infra commerce

Sua estratégia, nosso ecossistema.

POLÍTICA GLOBAL DE PRIVACIDAD Y PROTECCIÓN DE DATOS

ÍNDICE

1. OBJETIVO

Esta Política Global de Privacidad y Protección de Datos ("Política") establece los lineamientos y principios generales que rigen el Programa de Privacidad de Infracommerce y subsidiarias, aplicándose a todo el Tratamiento de Datos Personales realizado en el contexto de las actividades de la organización, en cualquier país donde opere. El propósito de este documento es garantizar un estándar corporativo uniforme de gobierno en privacidad y protección de datos, que sirva como base para el cumplimiento de la legislación local aplicable.

Considerando las particularidades regulatorias de cada jurisdicción, esta Política puede complementarse con documentos normativos específicos, con lineamientos y procedimientos operativos adicionales ajustados a los requisitos legales y regulatorios de cada país donde operan Infracommerce y sus subsidiarias.

2. APLICABILIDAD

Esta Política es aplicable a Infracommerce y sus filiales, en todos los países en los que operan, cubriendo cualquier actividad que implique el Tratamiento de Datos Personales bajo su responsabilidad.

Teniendo en cuenta las especificidades legales de cada jurisdicción, esta Política establece directrices corporativas mínimas y uniformes, que pueden complementarse con directrices y estructuras locales, según sea necesario para garantizar el cumplimiento de la legislación aplicable en cada territorio.

En caso de conflicto entre las disposiciones de esta Política y las leyes o regulaciones locales de protección de datos, prevalecerán las normas legales vigentes en el territorio respectivo, y las prácticas de Infracommerce y sus subsidiarias se ajustarán para garantizar el cumplimiento local, sin perjuicio de los principios generales establecidos en este documento.

3. ABRANGENCIA

Esta Política es aplicable a todas las personas físicas o jurídicas que, directa o indirectamente, tengan una relación con Infracommerce y sus subsidiarias, o que actúen en su nombre. Esto incluye, entre otros, empleados, gerentes, pasantes, aprendices, consultores, terceros, proveedores de servicios, socios comerciales y proveedores.

Las disposiciones establecidas en este documento deben observarse siempre que dichos agentes realicen el Tratamiento de Datos Personales en el contexto de las actividades de Infracommerce y subsidiarias, incluso mediante el uso de sistemas, dispositivos, redes u otros recursos tecnológicos puestos a disposición por la organización.

4. GLOSARIO DE PROTECCIÓN DE DATOS

A los efectos de la interpretación y aplicación de esta Política, se adoptan las siguientes definiciones, que tienen como objetivo garantizar la claridad y la uniformidad terminológica en el contexto de las actividades de Tratamiento de Datos Personales realizadas por Infracommerce y sus filiales.

Las definiciones adoptadas en esta Política se estructuraron con base en los conceptos previstos en la Ley Federal n.º 13.709/2018 – Ley General de Protección de Datos Personales (LGPD), de Brasil, sirviendo como referencia normativa. Sin embargo, su aplicación es amplia y cubre todos los países en los que operan Infracommerce y sus filiales. De esta manera, estas definiciones pueden ser adaptadas, interpretadas o aprobadas de acuerdo con las leyes y regulaciones locales aplicables, respetando las especificidades legales de cada jurisdicción.

Dato personal: cualquier información relacionada con una persona física identificada o identificable, directa o indirectamente, por referencia a un identificador o características que permitan su individualización, independientemente del medio o formato en el que se almacenen los datos.

Dato personal sensible: un subconjunto de datos personales que incluye información sobre origen étnico o racial, creencias religiosas o filosóficas, opiniones políticas, membresía en organizaciones, datos de salud, datos biométricos, datos genéticos o información sobre la vida u orientación sexuales.

Titular de los datos (Interesado/ *Data Subject*): la persona a la que se refieren los datos personales.

Tratamiento: cualquier operación realizada con Datos Personales, automatizada o no, incluyendo, pero no limitado a: recopilación, acceso, uso, intercambio, almacenamiento, organización, estructuración, adaptación, modificación, extracción, eliminación, archivo o cualquier otra forma de procesamiento.

Leyes de Protección de Datos Personales aplicables: conjunto de normas legales, reglamentarias o sectoriales, vigentes en las jurisdicciones en las que operan Infracommerce y sus subsidiarias, que establecen obligaciones relacionadas con la privacidad y protección de Datos Personales.

