10 años posteriores cuando sea necesario para defensa civil o contractual.
4.13.	Proveedores, contratos y debida diligencia	Durante la relación y hasta 7 años; procesos de debida diligencia no contratados, hasta 5 años o un plazo menor definido.
4.14.	Solicitudes de derechos e incidentes de privacidad	Durante la gestión y por el plazo necesario para demostrar atención, cumplimiento y defensa ante autoridad.

4.15. Cumplida la finalidad y vencidos los plazos aplicables, los datos serán eliminados, anonimizados o bloqueados cuando exista una obligación o necesidad legítima de conservación restringida. Los respaldos y copias de seguridad se depurarán conforme a ciclos técnicos razonables.

5. Existencia de bases de datos

5.1. FRANCEB y LCR mantienen bases de datos, registros y archivos físicos o electrónicos que pueden contener datos personales relacionados con sus actividades. Estas bases pueden estar alojadas en infraestructura propia o de proveedores autorizados.

5.2. Entre los repositorios y sistemas identificados se encuentran, según corresponda, NEOLA, sistemas POS, portal web y comercio electrónico, PAGOPLUX, plataformas de delivery, plataformas de telefonía y grabación, herramientas de email marketing y redes sociales, soluciones de analítica, ERP, sistemas contables, nómina, expedientes de talento humano, sistemas de salud ocupacional, correo corporativo, gestores documentales, hojas de cálculo controladas, servidores, respaldos, sistemas CCTV con NVR o DVR, sistemas de control de acceso y archivos físicos autorizados.

5.3. La existencia de una base de datos no implica que todos los titulares estén registrados en todos los sistemas. El repositorio aplicable depende de la relación, canal, área y finalidad concreta.

6. Origen de los datos personales cuando no se obtengan directamente del titular

- 6.1.** Plataformas de delivery como Uber Eats, Rappi y PedidosYa, respecto de pedidos, contactos y datos necesarios para entrega, soporte, conciliación o facturación.
- 6.2.** Pasarelas de pago, bancos, adquirentes y sistemas de conciliación, respecto de identificadores de transacción, estados de pago, montos y datos financieros parciales o tokenizados.
- 6.3.** Sistemas POS, locales, franquiciados y áreas internas autorizadas, cuando el dato se origine en una interacción previa con la marca o en procesos operativos.
- 6.4.** Proveedores de call center, telefonía, soporte, tecnología, correo, nube, analítica, facturación electrónica y servicios logísticos, cuando generen registros por cuenta de FRANCEB o LCR.
- 6.5.** IESS, Ministerio del Trabajo, SRI, autoridades competentes, aseguradoras, brokers, laboratorios, proveedores de salud ocupacional y sistemas de seguridad social, en la medida permitida por la ley.
- 6.6.** Referencias laborales, académicas o profesionales proporcionadas por candidatos, empleadores anteriores o fuentes legítimas para procesos de selección y debida diligencia.
- 6.7.** Registros públicos y fuentes accesibles al público, únicamente cuando su uso sea compatible con la finalidad de publicación y resulte necesario y proporcional.
- 6.8.** Cámaras de videovigilancia, bitácoras de seguridad, sistemas de acceso, logs, dispositivos, redes y sistemas corporativos, respecto de registros generados automáticamente por el uso de instalaciones o sistemas.
- 6.9.** Cuando los datos no se obtengan directamente del titular, se proporcionará la información exigida por la LOPDP dentro del plazo legal o en la primera comunicación, salvo que concurra una excepción prevista en la normativa o el titular ya disponga de dicha información.

7. Otras finalidades y tratamientos ulteriores

- 7.1.** FRANCEB y LCR no utilizarán datos para finalidades incompatibles con aquellas informadas. Antes de un tratamiento ulterior se evaluará la relación entre las finalidades, el contexto de recolección, las expectativas razonables del titular, la naturaleza de los datos, las consecuencias del nuevo uso y las garantías aplicables.
- 7.2.** Cuando un tratamiento ulterior sea compatible y pueda sustentarse en la misma base, se actualizará la información al titular cuando corresponda. Si requiere una base diferente, se documentará dicha base y se obtendrá consentimiento cuando sea necesario.
- 7.3.** El uso posterior de datos de pedidos, call center, web o POS para fidelización, segmentación o marketing solo procederá cuando exista una base jurídica válida. En relaciones previas compatibles podrá evaluarse interés legítimo; en prospectos, cookies no necesarias, remarketing o publicidad comportamental se aplicará consentimiento cuando corresponda.

