

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		CÓDIGO: GSI-PO-004-PA
	POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES		VERSIÓN: 1.0
			FECHA: 25/09/2026

CONTENIDO

CAPÍTULO I. Datos generales de ULTRAGP PA, S.A. como responsable del tratamiento.....	2
CAPÍTULO II. Objetivo	2
CAPÍTULO III. Alcance	3
CAPÍTULO IV. Marco normativo	4
CAPÍTULO V. Definiciones	4
CAPÍTULO VI. Principios que orientan el tratamiento	5
CAPÍTULO VII. Finalidades del tratamiento	6
CAPÍTULO VIII. Licitud del tratamiento y consentimiento del titular	8
CAPÍTULO IX. Tratamiento de datos personales.....	9
CAPÍTULO X. Revocatoria del consentimiento y supresión de datos	10
CAPÍTULO XI. Derechos de los titulares	11
CAPÍTULO XII. Procedimiento para consultas y reclamos	12
CAPÍTULO XIII. Deberes del responsable del tratamiento	13
CAPÍTULO XIV. Uso de cookies y medios digitales	14
CAPÍTULO XV. Transferencia y flujo transfronterizo de datos personales	15
CAPÍTULO XVI. Oficial de protección de datos personales	15
CAPÍTULO XVII. Registro de bases de datos	16
CAPÍTULO XVIII. Protocolo ante vulneración de datos personales	16
CAPÍTULO XIX. Evaluación preliminar de impacto en la privacidad	17
CAPÍTULO XX. Tratamiento de datos personales mediante sistemas y agentes de inteligencia artificial.....	17
CAPÍTULO XXI. Régimen sancionatorio y responsabilidad.....	18
CAPÍTULO XXII. Modificación de la política	19
CAPÍTULO XXIII. Control de cambios	19

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: GSI-PO-004-PA
	POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES	VERSIÓN: 1.0
		FECHA: 25/09/2026

CAPÍTULO I

DATOS GENERALES DE ULTRAGP PA, S.A. COMO RESPONSABLE DEL TRATAMIENTO

Razón social: ULTRAGP PA, S.A.

RUC: 155745300-2-2023

Domicilio principal: Provincia de Panamá, Distrito de Panamá, Corregimiento de Betania, Urbanización Locería, Calle Ricardo J. Alfaro, Edificio Centro Comercial Siglo XXI, tercer piso, oficina N.º 53, República de Panamá

Teléfono B2C: (507) 8386942

Teléfono B2B: (507) 8335796

Correo electrónico: notificaciones@linextravel.com

Sitio web: <https://panama.linexgo.com/>

ULTRAGP PA, S.A. es una sociedad constituida y domiciliada en la República de Panamá, que forma parte del grupo empresarial al que pertenece STRATEGIC POINTS S.A.S. y que opera bajo las marcas Linex Travel, Linex Loyalty, Linex Trip y Linex GO. Para efectos de la presente política actúa como responsable del tratamiento de los datos personales que recolecta en el desarrollo de su objeto social en territorio panameño.

Cuando el titular acceda a los portales o canales digitales de cualquiera de las marcas del grupo y contrate servicios con ULTRAGP PA, el responsable del tratamiento de sus datos personales es ULTRAGP PA, S.A., y no las demás sociedades del grupo, sin perjuicio de que estas puedan actuar como encargadas del tratamiento en los términos del Capítulo correspondiente de esta política.

CAPÍTULO II

OBJETIVO

La presente política tiene como objetivo establecer los principios, directrices, responsabilidades y mecanismos mediante los cuales ULTRAGP PA, S.A. garantiza una gestión adecuada, segura, transparente y lícita de los datos personales que trata en el ejercicio de sus actividades, conforme a la Ley 81 del 26 de marzo de 2019, sobre

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		CÓDIGO: GSI-PO-004-PA
	POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES		VERSIÓN: 1.0
			FECHA: 25/09/2026

Protección de Datos Personales, vigente desde el 29 de marzo de 2021 y a su reglamento.

Adicionalmente, ULTRAGP PA, como entidad que interviene en la administración de datos financieros y en el procesamiento de pagos, se compromete a cumplir con los estándares de seguridad definidos por el Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS), integrándolos como parte de este marco de tratamiento y protección de datos personales.

Este objetivo abarca tres líneas estratégicas:

1. Garantizar los derechos de los titulares y el cumplimiento estricto de la normativa panameña sobre protección de datos personales.
2. Integrar estándares internacionales de seguridad, en especial PCI DSS, en la administración de datos personales y financieros.
3. Promover una cultura de seguridad y privacidad, asegurando que colaboradores, proveedores y terceros que intervienen en el tratamiento cumplan los controles y obligaciones aquí descritos.

