Envelope ID: bCNd75ZXVt

PO-TD-IT-8.
"Política Regional de Protección de Datos"

Seguridad de la Información

Envelope ID: bCNd75ZXVt

1. Introducción y compromiso corporativo

LATAM TRADE CAPITAL, sus filiales y empresas relacionadas (en adelante "LTC" o "el Grupo") desarrollan operaciones de factoring y financiamiento en Colombia, Chile y Perú, tres jurisdicciones con regímenes de protección de datos personales autónomos, con autoridades, definiciones, plazos y obligaciones propias.

El Grupo garantiza la protección de los derechos de hábeas data, privacidad, intimidad, buen nombre e imagen de las personas cuyos datos trata, y asume como estándar corporativo el cumplimiento riguroso del régimen de cada jurisdicción donde opera.

La presente Política Marco responde a una restricción jurídica estructural: el consentimiento del titular debe ser informado bajo la legislación específica que le aplica. En Colombia, los artículos 9 de la Ley 1581 de 2012 y 12 del Decreto 1377 de 2013 (incorporado en el Decreto 1074 de 2015) exigen que el titular conozca con precisión el responsable, las finalidades y sus derechos; exigencias equivalentes existen en la Ley 29733 del Perú y en la Ley 19.628 de Chile (según el texto de la Ley 21.719). Ninguna autorización obtenida bajo un régimen puede extenderse válidamente a las obligaciones de otro. Por ello, este documento no sustituye a los instrumentos locales: los organiza.

2. Objetivo

Establecer el marco corporativo común de protección de datos personales del Grupo (principios, gobierno, estándares de seguridad, gestión de terceros, flujos intragrupo y proceso interno de incidentes) y definir la arquitectura documental mediante la cual cada jurisdicción desarrolla, en su anexo, las obligaciones específicas frente a sus titulares y su autoridad.

3. Alcance

3.1. Modelo: marco + anexos jurisdiccionales

El sistema documental de protección de datos del Grupo se compone de esta Política Marco y de un anexo por jurisdicción. El marco contiene lo que es decisión corporativa y no depende de la ley local; los anexos contienen todo aquello que produce efectos frente al titular o la autoridad local.

3.2. Regla de prevalencia

En caso de conflicto entre esta Política Marco y un anexo jurisdiccional, prevalece el anexo. La normativa local es imperativa; el marco es política corporativa y en ningún caso reduce las protecciones que la ley de cada país otorga a sus titulares

La información contenida en este documento es estrictamente de **uso interno** y pertenece exclusivamente a LATAM TRADE CAPITAL por lo que no deberá ser divulgada, ni transmitida a personas ajenas a la Institución, sin previa aprobación formal. Su contenido deberá ser acatado en todas sus partes

Envelope ID: bCNd75ZXVt

3.3. Reglas de publicación y de instrumentos

- En cada país se publica al titular el consolidado compuesto por esta Política Marco y el anexo de su jurisdicción. Los anexos de otras jurisdicciones no forman parte de la información dirigida a ese titular.
- Las autorizaciones, avisos de privacidad y demás instrumentos dirigidos al titular referencian únicamente el anexo local, que es donde constan el responsable identificado, las finalidades y los derechos que hacen del consentimiento uno informado.
- Ningún instrumento del Grupo solicitará al titular aceptar el tratamiento bajo legislaciones distintas a la suya.

3.4. Relación con el Sistema de Gestión de Seguridad de la Información

El Grupo cuenta con instrumentos regionales de seguridad de la información que son plenamente aplicables y que esta Política no sustituye ni duplica:

Código	Documento	Relación con esta Política
PO-TD-IT-6	Política de Gestión de Incidentes de Seguridad de la Información	Rige el gobierno del incidente: severidad, SLA, matriz RACI y matriz de comunicación. Esta Política añade la capa de protección de datos (sección 11).
P-TD-IT-1	Procedimiento regional de gestión de incidentes de seguridad de la información	Ejecuta las fases operativas del incidente. Su fase de reporte externo se ejecuta conforme a la sección A.12 del anexo de la jurisdicción afectada.

Regla de articulación: los instrumentos del SGSI gobiernan el proceso operativo del incidente (cómo se detecta, clasifica, contiene y cierra). Esta Política y sus anexos gobiernan las obligaciones exigibles cuando el incidente involucra datos personales (a quién se notifica, en qué plazo y con qué contenido). Ninguno de los dos cuerpos documentales reemplaza al otro y ambos deben leerse de forma conjunta.