Autoridad(es) de protección de datos competente(s): organismo público u organismo regulador dotado de competencia legal para supervisar, supervisar y guiar el cumplimiento de las normas de privacidad y protección de datos, así como para recibir quejas de los interesados, realizar investigaciones, aplicar sanciones y cooperar con otras autoridades de protección de datos.

Compartimiento de los datos personales: todas y cada una de las formas de poner los Datos Personales a disposición de Terceros o empresas subsidiarias de Infracommerce, incluida la comunicación, divulgación, transferencia, envío, recepción o acceso a Datos Personales, independientemente del medio utilizado o del propósito involucrado.

Transferencia internacional de datos personales: Intercambio de datos personales entre países distintos de aquel en el que se procesó originalmente la información, incluso en el contexto de operaciones de transferencia entre subsidiarias de Infracommerce.

***Global Data Protection Officer*:** persona o estructura designada para coordinar, a nivel institucional, las actividades de gobernanza de privacidad y protección de datos dentro de Infracommerce y sus subsidiarias. El DPD actúa como punto de contacto con las autoridades competentes en materia de protección de datos y los interesados en cuestiones estratégicas o transversales.

Delegado local: persona o estructura designada en una jurisdicción o territorio determinado, cuando sea necesario, para apoyar la implementación local de las pautas corporativas de protección de datos, actuar como canal de comunicación con los Sujetos de Datos y las Autoridades Competentes de Protección de Datos, y garantizar el cumplimiento de las Leyes de Protección de Datos Personales Aplicables. El delegado Local actúa de acuerdo con las directrices del Oficial. La función principal del delegado es acercar a las empresas al gobierno de los datos, facilitando la imagen de privacidad y protección de datos como beneficio para el desarrollo empresarial. El delegado comunica las preocupaciones y perspectivas de privacidad y protección de datos a las unidades de negocio y, por otro lado, presenta los objetivos de negocio a los equipos de seguridad, facilitando así la convergencia de las dos visiones.

Operador/*Data Processor*: persona, agencia u otro organismo que lleve a cabo el Tratamiento de Datos Personales en nombre y bajo la dirección del responsable del Tratamiento/Responsable del Tratamiento de Datos Personales.

Controlador/*Data Controller*: persona, agencia u otro organismo que determine los fines y medios del Tratamiento de Datos Personales.

Terceros o Proveedores: personas que no forman parte de la estructura organizativa

de Infracommerce y sus filiales, pero que actúan en su nombre o interés, o que, de cualquier manera, tienen acceso, pueden tratar o ser destinatarios de Datos Personales en el contexto de sus actividades. Esto incluye, entre otros, proveedores de servicios, proveedores, socios comerciales o consultores.

Informe de Impacto: documento que describe, analiza y evalúa los riesgos relacionados con las operaciones de Tratamiento de Datos Personales que pueden afectar los derechos y libertades de los Titulares, incluyendo las medidas y salvaguardas adoptadas para mitigar dichos riesgos.

Privacy Impact Assessment **(PIA):** instrumento preventivo de evaluación de riesgos, destinado a identificar, analizar y documentar los riesgos que puede generar una determinada actividad de Tratamiento.

5. DIRECTRICES GENERALES PARA EL TRATAMIENTO DE DATOS PERSONALES

Infracommerce y sus filiales llevarán a cabo el Tratamiento de Datos Personales de acuerdo con los principios de protección de datos reconocidos internacionalmente. Así, el Tratamiento de Datos Personales debe seguir los siguientes compromisos:

- Procesar datos personales para un propósito legítimo, específico e informado. y se prohíbe su uso para fines incompatibles con los declarados originalmente.
- Hacer que toda la actividad de procesamiento sea compatible con el contexto en el que se recopilaron los datos personales, limitando el procesamiento al mínimo necesario para lograr los objetivos previstos.
- Limitar la retención de los Datos Personales al tiempo estrictamente necesario para el cumplimiento de la finalidad para la que fueron recopilados, sujeto a los plazos legales y reglamentarios aplicables.
- Mantener los Datos Personales exactos, actualizados y pertinentes a los fines para los que están destinados, adoptando las medidas técnicas y organizativas

adecuadas para garantizar la seguridad e integridad.