CAPÍTULO III

ALCANCE

Esta política aplica a:

1. Empleados, exempleados y candidatos.
2. Clientes, usuarios y titulares de información financiera.
3. Proveedores, contratistas, aliados estratégicos y terceros.
4. Visitantes y cualquier persona natural cuyos datos sean tratados.
5. Todas las sedes físicas, sistemas tecnológicos, procesos, canales y soportes utilizados para el tratamiento de datos personales.

Comprende todas las bases de datos y tratamientos administrados por ULTRAGP PA, así como aquellos gestionados por encargados del tratamiento bajo relación contractual.

Esta política se aplica a los tratamientos de datos personales sujetos a la legislación de Panamá. Los tratamientos realizados por otras sociedades del grupo se rigen por la política correspondiente a su propia jurisdicción.

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: GSI-PO-004-PA
	POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES	VERSIÓN: 1.0
		FECHA: 25/09/2026

CAPÍTULO IV

MARCO NORMATIVO

Esta política se fundamenta en:

1. Constitución Política de la República de Panamá, artículo 44 derecho de habeas data.
2. Ley 81 del 26 de marzo de 2019, sobre Protección de Datos Personales.
3. Decreto Ejecutivo 285 del 28 de mayo de 2021, que reglamenta la Ley 81 de 2019.
4. Ley 6 de 2002, sobre transparencia en la gestión pública y habeas data, en lo pertinente.
5. Resoluciones, guías y modelos que expida la ANTAI a través de la Dirección de Protección de Datos Personales.
6. PCI DSS (Payment Card Industry Data Security Standard), aplicable a las organizaciones que procesan, transmiten o almacenan datos de tarjetas de pago.

CAPÍTULO V

DEFINICIONES

Se adoptan las definiciones de la Ley 81 de 2019 y de su reglamento, entre ellas:

1. **Titular:** Persona natural cuyos datos personales son objeto de tratamiento.
2. **Dato personal:** Cualquier información vinculada o que pueda asociarse a una persona natural identificada o identificable.
3. **Datos sensibles:** Datos que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación: origen étnico o racial, convicciones religiosas o filosóficas, afiliación sindical, opiniones políticas, datos relativos a la salud, la vida u orientación sexual, datos genéticos y datos biométricos.
4. **Dato financiero o transaccional:** Información relacionada con métodos de pago, tarjetas, historiales de compra o transacciones electrónicas, protegida mediante los estándares PCI DSS.
5. **Responsable del tratamiento:** Persona natural o jurídica que decide sobre la finalidad y el contenido del tratamiento.
6. **Encargado del tratamiento:** Persona natural o jurídica que trata datos personales por cuenta y bajo instrucciones del responsable.

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: GSI-PO-004-PA
	POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES	VERSIÓN: 1.0
		FECHA: 25/09/2026

7. **Consentimiento:** Manifestación de voluntad libre, específica, informada e inequívoca del titular que autoriza el tratamiento de sus datos.
8. **Tratamiento:** Cualquier operación sobre datos personales: recolección, registro, almacenamiento, uso, circulación, transferencia o supresión.
9. **Base de datos o banco de datos:** Conjunto organizado de datos personales sometidos a tratamiento.
10. **Vulneración de seguridad:** Incidente que ocasione la destrucción, pérdida, alteración, comunicación o acceso no autorizado a datos personales.
11. **Elaboración de perfiles:** Tratamiento automatizado destinado a evaluar aspectos personales del titular, en particular para analizar o predecir su comportamiento.
12. **Autoridad de control:** Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI), a través de la Dirección de Protección de Datos Personales.

CAPÍTULO VI

PRINCIPIOS QUE ORIENTAN EL TRATAMIENTO

Los principios que se enuncian a continuación constituyen el marco fundamental bajo el cual ULTRAGP PA realiza el tratamiento de datos personales:

1. **Lealtad:** Los datos se obtienen y tratan sin engaño ni medios fraudulentos.
2. **Finalidad:** Los datos se tratan para la finalidad específica informada al titular al momento de su recolección.
3. **Proporcionalidad:** Solo se tratan los datos adecuados y estrictamente necesarios para la finalidad perseguida.
4. **Veracidad y exactitud:** Los datos deben ser veraces, exactos y estar actualizados; los inexactos se corrigen o suprimen.
5. **Seguridad de los datos:** Se adoptan medidas que garanticen la confidencialidad, integridad, disponibilidad y resiliencia permanente del tratamiento, incluidas las exigidas por PCI DSS cuando se tratan datos de tarjetas de pago.
6. **Transparencia:** La información sobre el tratamiento se entrega al titular en lenguaje claro y sencillo.
7. **Confidencialidad:** Quien interviene en el tratamiento está obligado al secreto, incluso después de terminada la relación con el responsable.
8. **Licitud:** El tratamiento se realiza con el consentimiento del titular o con fundamento en una causa legal que lo habilite.