4. Marco Normativo

Cada anexo desarrolla su régimen con citas de nivel de artículo. A nivel de marco, los regímenes de referencia son:

La información contenida en este documento es estrictamente de **uso interno** y pertenece exclusivamente a LATAM TRADE CAPITAL por lo que no deberá ser divulgada, ni transmitida a personas ajenas a la Institución, sin previa aprobación formal. Su contenido deberá ser acatado en todas sus partes

Envelope ID: bCNd75ZXVt

- **Colombia:** Ley Estatutaria 1581 de 2012; Ley 1266 de 2008 (modificada por la Ley 2157 de 2021); Decreto 1074 de 2015; Circular Única de la SIC, Título V; Circulares Externas 001 y 002 de 2025 de la SIC.
- **Chile:** Ley 19.628 (régimen transicional vigente) y Ley 21.719 (plena vigencia en diciembre de 2026), con el régimen gradual de sanciones para empresas de menor tamaño de la Ley 20.416.
- **Perú:** Ley 29733 y su reglamento aprobado por el D.S. 016-2024-JUS, en plena vigencia desde marzo de 2025.

La convergencia material entre estos regímenes (principios, deber de seguridad, gestión de encargados, notificación de incidentes y control de transferencias internacionales) es lo que hace viable un marco común; sus divergencias (titulares cubiertos, plazos, registros y autoridades) son lo que hace obligatorios los anexos.

5. Definiciones

A efectos operativos de esta Política Marco se emplean las siguientes definiciones funcionales:

- **Dato personal:** información vinculada o asociable a una persona identificada o identificable, en el alcance que la ley de cada jurisdicción determine.
- **Tratamiento:** cualquier operación sobre datos personales: recolección, almacenamiento, uso, circulación, transferencia o supresión.
- **Tercero procesador:** persona natural o jurídica que trata datos por cuenta de una entidad del Grupo (encargado, mandatario u homólogo según la ley local).
- **Incidente de seguridad:** evento que comprometa la confidencialidad, integridad o disponibilidad de datos personales bajo responsabilidad del Grupo.
- **Transferencia internacional:** todo flujo de datos personales desde una jurisdicción hacia otra, incluidas las demás entidades del Grupo.
- **Anexo jurisdiccional:** documento que desarrolla, para un país, las obligaciones específicas de su régimen y forma parte integral de esta Política.

Las definiciones con efectos jurídicos, en particular “Titular”, “dato sensible” y los roles de responsable y encargado, se definen exclusivamente en cada anexo. La razón es sustantiva: en Colombia, la Ley 1266 de 2008 reconoce como titulares de información financiera, crediticia, comercial y de servicios tanto a personas naturales como jurídicas, mientras que los regímenes generales colombiano (Ley 1581), chileno y peruano protegen a personas naturales. Una definición única de “Titular” en el marco sería incorrecta en al menos una jurisdicción.

La información contenida en este documento es estrictamente de **uso interno** y pertenece exclusivamente a LATAM TRADE CAPITAL por lo que no deberá ser divulgada, ni transmitida a personas ajenas a la Institución, sin previa aprobación formal. Su contenido deberá ser acatado en todas sus partes

Envelope ID: bCNd75ZXVt

6. Disposiciones Generales

6.1. Principios Comunes

El Grupo adopta como estándar corporativo los principios que convergen en los tres regímenes. La siguiente tabla identifica el anclaje normativo de cada principio; su desarrollo y consecuencias específicas corresponden a cada anexo.