- Apoyar las actividades de Tratamiento sobre una Base Legal válida, según lo dispuesto en las Leyes de Protección de Datos Aplicables en cada jurisdicción, teniendo en cuenta la naturaleza de los datos tratados y el contexto de la operación.
- Garantizar la transparencia en las prácticas de Tratamiento, así como proporcionar medios accesibles para el ejercicio de los derechos garantizados a los Interesados, incluido el derecho de acceso a la información sobre el Tratamiento, siempre que Infracommerce o sus filiales actúen como responsable del Tratamiento.
- Mantener el compromiso con la adopción de medidas encaminadas a la prevención de riesgos, la prohibición de tratos discriminatorios y la demostración continua del cumplimiento de esta Política, así como de la legislación aplicable en cada jurisdicción.

6. GOBERNANZA EN PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

Infracommerce y sus subsidiarias mantienen una estructura de gobierno en privacidad y protección de Datos Personales compuesta por actividades operativas y estratégicas, diseñadas para garantizar el cumplimiento de las Leyes de Protección de Datos Personales Aplicables, la gestión de riesgos y la consolidación de una cultura organizacional orientada a la privacidad.

Las rutinas operativas son definidas y formalizadas por cada territorio en documentos específicos, de acuerdo con la estructura organizativa local, los requisitos reglamentarios aplicables y las particularidades de las operaciones regionales. Estos documentos complementarios detallan los flujos, responsabilidades y controles adoptados para la ejecución de las actividades de Tratamiento de Datos Personales.

Las actividades estratégicas, comunes a toda la estructura de Infracommerce y

subsidiarias, forman el núcleo del Programa de Privacidad y se presentan a continuación.

6.1. Registro de actividades de tratamiento

Todas las actividades de Tratamiento de Datos Personales deben ser debidamente registradas y archivadas por Infracommerce y sus subsidiarias, de manera estructurada y actualizada, en los términos de esta Política. El inventario de actividades de Tratamiento debe contener, al menos, la siguiente información:

- Indicación del área responsable de la actividad de Tratamiento;
- Finalidad del tratamiento;
- Categorías de datos personales involucrados;
- Origen de los datos personales;
- Existencia de Compartir con Terceros u otras subsidiarias de Infracommerce;
- Existencia de transferencia internacional de datos;
- Ubicación de los datos personales y descripción de la infraestructura de almacenamiento;
- Sistemas, plataformas y herramientas utilizados en el Tratamiento;
- Período de retención de datos personales; y
- Medidas de seguridad técnicas y organizativas aplicadas a la actividad.

Cada región o subsidiaria de Infracommerce, a través de sus áreas de negocio (o Unidades de Negocio) es responsable de mantener un inventario estructurado, completo y actualizado de las actividades de Tratamiento de Datos Personales, de acuerdo con los lineamientos establecidos en esta Política.

El inventario debe ser elaborado por las áreas de negocio de cada unidad

organizativa de Infracommerce y realizado bajo la coordinación y supervisión del delegado Local y/o Responsable. Siempre que sea necesario, el responsable podrá solicitar registros consolidados, con el fin de supervisar y centralizar las prácticas de Tratamiento a nivel corporativo.

El inventario debe revisarse y actualizarse al menos cada dos años o cada vez que haya cambios relevantes en los flujos de Tratamiento o como resultado de cambios legales o reglamentarios aplicables en la jurisdicción correspondiente.

6.2. Gestión de riesgos y cumplimiento

La gestión de los riesgos de privacidad y protección de datos personales en el ámbito de Infracommerce y sus filiales se lleva a cabo mediante la realización de evaluaciones en dos niveles: el análisis de Impacto en la Privacidad (PIA) y, cuando corresponda, Evaluación de Impacto de Protección de Datos (EIPD).

La PIA es aplicable a todas las iniciativas, proyectos o procesos que impliquen el Tratamiento de Datos Personales, especialmente en la implementación de nuevas actividades, productos, servicios o tecnologías.

La Evaluación de Impacto de Protección de Datos (EIPD) es el documento que describe los procesos de tratamiento de datos personales que pueden suponer un alto riesgo para la garantía de los principios generales de protección de datos personales y las libertades civiles y los derechos fundamentales del interesado. Así, la EIPD representa un instrumento relevante en el marco de la gestión de riesgos y el cumplimiento de la protección de datos personales tratados por Infracommerce y sus filiales.

Dependiendo de la naturaleza y la criticidad de los riesgos identificados en el

PIA, puede ser necesario un informe de impacto. Los factores que pueden desencadenar el requisito del Informe de Impacto incluyen:

- Tratamiento a gran escala de datos personales;
- Actividades de procesamiento con un impacto significativo potencial en los derechos y libertades de los Interesados;
- Uso de tecnologías emergentes o innovadoras;
- Decisiones automatizadas sin intervención humana;
- Tratamiento de Datos Personales Sensibles, Datos Personales de niños, adolescentes o adultos mayores.