 Formerly  UltraGroup	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: GSI-PO-004-PA
	POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES	VERSIÓN: 1.0
		FECHA: 25/09/2026

9. **Portabilidad:** El titular puede obtener copia de sus datos en un formato estructurado, genérico y de uso común.

CAPÍTULO VII

FINALIDADES DEL TRATAMIENTO

Tipo de titular	Finalidades del tratamiento
Clientes y usuarios	• Gestionar solicitudes, requerimientos, servicios y transacciones de viaje. • Procesar pagos, facturación, recaudo y operaciones asociadas. • Verificar identidad, realizar autenticación y prevenir fraude. • Garantizar el cumplimiento de obligaciones contractuales. • Gestionar garantías, devoluciones, soporte y posventa. • Realizar encuestas de satisfacción y calidad del servicio. • Enviar comunicaciones informativas y operativas relacionadas con el servicio. • Cumplir requisitos legales, regulatorios, tributarios y de protección al consumidor. • Aplicar controles de seguridad bajo la normativa de protección de datos y PCI DSS.
Empleados (actuales y antiguos)	• Gestionar procesos de selección, contratación, nómina y beneficios. • Cumplir obligaciones laborales, legales, fiscales y de seguridad social. • Realizar evaluaciones de desempeño y planes de formación. • Garantizar la seguridad física y digital en instalaciones y sistemas. • Administrar accesos físicos y lógicos según roles. • Gestionar historial laboral y certificaciones.
Candidatos	• Gestionar procesos de selección, entrevistas y evaluaciones. • Verificar información y referencias laborales permitidas por la ley. • Mantener bases de talento para futuras oportunidades, previa autorización.
Proveedores y contratistas	• Verificar requisitos legales, fiscales y laborales. • Gestionar relaciones contractuales, pagos, órdenes de compra y entregas. • Administrar accesos físicos y lógicos cuando aplique. • Realizar auditorías y evaluaciones de cumplimiento y riesgos.
Aliados comerciales y socios de negocio	• Gestionar acuerdos comerciales y actividades de cooperación. • Realizar evaluaciones de riesgo y cumplimiento.

 Formerly  UltraGroup	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: GSI-PO-004-PA
	POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES	VERSIÓN: 1.0
		FECHA: 25/09/2026

	• Administrar accesos, integraciones y uso compartido de información bajo acuerdos.
Visitantes y público general	• Controlar el acceso a instalaciones mediante registro y verificación de identidad. • Mantener trazabilidad en accesos físicos. • Atender solicitudes, quejas y requerimientos de contacto.
Titulares con datos financieros o transaccionales (PCI DSS)	• Efectuar procesos de autorización y validación de transacciones. • Procesar pagos seguros bajo estándares PCI DSS. • Prevenir fraude, suplantación y actividades inusuales. • Implementar controles reforzados: cifrado, tokenización, monitoreo y restricciones de almacenamiento.
Usuarios de canales digitales (web, apps, chat, redes)	• Habilitar autenticación y acceso a plataformas. • Analizar comportamiento para seguridad, antifraude y optimización de servicios. • Implementar cookies para funcionamiento, estadísticas o experiencia del usuario, según el aviso de cookies. • Garantizar trazabilidad de operaciones digitales.

ULTRAGP PA no almacena datos prohibidos por PCI DSS, tales como el contenido completo de la banda magnética, el código de verificación (CVV2/CVC2/CID) o el bloque de PIN, después de la autorización de la transacción.

CAPÍTULO VIII

LICITUD DEL TRATAMIENTO Y CONSENTIMIENTO DEL TITULAR

ULTRAGP PA trata datos personales únicamente cuando concurre alguna de las siguientes bases de licitud previstas en la Ley 81 de 2019:

1. Consentimiento del titular, obtenido de forma que permita su trazabilidad y revocable en cualquier momento, sin efecto retroactivo.
2. Ejecución o cumplimiento de una relación contractual en la que el titular es parte.
3. Cumplimiento de una obligación legal o de un mandato de autoridad competente.
4. Salvaguarda de un interés vital del titular o de otra persona.
5. Ejercicio de funciones propias de las autoridades públicas, en el ámbito de su competencia.
6. Demás supuestos de tratamiento lícito previstos en la Ley 81 de 2019 y en su reglamento.