Principio	Colombia	Chile	Perú
Legalidad / licitud	art. 4 lit. a, Ley 1581	art. 3º, Ley 19.628 (texto Ley 21.719)	art. 4, Ley 29733
Finalidad	art. 4 lit. b, Ley 1581	art. 3º, Ley 19.628 (texto Ley 21.719)	art. 6, Ley 29733
Libertad / consentimiento	art. 4 lit. c y art. 9, Ley 1581	consentimiento como base de licitud (Ley 21.719)	arts. 5 y 13, Ley 29733
Calidad / veracidad	art. 4 lit. d, Ley 1581	art. 3º, Ley 19.628 (texto Ley 21.719)	art. 8, Ley 29733
Transparencia e información	art. 4 lit. e, Ley 1581	art. 3º, Ley 19.628 (texto Ley 21.719)	art. 18, Ley 29733
Proporcionalidad / minimización	derivado del principio de finalidad (art. 4 lit. b)	art. 3º, Ley 19.628 (texto Ley 21.719)	art. 7, Ley 29733
Seguridad	art. 4 lit. g y art. 17 lit. d, Ley 1581	art. 3º y deberes del responsable (Ley 21.719)	art. 9, Ley 29733 y su reglamento
Confidencialidad	art. 4 lit. h, Ley 1581	art. 3º, Ley 19.628 (texto Ley 21.719)	art. 17, Ley 29733
Responsabilidad demostrada	art. 2.2.2.25.6.1, Decreto 1074/2015	principio de responsabilidad, art. 3º (Ley 21.719)	medidas de cumplimiento del D.S. 016-2024-JUS

Nota: *las citas de Chile corresponden al texto de la Ley 19.628 según las modificaciones de la Ley 21.719, cuya plena vigencia inicia en diciembre de 2026. El Anexo II desarrolla el régimen transicional aplicable hasta esa fecha.*

La información contenida en este documento es estrictamente de **uso interno** y pertenece exclusivamente a LATAM TRADE CAPITAL por lo que no deberá ser divulgada, ni transmitida a personas ajenas a la Institución, sin previa aprobación formal. Su contenido deberá ser acatado en todas sus partes

Envelope ID: bCNd75ZXVt

6.2. Modelo de gobierno

Comité de Seguridad de Datos (regional): supervisa el cumplimiento de esta Política y de los anexos, aprueba sus actualizaciones, conoce los incidentes relevantes y las evaluaciones de terceros críticos.

Función local de protección de datos: cada jurisdicción cuenta con una persona o área designada, identificada en su anexo, con acceso directo a la alta dirección. La forma de la designación responde a cada régimen: en Colombia es exigible la designación de una persona o área (art. 2.2.2.25.4.4, Decreto 1074/2015); en Perú, el D.S. 016-2024-JUS hace obligatorio el Oficial de Datos Personales para las entidades que alcanzan los umbrales allí previstos; en Chile, la designación de delegado es voluntaria para entidades privadas bajo la Ley 21.719, sin perjuicio de que el Grupo la adopte como buena práctica, siendo centralizado en el cargo "DPO- Delegado de protección de Datos Regional".

Propietarios de datos: cada conjunto de datos tiene un propietario responsable de su manejo conforme a esta Política y al anexo aplicable.

> **Equivalencia de órganos:** el Comité de Seguridad de Datos referido en esta Política es el mismo órgano denominado Comité de Seguridad de la Información en la PO-TD-IT-6, y se activa conforme a los criterios de severidad allí previstos. El Delegado de Protección de Datos (DPO) regional integra la función de protección de datos del Grupo y participa en la gestión de incidentes con el rol que le asigna la matriz RACI de la PO-TD-IT-6. La función local de protección de datos de cada jurisdicción reporta al DPO regional.

6.3. Estándares comunes de seguridad

Los tres regímenes imponen un deber de seguridad sobre los datos personales. El Grupo lo satisface con un estándar técnico único, aplicado en las tres jurisdicciones al nivel más exigente dimensión por dimensión:

- Control de acceso basado en roles (RBAC) con revisión periódica de permisos.
- Autenticación multifactor (MFA) para sistemas críticos y datos clasificados como confidenciales o sensibles.
- Cifrado de datos sensibles y confidenciales en reposo y de todo dato en tránsito (TLS, VPN).
- Clasificación de la información; el dato más restrictivo de un conjunto determina el nivel de protección de todo el conjunto.
- Respaldos periódicos cifrados y procedimientos de recuperación ante desastres.
- Pruebas de seguridad periódicas (penetración y vulnerabilidades) y gestión de parches.

La información contenida en este documento es estrictamente de **uso interno** y pertenece exclusivamente a LATAM TRADE CAPITAL por lo que no deberá ser divulgada, ni transmitida a personas ajenas a la Institución, sin previa aprobación formal. Su contenido deberá ser acatado en todas sus partes

Envelope ID: bCNd75ZXVt

- Registro y monitoreo de accesos a datos personales.