Además de estos criterios, otros factores pueden justificar la elaboración del Informe de Impacto, dependiendo de los requisitos legales o reglamentarios aplicables en cada territorio donde opera Infracommerce. La plantilla de informes de impacto se puede adaptar según sea necesario, respetando los requisitos locales.

Es responsabilidad del responsable del área de negocio cumplimentar correctamente la PIA, así como comunicarla al delegado Local y/o al responsable siempre que la actividad de Tratamiento presente características que puedan dar lugar a la elaboración de un Informe de Impacto. Corresponderá al responsable constituir formalmente el Informe de Impacto, con base en la información proporcionada por el área, y el documento deberá ser devuelto al gestor responsable de la implementación de las medidas de mitigación de riesgos recomendadas.

En los casos en que persistan riesgos residuales relevantes, ya sea por la no implementación de las medidas sugeridas o por la naturaleza de la propia actividad, el responsable de área deberá formalizar la aceptación del riesgo,

asumiendo la responsabilidad de la continuidad de la operación en los términos definidos. Todos los riesgos residuales formalizados deben ser reportados al Comité de Privacidad para fines de registro y seguimiento.

Teniendo en cuenta los fundamentos de la protección de datos personales, la buena fe y otros principios que deben observarse en las actividades de tratamiento de datos personales, Infracommerce cuenta con diferentes sistemas de control interno, que varían según la naturaleza de los datos personales, para mitigar cualquier riesgo de falla en la protección de datos personales. Sin embargo, a pesar del alto grado de madurez de la gestión de riesgos de Infracommerce con la implementación de diversos controles y medidas de mitigación, no es posible garantizar la eliminación total de los riesgos que, en caso de materialización, podrían afectar la privacidad de los datos personales de la empresa.

6.3. Derechos de los interesados (*Data Subject*)

En los casos en que Infracommerce o sus filiales actúen como responsable/Responsable del Tratamiento de Datos Personales, se debe garantizar a los Titulares la posibilidad de ejercer derechos relacionados con el Tratamiento de sus Datos Personales.

Los derechos que pueden ser ejercitados por los Interesados, según lo previsto en la legislación aplicable de cada país, son:

- Confirmación de la existencia de Tratamiento;
- Acceso a los datos personales procesados;
- Solicitud de corrección, actualización o complementación;
- Eliminación, anonimización o bloqueo de datos;
- Revisión de las decisiones tomadas únicamente sobre la base del

procesamiento automatizado;

- Solicitud de información sobre el intercambio de datos con terceros.

En relación con el contexto y el país desde el que los interesados solicitan sus derechos, puede haber ciertas diferencias, en particular, en la forma en que se pueden ejercer estos derechos. Por ejemplo, a través de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), el derecho a la portabilidad, transparencia y tratamiento de los terceros involucrados. Por este motivo, aconsejamos a nuestros clientes y terceros que conozcan esta política en todo momento. Para realizar una solicitud sobre los derechos aquí señalados o para aclarar dudas, comuníquese con nosotros a través del Formulario de Atención al Titular.

Con sujeción a las disposiciones específicas de la legislación local, que pueden prever derechos adicionales, cualquier solicitud debe ser satisfecha dentro de un plazo razonable. Por ejemplo, según la LGPD (Brasil), las solicitudes de los interesados deben ser respondidas en un plazo máximo de 15 días naturales desde su recepción, salvo que la legislación específica establezca un plazo más corto. Por lo tanto, las unidades de negocio deben adaptar sus procesos para priorizar el plazo más corto establecido por la legislación local. Así, el Delegado local debe velar por el cumplimiento de estos plazos.

Las solicitudes de los Interesados deben registrarse y procesarse de manera consolidada, asegurando la trazabilidad del servicio. El canal oficial para enviar solicitudes es la dirección de correo electrónico institucional: dpo@infracommerce.com.br.

6.4. Incidentes de seguridad relacionados con datos personales

Infracommerce y sus subsidiarias mantienen rutinas destinadas a la adopción de medidas técnicas y administrativas destinadas a prevenir y responder a incidentes de seguridad que involucren Datos Personales.

