POLÍTICA INTEGRAL DE TRATAMIENTO DE DATOS PERSONALES

TABLA DE CONTENIDO

AUTENTIC LATAM S.A.S. (en adelante "AutenTIC"), identificada con NIT 901.273.383, domiciliada en la Calle 93B # 13-30 Oficina 202 en la ciudad de Bogotá D.C., en virtud del cumplimiento de la normatividad vigente para la protección y tratamiento de datos personales, reconoce la privacidad, la seguridad de la información y la confianza digital como pilares fundamentales para el desarrollo de sus actividades corporativas, tecnológicas y de innovación digital. En el marco de sus servicios asociados a identidad digital, validación de identidad, biometría, firma electrónica, automatización e interoperabilidad tecnológica, la organización adopta la presente Política Integral de Tratamiento de Datos Personales, aplicable a todos los datos personales recolectados, almacenados, usados, procesados, transmitidos, transferidos, actualizados y suprimidos bajo su responsabilidad.

La presente política forma parte del Programa Integral de Gestión de Datos Personales (PIGDP) de AutenTIC y establece el marco institucional para garantizar un tratamiento legítimo, transparente y seguro de los datos personales, integrando principios de responsabilidad demostrada (accountability), privacidad desde el diseño, gestión de riesgos y mejora continua, en articulación con el Sistema de Gestión de Seguridad de la Información (SGSI) de la organización. Su cumplimiento es obligatorio para todos los colaboradores, contratistas, proveedores, aliados y terceros que intervengan en actividades relacionadas con el tratamiento de datos personales bajo responsabilidad de AutenTIC.

1. OBJETIVO

Establecer los lineamientos institucionales, jurídicos, organizacionales y de seguridad aplicables al tratamiento de datos personales realizado por AutenTIC, con el fin de garantizar la protección de los derechos de los titulares, asegurar un tratamiento legítimo, transparente y seguro de la información personal, y fortalecer los principios de privacidad, responsabilidad demostrada (accountability), gestión de riesgos y confianza digital, en cumplimiento de la normatividad vigente en Colombia y en articulación con el Programa Integral de Gestión de Datos Personales (PIGDP) y el Sistema de Gestión de Seguridad de la Información (SGSI) de la organización.

2. ALCANCE

La presente Política Integral de Tratamiento de Datos Personales aplica a todas las actividades de recolección, almacenamiento, uso, circulación, procesamiento, transmisión, transferencia, actualización, conservación y supresión de datos personales realizadas por AutenTIC, en desarrollo de sus actividades corporativas, comerciales, tecnológicas, administrativas y de innovación digital.
El alcance de esta política comprende a todos los colaboradores, directivos, contratistas, proveedores, aliados, encargados del tratamiento y terceros que intervengan en operaciones relacionadas con el tratamiento de datos personales bajo responsabilidad de AutenTIC, incluyendo servicios asociados a identidad digital, validación de identidad, biometría, firma electrónica, automatización, interoperabilidad tecnológica y demás ecosistemas digitales administrados o gestionados por la

organización. Asimismo, aplica a los datos personales tratados mediante plataformas tecnológicas, servicios cloud, APIs, herramientas de analítica, mecanismos de autenticación y demás componentes tecnológicos utilizados por la organización, tanto a nivel nacional como internacional.

3. MARCO NORMATIVO

La presente Política Integral de Tratamiento de Datos Personales se fundamenta en la Ley Estatutaria 1581 de 2012, como base normativa principal en Colombia para la protección de datos personales y el ejercicio del derecho constitucional de habeas data, así como en sus decretos reglamentarios, normas complementarias y demás disposiciones aplicables en materia de privacidad, seguridad de la información, identidad digital, firma electrónica y tratamiento de información personal.

Asimismo, AutenTIC adopta estándares, buenas prácticas y lineamientos nacionales e internacionales relacionados con la protección de datos personales, gestión de riesgos, seguridad de la información y confianza digital.

El detalle de las disposiciones legales, regulatorias, técnicas y referenciales aplicables al Programa Integral de Gestión de Datos Personales (PIGDP) se encuentra documentado y actualizado en la Matriz Legal y Regulatoria de la organización, como parte integral de su modelo de cumplimiento corporativo.