8. Identidad y datos de contacto de los responsables del tratamiento

Numera l	Responsable	RUC	Domicilio	Teléfono	Correo
8.1.	FRANQUICIAS ALIMENTICIAS FRANCEB CIA. LTDA.	179256874900 1	Calle Manuel Mogollón N45 11 y José Paredes Tamarindo, Distrito Metropolitano de Quito, Pichincha, Ecuador.	098 280 4444 / 1800 CEBICHES (232424)	dpd_lcr@lcrcebiches.com
8.2.	LCR PRODUCTOS & SERVICIOS CIA. LTDA.	179195035600 1	Calle de los Aceitunos E3 76 y Av. Eloy Alfaro, Distrito Metropolitano de Quito, Pichincha, Ecuador.	098 280 4444 / 1800 CEBICHES (232424)	dpd_lcr@lcrcebiches.com

8.3. Cada entidad actúa como responsable respecto de los tratamientos que determina dentro de su ámbito. El uso compartido de la marca y la coordinación operativa no convierte automáticamente todos los tratamientos en responsabilidad conjunta. Cuando exista una operación compartida, se documentará el rol de cada parte y se informará al titular cuando corresponda.

9. Identidad y datos de contacto del Delegado de Protección de Datos Personales

9.1. Delegado de Protección de Datos Personales: Juan Felipe Rivas Bock.

9.2. Canal específico de privacidad y ejercicio de derechos: dpd_lcr@lcrcebiches.com.

9.3. Correo del DPD: dpd_lcr@lcrcebiches.com.

9.4. Domicilio profesional de contacto: Baquerizo Moreno y José Tamayo, Edificio Torres del Castillo, piso 7, oficina 707, Quito, Ecuador.

9.5. Teléfonos profesionales de contacto: +593 (2) 223 9245 y +593 (2) 255 4473.

9.6. El DPD actúa como punto de contacto especializado para los titulares, los responsables y la Superintendencia de Protección de Datos Personales, y coordina internamente la identificación de la entidad responsable cuando una solicitud pueda involucrar a FRANCEB, LCR o a ambas.

10. Transferencias y comunicaciones nacionales o internacionales

10.1. Destinatarios internos. Gerencia, operaciones, locales, caja, contabilidad, tesorería, finanzas, talento humano, seguridad y salud ocupacional, legal, marketing, soporte, call center, tecnología, auditoría, administración de franquicias y responsables funcionales autorizados, según necesidad y mínimo privilegio.

10.2. Autoridades y organismos. SRI, IESS, Ministerio del Trabajo, Superintendencia de Protección de Datos Personales, autoridades judiciales, administrativas, de control y otras autoridades competentes, cuando exista obligación o habilitación legal.

10.3. Proveedores y encargados. Bancos, adquirentes, pasarelas de pago, proveedores POS, call center, telefonía y monitoreo, facturación electrónica, nube, correo, soporte tecnológico, ciberseguridad, salud ocupacional, laboratorios, aseguradoras, brokers, CCTV, control de acceso, capacitación, logística, marketing, analítica y otros proveedores autorizados que actúen bajo instrucciones y contratos de tratamiento cuando corresponda.

10.4. Plataformas y aliados independientes. Uber Eats, Rappi, PedidosYa, pasarelas, redes sociales, franquiciados y otros aliados pueden actuar como responsables independientes o, según la operación, bajo otra relación jurídica. Sus propias políticas podrán resultar aplicables en los tratamientos que determinen por cuenta propia.

10.5. Comunicación entre FRANCEB y LCR. Los datos podrán comunicarse entre ambas entidades únicamente cuando resulte necesario para producción, comercialización, pedido, facturación, soporte, cumplimiento, auditoría, seguridad, relación laboral o defensa, respetando la finalidad, minimización, acceso autorizado y rol jurídico aplicable.

10.6. Transferencias internacionales. Algunos proveedores de nube, delivery, redes sociales, pasarelas, analítica, correo, soporte o tecnología pueden implicar almacenamiento o acceso remoto desde fuera del Ecuador. Estas transferencias se realizarán únicamente con base jurídica, finalidad legítima y garantías adecuadas, que podrán incluir decisiones de nivel adecuado, cláusulas contractuales, compromisos exigibles, medidas técnicas, cifrado, seudoanonimización, evaluaciones de proveedor y demás salvaguardas exigidas por la normativa.