En caso de ocurrencia o sospecha de incidentes de esta naturaleza, la acción debe cumplir con los lineamientos establecidos en el plan corporativo de respuesta a incidentes, de acuerdo con los requisitos legales y reglamentarios aplicables en cada región.

A los efectos del registro y seguimiento, cualquier incidente de seguridad que involucre Datos Personales debe ser informado, sin demora, a través del sistema corporativo designado para tal fin, o a través del correo electrónico de dpo@infracommerce.com.br. La inscripción debe realizarse dentro de los plazos definidos por el responsable a partir del conocimiento del evento. Es responsabilidad de las unidades de negocio tomar conocimiento de los incidentes operativos relacionados con la privacidad y la protección de datos. Por lo tanto, el delegado local y el oficial a cargo deberán adaptar los planes de respuesta a incidentes a escenarios de amenazas a la privacidad y garantizar que los plazos reglamentarios locales se puedan cumplir de manera oportuna.

6.5. Compartición de datos personales con terceros

LA compartición de Datos Personales con Terceros se llevará a cabo solo cuando sea estrictamente necesario para el logro de fines legítimos, sujeto a los requisitos legales aplicables y los principios de esta Política.

Antes de establecer cualquier relación contractual con Terceros que puedan tener acceso a Datos Personales, Infracommerce y sus filiales evaluarán el

nivel de cumplimiento y madurez del agente externo en relación con la protección de datos, de acuerdo con los criterios definidos por la estructura de gobierno corporativo de privacidad, sin perjuicio de los criterios específicos aplicables a cada región. El área propietaria de las compras y contrataciones es responsable de la aprobación de terceros, con base en los requisitos de seguridad y privacidad de la información.

En función del riesgo identificado, se pueden adoptar medidas complementarias de seguimiento, incluyendo controles de seguridad y acciones de seguimiento y, en su caso, procesos de diligencia debida y auditoría para verificar el mantenimiento de los controles implementados.

La contratación formal debe garantizar la inclusión de cláusulas contractuales adecuadas, que establezcan obligaciones específicas sobre privacidad y seguridad de la información, que no se limiten a sanciones o multas de acuerdo con las leyes aplicables en cada país.

En los casos en que la relación con Terceros implique Transferencia Internacional de Datos Personales, la existencia o no de dicha transferencia deberá ser previamente declarada y formalizada por escrito por el tercero antes del inicio de la relación contractual. Todas las Transferencias Internacionales de Datos realizadas por Infracommerce y sus subsidiarias deben estar formalmente documentadas, en alineación con los controles internos y los requisitos reglamentarios aplicables en cada jurisdicción.

Toda transferencia internacional debe ir precedida de la adopción de mecanismos de legitimación adecuados, según lo previsto en la legislación aplicable. Esto incluye, entre otros, el uso de cláusulas contractuales tipo o instrumentos equivalentes puestos a disposición o reconocidos por las

autoridades competentes. Por ello, los responsables de seguridad legal y de la información deben asegurarse de que todos los proveedores de la empresa cuenten con una aprobación completa o sencilla del área de privacidad y protección de datos como requisito para la contratación antes de ser contratados. Dependiendo de la relevancia del valor económico del contrato, dependencia y criticidad del proveedor en las operaciones y productos de la empresa. Los terceros pueden clasificarse como core y corporativos. Por lo tanto, el área de privacidad es responsable de llevar a cabo la diligencia de estos proveedores, no limitándose a exigir o adoptar mecanismos legitimadores, como estándares internacionales, tales como: Normas corporativas vinculantes; informes de auditoría independientes; certificaciones internacionales como ISO, AICPA SOC 1, SOC 2 y SOC 3; Estándares de seguridad PCI, entre otros).

6.6. Transferencia internacional de datos entre Infracommerce y subsidiarias

Las Transferencias Internacionales de Datos Personales entre Infracommerce y sus subsidiarias deben ocurrir exclusivamente cuando sea estrictamente necesario, vinculadas a fines legítimos y previamente justificadas en el contexto de las operaciones o necesidades justificadas por los titulares de las áreas de negocio.

Todas las transferencias deben ser debidamente registradas por las partes involucradas, con una clara identificación del propósito, las categorías de datos, los destinatarios y las garantías adoptadas.

Estas operaciones deben cumplir con los límites y requisitos establecidos por las leyes de protección de datos aplicables en cada jurisdicción involucrada, incluyendo, cuando sea necesario, la adopción de mecanismos de

Transferencia Internacional reconocidos por las autoridades competentes.