4. DEFINICIONES

4.1. Definiciones Generales de Habeas Data

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.
- **Aviso de Privacidad:** Comunicación verbal o escrita generada por el Responsable del Tratamiento, dirigida al Titular, mediante la cual se informa la existencia de las políticas de tratamiento de información, las finalidades aplicables, los derechos del Titular y los mecanismos para acceder a dicha información.
- **Base de Datos:** Conjunto organizado de datos personales que sea objeto de tratamiento.
- **Dato Personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Dato Público:** Dato calificado como tal según la ley y que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los relativos al estado civil de las personas, su profesión u oficio, su calidad de comerciante o servidor público y aquellos contenidos en registros públicos.
- **Dato Sensible:** Información que afecta la intimidad del Titular o cuyo uso indebido puede generar discriminación, tales como datos relacionados con

origen racial o étnico, orientación política, convicciones religiosas o filosóficas, afiliación sindical, datos relativos a la salud, vida sexual y datos biométricos.

- **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realiza el tratamiento de datos personales por cuenta del Responsable del Tratamiento.
- **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que decide sobre la base de datos y/o el tratamiento de los datos personales.
- **Titular:** Persona natural cuyos datos personales son objeto de tratamiento.
- **Transferencia:** Envío de datos personales por parte del Responsable y/o Encargado del Tratamiento ubicado en Colombia a otro Responsable ubicado dentro o fuera del país.
- **Transmisión:** Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio colombiano cuando tenga por objeto la realización de un tratamiento por parte de un Encargado por cuenta del Responsable.
- **Tratamiento:** Cualquier operación o conjunto de operaciones realizadas sobre datos personales, tales como recolección, almacenamiento, uso, circulación, procesamiento, actualización, transmisión, transferencia o supresión.

4.2. Definiciones de Seguridad y Privacidad

- **Accountability (Responsabilidad Demostrada):** Principio mediante el cual el Responsable del Tratamiento debe ser capaz de demostrar la adopción de medidas apropiadas y efectivas para garantizar el cumplimiento de las obligaciones en materia de protección de datos personales.
- **Privacidad desde el Diseño (Privacy by Design):** Enfoque mediante el cual la protección de datos personales y la privacidad son incorporadas desde las etapas iniciales del diseño, desarrollo y operación de procesos, servicios y tecnologías.
- **Privacidad por Defecto (Privacy by Default):** Principio según el cual solo deben tratarse los datos personales estrictamente necesarios para cada finalidad específica.

4.3. Definiciones de Biometría e Identidad Digital

- **Dato Biométrico:** Dato personal sensible obtenido a partir de características físicas, fisiológicas o conductuales de una persona natural que permiten o confirman su identificación única.
- **Identidad Digital:** Conjunto de atributos, credenciales, evidencias y mecanismos tecnológicos utilizados para representar y validar la identidad de una persona en entornos digitales.
- **Autenticación:** Proceso mediante el cual se verifica la identidad declarada de un usuario o titular.

4.4. Definiciones de Inteligencia Artificial

- **Inteligencia Artificial (IA):** Sistemas o modelos tecnológicos diseñados para realizar tareas que normalmente requieren inteligencia humana, incluyendo análisis, predicción, clasificación, automatización o generación de contenido.
- **Sistema Automatizado de Decisión:** Herramienta tecnológica que utiliza reglas, algoritmos o modelos automatizados para apoyar o ejecutar decisiones que puedan producir efectos sobre los titulares de los datos.
- **Supervisión Humana Significativa:** Participación activa y efectiva de personas en la revisión, validación o control de decisiones asistidas o automatizadas mediante inteligencia artificial.

4.5. Definiciones de Firma Electrónica y Evidencia Digital

- **Firma Electrónica:** Métodos, códigos, datos o mecanismos electrónicos utilizados para identificar a una persona en relación con un mensaje de datos, siempre que sean confiables y apropiados para los fines perseguidos.
- **Evidencia Electrónica:** Información generada, almacenada o transmitida en medios electrónicos que puede ser utilizada como elemento probatorio o de trazabilidad.
- **Log o Registro de Auditoría:** Registro cronológico de eventos, actividades o transacciones realizadas sobre sistemas, aplicaciones o datos, utilizado para trazabilidad, monitoreo y control.