11. Consecuencias de entregar o negarse a entregar datos personales

11.1. Pedidos y compras. La negativa a facilitar datos necesarios de identificación, contacto, entrega o facturación puede impedir procesar el pedido, entregar productos, emitir comprobantes, gestionar pagos, cambios, devoluciones o reclamos.

11.2. Relaciones contractuales. La negativa a entregar datos necesarios puede impedir analizar una solicitud de franquicia, contratar o administrar proveedores, formalizar contratos o ejecutar obligaciones pactadas.

11.3. Relación laboral. La falta de datos legal o contractualmente necesarios puede impedir contratar, pagar nómina, afiliarse al IESS, administrar beneficios, registrar asistencia, cumplir obligaciones tributarias o ejecutar deberes de seguridad y salud en el trabajo.

11.4. Seguridad. La negativa a facilitar datos mínimos de control de acceso puede impedir el ingreso a áreas restringidas cuando la identificación sea necesaria y proporcional por seguridad.

11.5. Datos opcionales. La negativa a entregar datos para marketing, encuestas, cookies no necesarias, programas opcionales o ubicación no impedirá acceder al servicio principal. El titular podrá buscar sucursales manualmente, rechazar cookies opcionales o no recibir promociones sin afectar su compra.

12. Efecto de suministrar datos personales erróneos o inexactos

12.1. Los datos inexactos pueden ocasionar entregas fallidas, facturas incorrectas, imposibilidad de contacto, problemas en conciliación de pagos, atención tardía de reclamos o errores en la cuenta de usuario.

12.2. En relaciones laborales o contractuales, datos erróneos pueden afectar pagos, afiliaciones, beneficios, retenciones, comunicaciones, acceso a sistemas, expedientes o cumplimiento de obligaciones.

12.3. El titular debe procurar que la información proporcionada sea correcta y actualizada. FRANCEB y LCR adoptarán medidas razonables para rectificar o actualizar datos inexactos cuando tengan conocimiento de ello y el titular podrá ejercer sus derechos de rectificación y actualización en cualquier momento.

13. Posibilidad de revocar el consentimiento

13.1. Cuando un tratamiento se base en consentimiento, el titular puede revocarlo en cualquier momento mediante el canal dpd_lcr@lcrcebiches.com, el Formulario ARSO+, los mecanismos de configuración de cookies o el medio específico de baja habilitado en la comunicación.

13.2. La revocatoria no afecta la licitud del tratamiento efectuado antes de su retiro y no impide continuar tratamientos que cuenten con otra base jurídica válida, como una obligación legal, ejecución contractual, interés vital o interés legítimo debidamente aplicable.

13.3. En comunicaciones comerciales, la palabra BAJA, la solicitud de oposición o un mecanismo equivalente será registrada en la lista de exclusión o preferencia correspondiente. Podrá conservarse información mínima para acreditar y respetar la baja sin utilizarla con fines promocionales.

14. Existencia y forma de hacer efectivos los derechos del titular

14.1. Información. Conocer las condiciones esenciales del tratamiento y recibir información clara sobre finalidades, bases, datos, conservación, fuentes, destinatarios, transferencias, consecuencias, derechos, reclamos y decisiones automatizadas.

14.2. Acceso. Conocer si FRANCEB o LCR tratan datos personales del titular y acceder a la información que corresponda, sin necesidad de justificar la solicitud.

14.3. Rectificación y actualización. Corregir o actualizar datos inexactos, incompletos o desactualizados.

14.4. Eliminación. Solicitar la supresión cuando proceda, salvo que exista obligación legal, defensa, bloqueo o una base jurídica que impida la eliminación inmediata.

14.5. Oposición. Oponerse a tratamientos cuando proceda, especialmente frente a marketing o tratamientos sustentados en interés legítimo, atendiendo la situación particular y la ponderación aplicable.

14.6. Anulación, suspensión o limitación. Solicitar la limitación temporal o suspensión de operaciones de tratamiento en los supuestos previstos por la normativa.

14.7. Revocatoria. Retirar el consentimiento respecto de tratamientos basados en esa manifestación.

14.8. No ser objeto de decisiones basadas únicamente en valoraciones automatizadas. Solicitar intervención, revisión o impugnación cuando una decisión automatizada produzca efectos jurídicos o afectaciones significativas, conforme a la normativa.

14.9. Canales de ejercicio. El titular o su representante podrá presentar la solicitud a dpd_lcr@lcrcebiches.com, utilizar el Formulario ARSO+ digital o descargable, o presentar una solicitud por los canales habilitados. Las solicitudes recibidas por otros canales serán remitidas internamente al DPD.