Si tiene alguna duda respecto a qué filiales son, póngase en contacto con el canal de Privacidad o directamente con el responsable, en el tema 6.3 de esta Política.

6.7. Medidas de sensibilización

Infracommerce y sus filiales deben promover acciones continuas de sensibilización y formación en materia de privacidad y protección de datos, con el objetivo de difundir la cultura de protección de datos en todas las unidades y áreas de la organización.

Las iniciativas de sensibilización deben incluir formación general o específica, acciones educativas, campañas de comunicación interna y directrices específicas, de acuerdo con el perfil de desempeño de los equipos. Por lo tanto, la capacitación y asistencia a las áreas de negocio en relación con los temas de esta política será responsabilidad del área de privacidad y protección de datos.

Corresponde a cada unidad regional implementar estas acciones de acuerdo con los lineamientos de esta Política, considerando las particularidades operativas y regulatorias de cada país. La definición de formatos y contenidos se llevará a cabo de acuerdo con el programa global sobre privacidad y protección de datos elaborado por el delegado de Protección de Datos.

6.8. Monitoreo del Programa Global de Privacidad y Protección de Datos

El Programa Global de Privacidad y Protección de Datos incorpora prácticas para monitorear los controles de protección de datos personales.

La medición de los resultados se realizará periódicamente, en un intervalo

no superior a 12 (doce) meses, en base a métricas e indicadores previamente definidos. Los resultados obtenidos servirán de base para que el responsable, siempre que sea necesario, proponga planes de acción correctivos o de mejora de iniciativas, centrándose en abordar los riesgos o debilidades identificados.

Las métricas e indicadores del Programa Global serán propuestos por el responsable y sometidos a la aprobación del Comité de Privacidad y Protección de Datos, asegurando la actualización continua y el cumplimiento de los requisitos regulatorios, operativos y estratégicos de Infracommerce.

El Comité de Privacidad y Protección de Datos tendrá como miembros permanentes a los responsables de la toma de decisiones de seguridad de la información, operaciones y tecnología de la información, infraestructura, marketing y datos, recursos legales y humanos. El responsable es responsable del cronograma y presentación de la agenda ante el comité.

7. RESPONSABILIDADES

Comité de Seguridad de la Información, Privacidad y Protección de Datos

El Comité de Privacidad y Protección de Datos es responsable de:

- Apoyar la definición estratégica del Programa de Privacidad y Protección de Datos de Infracommerce y subsidiarias;
- Resolver sobre la definición estratégica en la identificación de escenarios de amenazas y riesgos para la privacidad, la propiedad intelectual y la gobernanza de datos de Infracommerce y subsidiarias;
- Resolver sobre los riesgos residuales en las actividades de Tratamiento, formalizados por las áreas de negocio;
- Aprobar las métricas e indicadores de desempeño del Programa de Privacidad, con base en una propuesta presentada por el responsable;

- Actuar en caso de incidentes de seguridad, de acuerdo con el plan corporativo aplicable; y
- Fomentar la concienciación, formación y sensibilización de las personas que realizan cualquier actividad de tratamiento de datos personales.

Data Protection Officer (DPO global)

Corresponde a la persona a cargo:

- Participar en proyectos o comités tanto en el lado comercial como en el de seguridad, especialmente en temas relacionados con el gobierno corporativo de datos y los riesgos de la información;
- Comprenda cómo se procesan los datos y determine si las protecciones implementadas cumplen con los requisitos reglamentarios;
- Monitorear el panorama regulatorio global sobre privacidad y protección de datos personales;
- Coordinar, junto con las áreas de negocio, la elaboración y análisis de los Informes de Impacto, cuando corresponda;
- Consolidar y mantener actualizado el inventario de actividades de Tratamiento, con base en la información enviada por las regiones;
- Evaluar las solicitudes de los Titulares, en actividades en las que Infracommerce actúa como Agente de Tratamiento;
- Recibir y manejar comunicaciones de incidentes de seguridad, de acuerdo con el plan corporativo aplicable;
- Proponer y revisar, anualmente, las métricas e indicadores del Programa de Privacidad;
- Apoyar la evaluación de la madurez de terceros y apoyar la definición de cláusulas contractuales relacionadas con la protección de datos;
- Promover acciones para crear conciencia y aculturación de la privacidad, la protección de datos y la propiedad intelectual a nivel institucional; y