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		CÓDIGO: GSI-PO-004-PA
	POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES		VERSIÓN: 1.0
			FECHA: 25/09/2026

Características del consentimiento

Cuando la base del tratamiento sea el consentimiento, este se obtiene de forma previa, libre, específica, informada e inequívoca, mediante mecanismos que permitan acreditar su otorgamiento y conservar evidencia de la fecha, el medio y el contenido de la información entregada al titular. El consentimiento para el tratamiento de datos sensibles es explícito y el titular es informado de que no está obligado a autorizarlo.

El consentimiento puede ser revocado en cualquier momento, por el mismo canal en que fue otorgado o por los canales de atención dispuestos en esta política, sin efecto retroactivo sobre los tratamientos realizados con anterioridad y sin perjuicio de la conservación de los datos que deban mantenerse por obligación legal, contractual o por la existencia de una relación vigente.

Negativa a proveer datos e información errónea o inexacta

El titular puede negarse a entregar sus datos personales. En tal caso, ULTRAGP PA le informa que, por la naturaleza de los servicios de intermediación de viajes, sin esos datos no es posible perfeccionar la reserva, emitir el documento de viaje ni sostener la relación jurídica o comercial. La entrega de información errónea, incompleta o inexacta puede impedir la prestación del servicio y afecta la responsabilidad del titular sobre la veracidad de los datos suministrados.

Datos de niñas, niños y adolescentes

El tratamiento de datos de niñas, niños y adolescentes se realiza atendiendo a su interés superior y con la autorización del padre, madre, tutor o representante legal, en los términos y con las particularidades que establece la normativa de Panamá. Los servicios dirigidos a personas menores de edad incorporan información redactada en lenguaje claro y accesible.

CAPÍTULO IX

TRATAMIENTO DE DATOS PERSONALES

Categorías de datos tratados

En el desarrollo de su objeto social, ULTRAGP PA trata datos de identificación y contacto, datos de documentos de viaje, datos de facturación y financieros, datos de navegación y uso de canales digitales, datos laborales y de selección, y datos de acceso físico y videovigilancia. El tratamiento de datos sensibles se limita a los

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		CÓDIGO: GSI-PO-004-PA
	POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES		VERSIÓN: 1.0
			FECHA: 25/09/2026

supuestos estrictamente necesarios y se sujeta a consentimiento explícito o a una habilitación legal.

Calidad y actualización

Los datos se mantienen exactos, completos y actualizados. El titular es responsable de informar cualquier cambio en la información suministrada, y ULTRAGP PA habilita canales para su actualización.

Conservación

Los datos personales se conservan únicamente durante el tiempo necesario para cumplir las finalidades informadas o las obligaciones legales, contables, tributarias, contractuales o regulatorias aplicables. Vencido ese término, los datos se suprimen o anonimizan de forma segura e irreversible. Los plazos de conservación por categoría de dato se documentan en el registro de actividades de tratamiento.

Medidas de seguridad

ULTRAGP PA implementa medidas técnicas, organizativas y jurídicas apropiadas al riesgo, entre ellas control de acceso basado en roles y mínimo privilegio, autenticación multifactor, cifrado de datos en tránsito y en reposo, segmentación de red, gestión de vulnerabilidades, registro y monitoreo de eventos, respaldo y recuperación, gestión de proveedores y concienciación continua del personal. Cuando se tratan datos de tarjetas de pago, estas medidas se refuerzan con los controles exigidos por PCI DSS.

Encargados del tratamiento

Cuando ULTRAGP PA recurra a terceros para el tratamiento de datos personales por su cuenta incluidas otras sociedades del grupo empresarial y los proveedores de plataformas tecnológicas, pasarelas de pago, alojamiento en la nube y servicios de atención celebra con ellos un contrato o cláusula de tratamiento que define el objeto, la duración, la naturaleza y la finalidad del tratamiento, las categorías de datos y de titulares, las obligaciones de seguridad y confidencialidad, la prohibición de usar los datos para fines propios, el deber de notificar vulneraciones de seguridad y el destino de los datos a la terminación del contrato.