14.10. Contenido mínimo de la solicitud. Deberá permitir identificar al titular o representante, indicar un medio para notificaciones, señalar el derecho ejercido y describir de manera suficientemente clara la solicitud. Solo se pedirán documentos adicionales cuando sean necesarios para verificar identidad, representación o localizar el tratamiento.

14.11. Selector de responsable. El formulario podrá permitir seleccionar FRANCEB, LCR o “No estoy seguro”. La falta de selección no impedirá el envío; el DPD determinará internamente la entidad responsable según el canal, proceso, sistema y contexto.

15. Mecanismos para hacer efectivo el derecho a la portabilidad

15.1. Cuando la portabilidad resulte aplicable técnica y jurídicamente, el titular podrá solicitar recibir sus datos en un formato estructurado, interoperable y de lectura común, o solicitar su transmisión a otro responsable cuando sea técnicamente posible y se cumplan los requisitos legales.

15.2. La solicitud se presentará por dpd_lcr@lcrcebiches.com o mediante el Formulario ARSO+, identificando los datos o tratamiento objeto de portabilidad y, cuando corresponda, el destinatario.

15.3. La portabilidad no afectará derechos de terceros, secretos empresariales, obligaciones de conservación ni información que no pueda separarse razonablemente de datos ajenos. El DPD comunicará cualquier limitación de forma motivada.

16. ¿Dónde y cómo realizar reclamos?

16.1. Reclamo o consulta ante los responsables. El titular puede escribir a dpd_lcr@lcrcebiches.com, utilizar el Formulario ARSO+ o remitir su reclamo al DPD. El caso será radicado, identificado con un código o constancia y gestionado por FRANCEB, LCR o ambas según el tratamiento involucrado.

16.2. Reclamo ante la Autoridad de Protección de Datos Personales. Si el titular considera que sus derechos no han sido debidamente atendidos o existe una vulneración, podrá presentar un reclamo ante la Superintendencia de Protección de Datos Personales del Ecuador (SPDP) a través de los canales oficiales vigentes publicados en spdp.gob.ec.

16.3. La presentación de un reclamo no limita otros mecanismos de tutela reconocidos por la Constitución, la LOPDP y el ordenamiento jurídico aplicable.

17. Existencia de valoraciones y decisiones automatizadas, incluida la elaboración de perfiles

17.1. Por regla general, FRANCEB y LCR no adoptan decisiones basadas únicamente en valoraciones automatizadas que produzcan efectos jurídicos o afectaciones significativas para clientes, trabajadores, proveedores, franquiciados o terceros.

17.2. FRANCEB puede utilizar segmentación, analítica, medición de campañas, preferencias, historial de compra, interacción con canales, productos consultados o comportamiento de navegación para personalizar comunicaciones, medir resultados y mejorar la experiencia. Estas actividades pueden constituir elaboración de perfiles comercial limitada, pero no deben utilizarse por sí solas para producir efectos jurídicos o afectaciones significativas.

17.3. El remarketing, publicidad comportamental y tecnologías de seguimiento no necesarias se sujetarán a consentimiento o a la base jurídica específica aplicable y a la Política de Cookies. El titular puede configurar preferencias, retirar consentimiento u oponerse al marketing por los mecanismos habilitados.

17.4. Si en el futuro se implementa una decisión automatizada con efectos jurídicos o significativos, el responsable informará previamente la existencia del proceso, proporcionará información significativa sobre la lógica general, consecuencias y salvaguardas, y habilitará intervención humana, revisión e impugnación cuando corresponda.

Disposición final. Vigencia, actualización y documentos relacionados

DF.1. Este aviso entra en vigencia con su publicación y podrá actualizarse cuando existan cambios normativos, tecnológicos, contractuales, de proveedores, finalidades, sistemas, bases jurídicas o criterios de la Superintendencia de Protección de Datos Personales.

DF.2. La versión vigente debe permanecer accesible desde el sitio web y los avisos de primera capa deben remitir a este aviso o al apartado específico que corresponda.

Documentos relacionados: Política General de Protección de Datos Personales de FRANCEB; Política General de Protección de Datos Personales de LCR; Política de Cookies; Términos y Condiciones de Uso; Procedimiento para el Ejercicio de Derechos; Formulario ARSO+; avisos específicos por canal y demás documentos vigentes del sistema de protección de datos.