- Comunicar formalmente al Comité de Privacidad los riesgos residuales relevantes identificados en el programa;
- Desarrollar el programa de gobernanza de privacidad y protección de datos para Infracommerce y sus subsidiarias;
- Aceptar quejas y comunicaciones de los interesados, proporcionar aclaraciones y adoptar medidas;
- Recibir comunicaciones de las autoridades reguladoras y competentes, en relación con la privacidad y la protección de datos, y adoptar medidas;
- Orientar a los empleados y subcontratistas de Infracommerce y subsidiarias sobre las prácticas a tomar en relación con la privacidad y protección de datos personales;
- Realizar las demás funciones determinadas en su ámbito como agente de transformación o establecidas en normas complementarias;
- Desarrollar las métricas e indicadores de desempeño del Programa de Privacidad;
- Garantizar la implementación efectiva de la gobernanza de datos en las subsidiarias y las respectivas unidades de negocio.

Delegado Local

Corresponde al delegado Local:

- Apoyar a la persona a cargo en la implementación local de la Política y Programa de Gobernanza de Privacidad y Protección de Datos, así como otras pautas corporativas;
- Coordinar, en el territorio bajo su responsabilidad, el levantamiento y actualización del inventario de actividades de procesamiento;
- Actuar como punto de contacto local con los Interesados y las autoridades reguladoras, cuando corresponda;
- Realizar un seguimiento y dar soporte a los incidentes de seguridad en su región, de acuerdo con el plan corporativo aplicable;

- Asegurar, antes de contratar a terceros locales, el cumplimiento de los requisitos de privacidad, de acuerdo con las directrices corporativas;
- Garantizar la adopción, en los contratos locales, de cláusulas apropiadas sobre la protección de los Datos Personales;
- Comunicar incidentes de seguridad y privacidad de manera inoportuna, de acuerdo con el plan corporativo aplicable;
- Apoyar el apoyo de las métricas e indicadores de desempeño del Programa de Privacidad, con base en una propuesta presentada por el responsable;
- Informar al responsable de la visión general de los riesgos operativos, empresariales y de terceros relacionados con el tratamiento de datos en su ubicación;
- Participe en equipos o comités de proyectos tanto en el lado comercial como en el de seguridad;
- Garantizar la ejecución de sesiones de concientización o soporte específicas del negocio, como el seguimiento de solicitudes relacionadas con el procesamiento de datos locales.

Empleados y filiales de Infracommerce

Las responsabilidades de todos los empleados de Infracommerce y subsidiarias son:

- Cumplir con los lineamientos establecidos en esta Política, así como en las normas internas relacionadas con la privacidad y la protección de datos;
- Participar en iniciativas de capacitación y sensibilización promovidas por la organización;
- Cooperar con los procesos de mapeo, evaluación de riesgos y servicio de los interesados, cuando se les solicite; y
- Informar, de buena fe, cualquier incidente, irregularidad o incumplimiento relacionado con el Tratamiento de Datos Personales, a través de los canales institucionales.

Propietarios de áreas de negocio

Corresponde a los responsables y tomadores de decisiones de las áreas de negocio:

- Asegurar que el DPO se involucre en las iniciativas y proyectos de sus áreas desde la concepción del producto y/o servicio a desarrollar, especialmente cuando cubren la protección y el tratamiento de datos personales;
- Asegurar la implementación de la Política, así como de otras directrices corporativas;
- Asegurar, sin excepción, la homologación de sus terceros en los procesos y buenas prácticas establecidas por el área de privacidad y protección de datos;
- Informar de manera inoportuna cualquier incidente de seguridad y privacidad que conozca, incluidos los de sus terceros;
- Apoyar en la manutención de métricas e indicadores de desempeño en el ámbito de la privacidad y la protección de datos, a partir de una propuesta presentada por el responsable;
- Garantizar que la evaluación de la madurez de terceros se defina en los requisitos contractuales relacionados con la privacidad y la protección de datos;
- Asegurar el mantenimiento del inventario de las actividades de Tratamiento y el análisis del impacto en la privacidad de su área de negocio;

8. NO CUMPLIMIENTO

Las violaciones, aunque sean por omisión, de las reglas establecidas en esta Política estarán sujetas a sanciones que serán evaluadas con base en las políticas internas de Infracommerce y subsidiarias. Sin embargo, la empresa se reserva el derecho de adoptar los mecanismos legales y judiciales que correspondan a los casos de violación y/o incumplimiento de las políticas internas de la empresa. Las violaciones de la política y las leyes aplicables pueden dar lugar a sanciones significativas impuestas por las Autoridades Competentes de Protección de Datos en cada país, que pueden incluir multas elevadas (por ejemplo, hasta el 2% de la facturación global o millones de

dólares), suspensión de las actividades de tratamiento o prohibición de acceso a las bases de datos.