6.4. Gestión de terceros y procesadores

Todo tercero que acceda reciba o trate datos personales por cuenta del Grupo se sujeta al siguiente proceso corporativo común:

- Evaluación previa mediante el instrumento corporativo de evaluación de proveedores, incluida su sección de protección de datos personales.
- Suscripción del instrumento contractual que corresponda según el anexo local (contrato de transmisión en Colombia conforme al Decreto 1074/2015; contrato de encargo o su equivalente en Chile y Perú), con cláusulas de confidencialidad, seguridad y protocolo de incidentes que incluya la obligación de notificar a LTC dentro de las 24 horas siguientes a la detección, conforme a la sección 11.2.
- Prohibición contractual expresa de que el tercero use los datos para fines propios; su incumplimiento reclasifica la operación y activa las consecuencias del régimen local de transferencias.
- Supervisión continua y derecho de auditoría durante la vigencia de la relación.

La ley aplicable al tratamiento se determina por el país donde ocurre el tratamiento y por el régimen del responsable que lo ordena, no por la ubicación del proveedor.

6.5. Flujos intragrupo y transferencias internacionales

Los flujos de datos entre entidades del Grupo son transferencias internacionales y se rigen por el régimen del país exportador. Reglas corporativas:

- Cada flujo intragrupo se instrumenta mediante un acuerdo de transferencia o de flujo transfronterizo que cumpla el mecanismo previsto en el anexo del país exportador (en Colombia, el art. 26 de la Ley 1581 y el listado de países con nivel adecuado de la SIC o la declaración de conformidad; en Perú, el régimen de flujo transfronterizo de la Ley 29733 y su reglamento; en Chile, el régimen de la Ley 21.719 según su vigencia).
- El consentimiento del titular se obtiene únicamente bajo su ley local. Ninguna entidad del Grupo empleará autorizaciones que pretendan cubrir simultáneamente los tres regímenes.
- Todas las transferencias se registran y quedan disponibles para auditoría.

La información contenida en este documento es estrictamente de **uso interno** y pertenece exclusivamente a LATAM TRADE CAPITAL por lo que no deberá ser divulgada, ni transmitida a personas ajenas a la Institución, sin previa aprobación formal. Su contenido deberá ser acatado en todas sus partes

Envelope ID: bCNd75ZXVt

6.6. Gestión de Incidentes de Seguridad

6.6.1. Proceso Operativo: remisión al SGSI

El proceso operativo de gestión de incidentes del Grupo está definido en la Política de Gestión de Incidentes de Seguridad de la Información (PO-TD-IT-6) y en el Procedimiento regional de gestión de incidentes de seguridad de la información (P-TD-IT-1), ambos de aplicación en las tres jurisdicciones. Se aplican íntegramente el modelo de severidad, los acuerdos de nivel de servicio, la matriz RACI, la matriz de comunicación y las fases operativas allí previstas, sin modificación por esta Política.

6.6.2. Capa de protección de datos personales

Cuando un incidente comprometa o pueda comprometer datos personales, se aplican adicionalmente las siguientes reglas:

- **Activación de la función de protección de datos.** Todo incidente que involucre datos personales se comunica al DPO regional y a la función local de protección de datos dentro de las 24 horas siguientes a su detección, cualquiera sea la severidad asignada conforme al modelo de la PO-TD-IT-6, incluidas las severidades Media y Baja. La razón es que el plazo regulatorio no depende de la severidad interna del incidente.
- **Inicio del reloj regulatorio.** El plazo de notificación externa se cuenta desde la detección del incidente, no desde su confirmación, su clasificación final ni su contención. Que el incidente ya se encuentre contenido no suspende ni extingue la obligación de notificar.
- **Decisión de notificación externa.** La decisión prevista en el P-TD-IT-1 para la fase de reporte externo se adopta dentro de las 48 horas siguientes a la detección, con concepto obligatorio del DPO y del área Legal. La decisión y su fundamento se documentan, incluso cuando se concluya que no procede notificar.
- **Ejecución de la notificación.** El reporte externo se ejecuta conforme a la sección A.12 del anexo de la jurisdicción afectada, que determina la autoridad competente, el plazo, el contenido, el canal y la procedencia de comunicar a los titulares.
- **Incidentes originados en terceros.** Los contratos con terceros que traten datos personales por cuenta del Grupo deben obligar al tercero a notificar a LTC dentro de las 24 horas siguientes a su detección del incidente. El plazo regulatorio del Grupo corre desde esa detección por el tercero, no desde su comunicación a LTC.