En particular, cuando la operación se soporte en plataformas administradas por STRATEGIC POINTS S.A.S. u otra sociedad del grupo, esta actúa como encargada del tratamiento por cuenta de ULTRAGP PA, quien conserva la condición de responsable frente al titular y frente a la ANTAI.

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		CÓDIGO: GSI-PO-004-PA
	POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES		VERSIÓN: 1.0
			FECHA: 25/09/2026

CAPÍTULO X

REVOCATORIA DEL CONSENTIMIENTO Y SUPRESIÓN DE DATOS

El titular puede, en cualquier momento, revocar el consentimiento otorgado y solicitar la supresión de sus datos personales, total o parcialmente, por los canales previstos en esta política. La solicitud se atiende dentro de los plazos establecidos en el capítulo de procedimiento para consultas y reclamos.

La supresión no procede cuando exista un deber legal o contractual que obligue a conservar la información, cuando los datos sean necesarios para la defensa de reclamaciones o cuando lo impida una orden de autoridad competente. En tales casos, ULTRAGP PA informa al titular la razón y el fundamento de la negativa, y limita el tratamiento a la finalidad que justifica la conservación.

CAPÍTULO XI

DERECHOS DE LOS TITULARES

De conformidad con la Ley 81 de 2019, el titular tiene los siguientes derechos:

- Derecho de acceso:** Obtener del responsable la información sobre sus datos personales y sobre el tratamiento que se les da.
- Derecho de rectificación:** Solicitar la corrección de datos erróneos, inexactos, equívocos o incompletos.
- Derecho de cancelación o supresión:** Solicitar la eliminación de sus datos cuando no se ajusten a lo dispuesto en la ley o cuando hayan dejado de ser necesarios.
- Derecho de oposición:** Oponerse al tratamiento de sus datos cuando exista causa legítima, y en particular frente a finalidades de mercadotecnia directa.
- Derecho de portabilidad:** Obtener copia de sus datos en un formato estructurado, genérico y de uso común, que permita su transmisión a otro responsable.
- Derecho a no ser objeto de decisiones automatizadas:** Solicitar intervención humana frente a decisiones basadas únicamente en el tratamiento automatizado que le afecten significativamente.
- Derecho a presentar denuncia:** Acudir ante la ANTAI cuando considere vulnerados sus derechos.

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		CÓDIGO: GSI-PO-004-PA
	POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES		VERSIÓN: 1.0
			FECHA: 25/09/2026

El ejercicio de estos derechos es gratuito y no puede condicionarse a la renuncia de ningún otro derecho. ULTRAGP PA no puede negar la prestación del servicio por el solo hecho de que el titular ejerza sus derechos.

CAPÍTULO XII

PROCEDIMIENTO PARA CONSULTAS Y RECLAMOS

Canales de atención

El titular, sus causahabientes o su representante debidamente acreditado pueden presentar consultas, solicitudes y reclamos por los siguientes canales:

1. Correo electrónico: notificaciones@linextravel.com
2. Sitio web: <https://panama.linexgo.com/>
3. Teléfono B2C: (507) 8386942
4. Teléfono B2B: (507) 8335796
5. Domicilio: Provincia de Panamá, Distrito de Panamá, Corregimiento de Betania, Urbanización Locería, Calle Ricardo J. Alfaro, Edificio Centro Comercial Siglo XXI, tercer piso, oficina N.º 53, República de Panamá

Requisitos de la solicitud

La solicitud debe contener, como mínimo, la identificación del titular y la acreditación de su identidad, la descripción clara del derecho que se ejerce y de los hechos que lo motivan, la dirección o canal para recibir la respuesta y los documentos que se quieran hacer valer. Cuando la solicitud la presente un representante, debe acreditarse la representación.

Plazos de atención

ULTRAGP PA atiende las solicitudes de acceso dentro de un plazo no mayor de diez (10) días hábiles, y las solicitudes de rectificación dentro de los cinco (5) días hábiles siguientes a su recepción, conforme a la Ley 81 de 2019. Las solicitudes de cancelación, oposición y portabilidad se atienden dentro del plazo de diez (10) días hábiles. El ejercicio de estos derechos es gratuito. Cuando la solicitud no reúna la información necesaria para su tramitación, se requerirá su complemento por una sola vez, y el plazo se suspenderá hasta que el titular responda.