9. VIGENCIA

Esta Política entrará en vigor en la fecha de su publicación, cuando su contenido será comunicado en los canales públicos oficiales de la empresa, y se derogarán todas y cada una de las disposiciones anteriores en contrario.

10. ACTUALIZACIONES Y DUDAS

La necesidad de actualizar la Política debe ser verificada por el responsable, al menos una vez al año o en cualquier momento, previa justificación.

Las preguntas sobre las reglas establecidas en esta Política o sobre el Programa de Privacidad de Infracommerce y subsidiarias deben enviarse a través del canal dpo@infracommerce.com.br.

11. ANEXOS:

Marco jurídico y reglamentario de referencia

Esta política está referenciada por las siguientes leyes y regulaciones de nuestras subsidiarias en los siguientes países:

País	Ley/ Reglamento	Documento	Año (Versión actual)	Fuente de Consulta	Transparancia (Aviso + Arco)	Terceros (Compartición)
Brasil	Lei Geral de Proteção de Dados Pessoais (LGPD)	Lei n° 13.709/2018	2018	Portal ANPD / Gov.br	LGPD ARCO + Aviso claro	Consentimento + Aviso
México	Ley Federal de Protección de Datos Personales en Posesión de Particulares	LFPDPPP, Ley Federal	2010	Diário Oficial DAON-5/jul/2010	ARCO + Aviso obrigatório	Consentimento + Aviso

Argentina	Ley de Protección de Datos Personales (Ley 25.326)	Ley 25.326 e Decreto 1558/2001 (e alterações recentes)	2000 (vigência); atualizações até 2023	Portal AAIP / Argentina.gob.ar	Informações claras	Aviso sobre destinatários
Peru	Ley de Protección de Datos Personales	Ley Nº 29733 (aplicável desde 2011, implementação iniciada 2015)	2011	Diário Oficial El Peruano / site do congresso peruano	Aviso + Direitos básico	Consentimento obrigatório
Colômbia	Ley Estatutaria 1581 de 2012 + Decreto regulamentador 1377 de 2013	Ley 1581 de 2012	2012	Diário Oficial / SIC (Superintendência de Indús	Transparência constitucional	Consentimento necessário
Chile	Ley Nº 19.628 sobre Protección de la Vida Privada	Ley 19.628	1999 (atualizações posteriores disponíveis online)	Biblioteca del Congreso Nacional de Chile	Aviso + Direito de oposição	Consentimento obrigatório
Uruguai	Ley Nº 18.331 – Protección de Datos Personales + Lei 19.030 (Convênio 108)	Ley 18.331 (2008); modificado por Ley 20075/2022 (vigente desde 2023)	2022/2023	Registro Oficial de Uruguay	Acesso público + Habeas data	Consentimento ou Lei.
Panamá	Ley 81 de 2019 – Protección de Datos Personales + Decreto 285/2021	Ley 81/2019 e Reglamento Decreto 285/2021	2019 (em vigor desde 29/mar/2021)	Autoridad Transparencia – ANTAI (Panamá)	Consentimento + Aviso	Consentimento + Aviso

12. INFORMACIONES DEL DOCUMENTO

Responsable de la Política	Data Protection Officer
Clasificación de la Información	Público

12.1. REVISIÓN Y MANTENIMIENTO

Esta Política Global de Privacidad de Datos se revisará anualmente o cuando se produzca un cambio significativo en la organización.

Este documento fue aprobado el: 04/08/2025.

13. VERSIONES DEL DOCUMENTO

Versión	Fecha	Editor / Revisor	comentarios
1.0	01/07/2025	Departamento de Privacidad y Protección de Datos	Versión inicial de la política global de privacidad y protección de datos

14. APROBACIÓN DEL DOCUMENTO

APROBADORES (CGSI)	CARGO	FECHA
Mariano Oriozabala	CEO	04/08/2025
César Gulam	General Manager LATAM	04/08/2025
Luiz Pavão	General Manager BRASIL	04/08/2025
Maria Elvira Saldaña	CHRO	04/08/2025
Iñaki Algañaras	CMO	04/08/2025
Bruno Vasques	CFO GLOBAL	04/08/2025
Leonardo Gabriel Landolfi	CISO	04/08/2025