La información contenida en este documento es estrictamente de **uso interno** y pertenece exclusivamente a LATAM TRADE CAPITAL por lo que no deberá ser divulgada, ni transmitida a personas ajenas a la Institución, sin previa aprobación formal. Su contenido deberá ser acatado en todas sus partes

Envelope ID: bCNd75ZXVt

6.6.3. Plazos regulatorios de referencia

El reloj interno del proceso se calibra al plazo externo más estricto del Grupo:

País	Plazo de notificación a la autoridad	Fuente
Perú	48 horas ante la ANPD	D.S. 016-2024-JUS
Colombia	15 días hábiles ante la SIC, vía RNBD	Título V, Circular Única SIC; Guía de Incidentes 2020
Chile	"Sin dilaciones indebidas" ante la Agencia	Ley 21.719 (autoridad en proceso de instalación)

El plazo peruano de 48 horas es el más estricto del Grupo y corre incluso si el incidente ya se encuentra controlado. Por ello calibra el reloj interno: un proceso capaz de cumplirlo satisface automáticamente el plazo colombiano de 15 días hábiles y el estándar chileno de "sin dilaciones indebidas". Los acuerdos de nivel de servicio de la PO-TD-IT-6 miden la respuesta técnica interna y no sustituyen estos plazos regulatorios, que son independientes de la severidad asignada.

6.6.4. Registro del incidente

El registro se realiza en el aplicativo corporativo conforme al P-TD-IT-1. Cuando el incidente involucre datos personales, el registro incorporará adicionalmente, como mínimo:

- Las bases de datos y las categorías de datos comprometidos, con indicación de si incluyen datos sensibles.
- Las categorías y el número aproximado de titulares afectados y su jurisdicción.
- La fecha y hora de ocurrencia y de detección del incidente.
- La evaluación del nivel de riesgo para los titulares y los factores considerados.
- Las medidas correctivas adoptadas.
- La prueba de la notificación a la autoridad y de la comunicación a los titulares, o la decisión motivada de no notificar.

6.7. Capacitación y cultura

Todos los colaboradores y terceros que traten datos personales reciben capacitación periódica sobre esta Política y sobre el anexo de su jurisdicción. El Grupo mantiene campañas de concientización continuas sobre amenazas y buenas prácticas.

La información contenida en este documento es estrictamente de **uso interno** y pertenece exclusivamente a LATAM TRADE CAPITAL por lo que no deberá ser divulgada, ni transmitida a personas ajenas a la Institución, sin previa aprobación formal. Su contenido deberá ser acatado en todas sus partes

Envelope ID: bCNd75ZXVt

6.8. Ejercicio de derechos de los titulares

El Grupo garantiza a los titulares el ejercicio pleno y efectivo de los derechos que su ley local les reconoce. El catálogo de derechos, los plazos de atención, los canales y los procedimientos se establecen íntegramente en cada anexo, por ser materia reservada al régimen local. Ningún plazo de atención se fija en esta Política.

6.9. Revisión, actualización y control documental

- Esta Política se revisa al menos una vez al año o ante cambios normativos u operativos relevantes.
- Cada anexo tiene su versión independiente: puede actualizarse sin modificar el marco ni los demás anexos. Ejemplo previsto: el Anexo II (Chile) deberá actualizarse hacia diciembre de 2026 con la plena vigencia de la Ley 21.719.
- Toda modificación del marco o de un anexo es aprobada por el Comité de Seguridad de Datos y comunicada a los interesados.

7. Anexos

- Anexo I – Colombia Base: política local PO-TD-COL-001 v2.0.
- Anexo II – Chile Base: Política Regional PO-TD-1. “POLÍTICA REGIONAL DE MANEJO DE DATOS”
- Anexo III – Base: Política Regional Perú PO-TD-1. “POLÍTICA REGIONAL DE MANEJO DE DATOS”

8. Control de Cambios

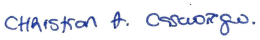
Fecha de Elaboración	Versión	Descripción de la Modificación
25/02/2025	1.0	Creación del primer ejemplar (política regional unificada).
28/07/2026	2.0	Conversión al modelo de Política Marco + anexos jurisdiccionales. Se retiran del marco las materias reservadas a la ley local (titulares, finalidades, plazos, registros, notificaciones a autoridad) y se incorporan la regla de prevalencia, las reglas de publicación e instrumentos, el

La información contenida en este documento es estrictamente de **uso interno** y pertenece exclusivamente a LATAM TRADE CAPITAL por lo que no deberá ser divulgada, ni transmitida a personas ajenas a la Institución, sin previa aprobación formal. Su contenido deberá ser acatado en todas sus partes

Envelope ID: bCNd75ZXVt

		estándar único de seguridad, el proceso de incidentes con reloj interno de 48 horas y la plantilla estándar de anexo.