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		CÓDIGO: GSI-PO-004-PA
	POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES		VERSIÓN: 1.0
			FECHA: 25/09/2026

Respuesta y recursos

La respuesta se comunica por el canal indicado por el titular y contiene el pronunciamiento sobre lo solicitado y su fundamento. Si el titular no está conforme con la respuesta, o si esta no se produce dentro del plazo, puede acudir ante la ANTAI mediante el procedimiento de tutela o reclamación previsto en la normativa aplicable.

Registro de solicitudes

Todas las solicitudes se registran con fecha de recepción, canal, tipo de derecho ejercido, responsable de la atención, fecha de respuesta y resultado. Este registro constituye evidencia de cumplimiento y es insumo de los informes de la responsabilidad demostrada.

CAPÍTULO XIII

DEBERES DEL RESPONSABLE DEL TRATAMIENTO

1. Garantizar al titular el ejercicio pleno y efectivo de sus derechos.
2. Solicitar y conservar copia de la autorización otorgada por el titular, cuando el tratamiento se base en el consentimiento.
3. Informar de manera clara, suficiente y previa al titular sobre la finalidad del tratamiento, la base de licitud y los derechos que le asisten.
4. Conservar la información bajo condiciones de seguridad que impidan su adulteración, pérdida, consulta, uso o acceso no autorizado.
5. Actualizar la información cuando sea necesario y comunicar oportunamente a los encargados del tratamiento las novedades que se presenten.
6. Rectificar la información incorrecta y atender oportunamente las solicitudes y reclamos dentro de los plazos legales.
7. Exigir a los encargados del tratamiento el cumplimiento de las condiciones de seguridad y privacidad, incluidas las obligaciones contractuales y de notificación de incidentes.
8. Informar al titular, a su solicitud, sobre el uso dado a sus datos personales.
9. Notificar a la autoridad de control y a los titulares las vulneraciones de seguridad en los términos y plazos previstos en esta política.
10. Cumplir las instrucciones y requerimientos que emita la ANTAI en su calidad de autoridad de control.

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: GSI-PO-004-PA
	POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES	VERSIÓN: 1.0
		FECHA: 25/09/2026

11. Adoptar y mantener actualizada esta política, y garantizar su disponibilidad permanente a los titulares por los canales institucionales.
12. Mantener el registro de tratamientos y la evidencia que soporta la responsabilidad demostrada.
13. Capacitar al personal que interviene en el tratamiento de datos personales.

CAPÍTULO XIV

USO DE COOKIES Y MEDIOS DIGITALES

1. **Finalidad del uso de cookies:** ULTRAGP PA utiliza cookies y tecnologías similares en sus sitios web, aplicaciones y plataformas digitales con el fin de mejorar la experiencia del usuario, permitir el funcionamiento adecuado del sitio, analizar patrones de uso y ofrecer contenidos relevantes.
2. **Tipos de cookies utilizadas:** Cookies esenciales para el funcionamiento técnico del sitio; cookies funcionales que facilitan la navegación; cookies de rendimiento para analizar el comportamiento y uso del sitio; y cookies de marketing destinadas a personalizar contenidos. Cada categoría responde a una finalidad específica y respeta los principios de necesidad y proporcionalidad.
3. **Autorización y configuración por parte del titular:** Al acceder a los medios digitales, el usuario es informado sobre el uso de cookies mediante un aviso visible que le permite aceptar, rechazar o configurar los tipos de cookies que autoriza, salvo aquellas estrictamente necesarias para el funcionamiento del sitio.
4. **Tratamiento de datos recolectados mediante cookies:** Los datos recolectados a través de cookies se tratan de acuerdo con las finalidades descritas en esta política, aplicando medidas de seguridad para impedir accesos no autorizados, adulteración o pérdida.
5. **Uso de medios digitales, analítica y terceros proveedores:** Cuando se utilicen herramientas de analítica web, plataformas de gestión de contenido o servicios de terceros que implementen sus propias cookies, ULTRAGP PA verifica que dichos proveedores actúen como encargados del tratamiento y cumplan las medidas de protección previstas en la normativa y en los contratos suscritos.
6. **Derechos del titular frente al uso de cookies:** Los titulares pueden solicitar información sobre el uso de tecnologías de seguimiento, modificar su configuración en cualquier momento y ejercer sus derechos por los canales oficiales de la organización.

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		CÓDIGO: GSI-PO-004-PA
	POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES		VERSIÓN: 1.0
			FECHA: 25/09/2026

- 7. Actualizaciones del aviso de cookies:** El aviso de cookies se actualiza cuando se modifiquen las categorías utilizadas, las finalidades o los proveedores tecnológicos involucrados, y los cambios se informan por los medios digitales institucionales.

CAPÍTULO XV

TRANSFERENCIA Y FLUJO TRANSFRONTERIZO DE DATOS PERSONALES

Las transferencias internacionales de datos personales solo se efectúan cuando el país de destino ofrezca un nivel de protección equivalente, cuando el responsable acredite garantías adecuadas cláusulas contractuales, modelos validados por la ANTAI, mecanismos de autorregulación vinculante o normas corporativas de grupos económicos, o cuando concorra alguno de los supuestos de transferencia lícita previstos en la Ley 81 de 2019, entre ellos el consentimiento del titular y la necesidad de ejecutar una relación contractual. La transferencia de datos sensibles a terceros se sujeta a las condiciones especiales del artículo 13 de la Ley 81 de 2019.

Las comunicaciones de datos personales a otras sociedades del grupo empresarial, incluidas las que se realizan hacia la República de Colombia para el soporte de plataformas tecnológicas, servicios compartidos y atención al cliente, se sustentan en un contrato de tratamiento que define el rol de cada parte, las finalidades autorizadas, las medidas de seguridad y las obligaciones de confidencialidad, y se limitan estrictamente a las finalidades informadas al titular.

CAPÍTULO XVI

OFICIAL DE PROTECCIÓN DE DATOS PERSONALES

El Decreto Ejecutivo 285 de 2021 incluye, entre los mecanismos de responsabilidad demostrada del responsable del tratamiento, la designación de un oficial de protección de datos personales. ULTRAGP PA designa un oficial de protección de datos personales, o un punto de contacto equivalente, encargado de atender las solicitudes de los titulares, supervisar el cumplimiento de la Ley 81 de 2019 y de su reglamento, coordinar la atención de las vulneraciones de seguridad y servir de enlace con la ANTAI. Sus datos de contacto se publican en el sitio web y se informan en los canales de atención.

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		CÓDIGO: GSI-PO-004-PA
	POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES		VERSIÓN: 1.0
			FECHA: 25/09/2026

CAPÍTULO XVII

REGISTRO DE BASES DE DATOS

ULTRAGP PA mantiene un registro actualizado de las bases de datos bajo su responsabilidad, conforme al artículo 35 del Decreto Ejecutivo 285 de 2021, así como la ficha técnica con los protocolos, procesos y procedimientos de gestión y transferencia segura de datos personales exigida por el artículo 33 del mismo decreto. El registro identifica, por cada base de datos, su finalidad, las categorías de titulares y de datos, los destinatarios, las transferencias internacionales, los plazos de conservación y las medidas de seguridad aplicadas.

CAPÍTULO XVIII

PROTOCOLO ANTE VULNERACIÓN DE DATOS PERSONALES

Ante el conocimiento de una violación de la seguridad de los datos personales, ULTRAGP PA notifica de inmediato a la autoridad de control y a los titulares afectados, dentro de las setenta y dos (72) horas siguientes, conforme al artículo 37 del Decreto Ejecutivo 285 de 2021. Los contratos con encargados del tratamiento estipulan la obligación de notificar a ULTRAGP PA sin dilación indebida, de modo que el responsable pueda cumplir su propio plazo.

La notificación contiene, como mínimo:

1. Naturaleza del incidente y fecha en que se tuvo conocimiento.
2. Categorías y número aproximado de titulares afectados.
3. Datos personales comprometidos y sistemas involucrados.
4. Acciones correctivas adoptadas y estado de la contención.
5. Recomendaciones dirigidas a los titulares para mitigar los efectos.
6. Datos de contacto del oficial de protección de datos personales.

La gestión interna del incidente se realiza conforme al procedimiento corporativo de gestión de incidentes de seguridad de la información, que define la detección, clasificación, contención, erradicación, recuperación, comunicación y lecciones aprendidas. Todo incidente que afecte datos personales se documenta en el registro de incidentes, con independencia de que haya sido o no notificable.

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		CÓDIGO: GSI-PO-004-PA
	POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES		VERSIÓN: 1.0
			FECHA: 25/09/2026

CAPÍTULO XIX

EVALUACIÓN PRELIMINAR DE IMPACTO EN LA PRIVACIDAD

ULTRAGP PA realiza una evaluación preliminar de impacto en la privacidad antes de iniciar tratamientos que puedan entrañar un riesgo significativo para los derechos de los titulares, en particular cuando se diseñe o adquiera un sistema, práctica, herramienta o dispositivo que recolecte o procese datos personales. La evaluación identifica los riesgos, valora su probabilidad e impacto y define las medidas de mitigación, y se documenta como parte de los mecanismos de responsabilidad demostrada del artículo 33 del Decreto Ejecutivo 285 de 2021.