9. Firmas

Control Documental		
Elaborado	Revisado	Aprobado
Andrea Moyano **DPO- Delegado de protección de Datos Regional** Nicolas Garcés **Jefe Legal**	Christian Casadiego **CISO – Chief Information Security Officer**	**Directorio** Oswaldo Sandoval **Director** Karla García **Directora**
		

La información contenida en este documento es estrictamente de **uso interno** y pertenece exclusivamente a LATAM TRADE CAPITAL por lo que no deberá ser divulgada, ni transmitida a personas ajenas a la Institución, sin previa aprobación formal. Su contenido deberá ser acatado en todas sus partes

Envelope ID: bCNd75ZXVt

Apéndice – Plantilla estándar de anexo jurisdiccional

Todo anexo sigue la estructura siguiente, con citas normativas de nivel de artículo. Las secciones son paralelas entre los tres países para facilitar auditoría y comparación; la sección A.13 recoge las particularidades que no deben trasladarse a las demás jurisdicciones.

Sección	Título	Contenido mínimo
A.1	**Responsables locales**	Razón social, identificación tributaria, domicilio, teléfono, correo y página web de cada entidad responsable.
A.2	**Marco normativo local**	Leyes, reglamentos, circulares y guías de la autoridad, citados por artículo.
A.3	**Definiciones legales**	Titular, dato personal, dato sensible, responsable, encargado y demás categorías del régimen local.
A.4	**Titulares cubiertos**	Personas naturales directas; personas naturales vinculadas a personas jurídicas; personas jurídicas cuando el régimen local las reconozca como titulares.
A.5	**Finalidades**	Segmentadas por grupo de interés. La distinción necesaria/accesorias solo si el régimen local la exige.
A.6	**Autorización y excepciones**	Requisitos del consentimiento, medios de obtención y excepciones legales.
A.7	**Derechos y plazos**	Catálogo local de derechos y plazos de atención de consultas y reclamos.
A.8	**Canales de atención**	Canal, área designada y procedimiento local.
A.9	**Datos sensibles y menores**	Régimen reforzado local.
A.10	**Transferencias internacionales**	Mecanismo local aplicable a flujos salientes, incluidos los intragrupo.
A.11	**Registros ante autoridad**	RNBD en Colombia; registro de banco de datos ante la ANPD en Perú; los que la Ley 21.719 llegue a exigir en Chile.
A.12	**Notificación de incidentes**	Autoridad competente, plazo, contenido y canal; comunicación a titulares.
A.13	**Particularidades locales**	Colombia: régimen dual Ley 1581/Ley 1266, preaviso del art. 12 Ley 1266 (Ley 2157/2021), finalidades necesarias/accesorias y decisiones automatizadas (CE 001/2025), RNBD. Perú: Oficial de Datos Personales

La información contenida en este documento es estrictamente de **uso interno** y pertenece exclusivamente a LATAM TRADE CAPITAL por lo que no deberá ser divulgada, ni transmitida a personas ajenas a la Institución, sin previa aprobación formal. Su contenido deberá ser acatado en todas sus partes

Envelope ID: bCNd75ZXVt

		obligatorio según umbrales del D.S. 016-2024-JUS. Chile: régimen transicional Ley 19.628 vs. plena vigencia Ley 21.719 (dic. 2026).
A.14	**Formatos locales**	Autorización de tratamiento y avisos de privacidad por audiencia, referenciando este anexo.

La información contenida en este documento es estrictamente de **uso interno** y pertenece exclusivamente a LATAM TRADE CAPITAL por lo que no deberá ser divulgada, ni transmitida a personas ajenas a la Institución, sin previa aprobación formal. Su contenido deberá ser acatado en todas sus partes