La evaluación se realiza de forma previa al inicio del tratamiento y se actualiza cuando cambien la naturaleza, el alcance, el contexto o las finalidades del tratamiento, o cuando se incorporen nuevas tecnologías que modifiquen el nivel de riesgo.

CAPÍTULO XX

TRATAMIENTO DE DATOS PERSONALES MEDIANTE SISTEMAS Y AGENTES DE INTELIGENCIA ARTIFICIAL

ULTRAGP PA podrá utilizar sistemas y agentes de inteligencia artificial en el desarrollo de sus actividades. Cuando dichos sistemas traten datos personales, el tratamiento se sujeta íntegramente a esta política y a las siguientes reglas:

1. Todo sistema de inteligencia artificial que trate datos personales debe estar inscrito en el registro corporativo de sistemas de inteligencia artificial antes de entrar en operación, y clasificado según su nivel de riesgo.
2. Los sistemas de inteligencia artificial no tratan el número de tarjeta (PAN), la fecha de vencimiento, el código de verificación ni datos de autenticación sensibles.
3. No se admiten decisiones basadas únicamente en tratamiento automatizado que produzcan efectos jurídicos sobre el titular o le afecten significativamente, sin garantizar intervención humana, el derecho a obtener una explicación y el derecho a impugnar la decisión.
4. El uso de datos personales para el entrenamiento, ajuste o evaluación de modelos requiere una base de licitud propia, la minimización de los datos utilizados y, cuando corresponda, su anonimización previa.

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: GSI-PO-004-PA
	POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES	VERSIÓN: 1.0
		FECHA: 25/09/2026

5. Los proveedores de soluciones de inteligencia artificial que traten datos personales por cuenta de ULTRAGP PA asumen la condición de encargados del tratamiento y las obligaciones contractuales correspondientes, incluida la prohibición de reutilizar los datos para entrenar sus propios modelos sin autorización expresa.
6. Los tratamientos de alto riesgo mediante inteligencia artificial requieren evaluación de impacto previa en los términos del capítulo anterior.

Las disposiciones de gobierno, clasificación de riesgo, registro, autorización y control de los sistemas de inteligencia artificial se desarrollan en la política corporativa de gobierno y uso de inteligencia artificial, que complementa este capítulo.

CAPÍTULO XXI

RÉGIMEN SANCIONATORIO Y RESPONSABILIDAD

El incumplimiento de la Ley 81 de 2019 da lugar a infracciones leves, graves y muy graves, sancionadas con multas de mil balboas (B/.1,000.00) a diez mil balboas (B/.10,000.00) y, en el caso de las muy graves, con la clausura de los registros o bases de datos y la inhabilitación para el tratamiento, sin perjuicio de la responsabilidad civil o penal a que haya lugar.

El incumplimiento de esta política por parte de los colaboradores da lugar a las medidas disciplinarias previstas en el reglamento interno de trabajo y en los contratos, sin perjuicio de las acciones legales que correspondan. En el caso de proveedores y contratistas, el incumplimiento constituye causal de terminación del contrato.

CAPÍTULO XXII

MODIFICACIÓN DE LA POLÍTICA

ULTRAGP PA podrá modificar, actualizar o complementar en cualquier momento esta política, con el fin de ajustarla a cambios normativos, regulatorios, tecnológicos o a nuevas prácticas internas relacionadas con el manejo de la información.

Cuando las modificaciones impliquen cambios sustanciales en las finalidades del tratamiento, en los derechos de los titulares o en los mecanismos de atención, se informará oportunamente a los titulares a través de los canales oficiales, incluyendo medios digitales, avisos públicos o comunicaciones directas.

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		CÓDIGO: GSI-PO-004-PA
	POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES		VERSIÓN: 1.0
			FECHA: 25/09/2026

La versión actualizada de la política estará siempre disponible para consulta en los canales institucionales, garantizando su accesibilidad permanente y el ejercicio pleno de los derechos de los titulares.

CAPÍTULO XXIII

CONTROL DE CAMBIOS

FECHA	OBJETIVO	VERSIÓN	ELABORÓ	REVISÓ	APROBÓ
25/09/2026	Emisión inicial de la política de protección de datos personales de ULTRAGP PA, S.A., aplicable a los tratamientos sujetos a la legislación de Panamá.	1.0	Elkin Corredor	Juliana Soto Restrepo	Comité SGSI