5. PRINCIPIOS

AutenTIC realizará el tratamiento de datos personales conforme a los principios establecidos en la Ley Estatutaria 1581 de 2012 y demás disposiciones aplicables, garantizando un tratamiento legítimo, transparente, seguro y responsable de la información personal bajo su responsabilidad.

a) **Legalidad:** El tratamiento de datos personales es una actividad regulada que deberá sujetarse a lo establecido en la normatividad vigente y demás disposiciones que la desarrollen.
b) **Finalidad:** El tratamiento de datos personales deberá obedecer a una finalidad legítima, específica, explícita e informada previamente al Titular.
c) **Libertad:** El tratamiento solo podrá ejercerse con el consentimiento previo, expreso e informado del Titular, salvo las excepciones previstas en la ley.
d) **Veracidad o Calidad:** La información sujeta a tratamiento deberá ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos o que induzcan a error.
e) **Transparencia:** AutenTIC garantizará al Titular el derecho a obtener información sobre la existencia, uso y tratamiento de sus datos personales.

f) **Acceso y Circulación Restringida:** El tratamiento de los datos personales se sujetará a los límites derivados de su naturaleza, de las disposiciones legales y de las autorizaciones otorgadas por el Titular.
g) **Seguridad:** AutenTIC adoptará medidas técnicas, humanas, administrativas y organizacionales razonables para proteger los datos personales contra pérdida, acceso no autorizado, alteración, uso fraudulento, divulgación o cualquier tratamiento no autorizado.
h) **Confidencialidad:** Todas las personas que intervengan en el tratamiento de datos personales estarán obligadas a garantizar la reserva y confidencialidad de la información, incluso después de finalizada su relación con la organización.
i) **Responsabilidad Demostrada (Accountability):** AutenTIC adoptará medidas apropiadas para demostrar el cumplimiento de las obligaciones aplicables en materia de protección de datos personales, gestión de riesgos y privacidad.
j) **Privacidad desde el Diseño y por Defecto:** La organización integrará medidas de privacidad y protección de datos personales desde las etapas de diseño, desarrollo, implementación y operación de procesos, servicios y tecnologías.
k) **Minimización de Datos:** AutenTIC realizará el tratamiento únicamente de los datos personales estrictamente necesarios para el cumplimiento de las finalidades autorizadas.
l) **Ética y Uso Responsable de Tecnologías:** La organización promoverá el uso responsable, transparente y seguro de tecnologías emergentes, incluyendo mecanismos de automatización, biometría e inteligencia artificial, garantizando el respeto por los derechos y libertades de los titulares.

6. GOBIERNO Y RESPONSABILIDADES

AutenTIC establece un modelo de gobierno orientado a garantizar la protección de los datos personales, la privacidad, la seguridad de la información y el cumplimiento de las obligaciones aplicables en materia de tratamiento de datos personales, conforme al Programa Integral de Gestión de Datos Personales (PIGDP) y demás lineamientos corporativos de la organización.

La organización establecerá los roles, responsabilidades, mecanismos de supervisión y controles necesarios para asegurar un tratamiento legítimo, transparente y seguro de los datos personales bajo su responsabilidad, promoviendo principios de responsabilidad demostrada (accountability), gestión de riesgos, confidencialidad, trazabilidad y mejora continua.

6.1. Responsable del Tratamiento

AUTENTIC LATAM S.A.S. actuará como Responsable del Tratamiento de los datos personales recolectados, almacenados, usados, procesados, transmitidos o suprimidos bajo su administración, garantizando el cumplimiento de las obligaciones establecidas en la normatividad aplicable.

6.2. Encargados del Tratamiento

La organización podrá apoyarse en Encargados del Tratamiento para el desarrollo de actividades relacionadas con el tratamiento de datos personales, quienes deberán cumplir las obligaciones contractuales, técnicas, organizacionales y de seguridad definidas por AutenTIC y por la normatividad vigente.

6.3. Terceros y Proveedores Tecnológicos

Los terceros, aliados, proveedores cloud, operadores tecnológicos y demás proveedores que intervengan en actividades relacionadas con el tratamiento de datos personales deberán adoptar medidas adecuadas de protección de la información y cumplir las obligaciones de confidencialidad, seguridad y privacidad definidas por la organización.

6.4. Roles Internos y Responsabilidades

AutenTIC definirá internamente los roles, responsabilidades y mecanismos de supervisión necesarios para garantizar la adecuada gestión del Programa Integral de Gestión de Datos Personales (PIGDP), conforme a su estructura organizacional y modelo de gobierno corporativo.

6.5. Oficial o Responsable de Protección de Datos

La organización podrá designar responsables, líderes o roles encargados de coordinar las actividades relacionadas con protección de datos personales, privacidad, cumplimiento y gestión de riesgos asociados al tratamiento de información personal.

6.6. Relación con el SGSI y Gobierno de Seguridad de la Información

El gobierno del PIGDP se articulará con el Sistema de Gestión de Seguridad de la Información (SGSI) de AutenTIC, integrando capacidades de protección de activos de información, gestión de riesgos, seguridad tecnológica, monitoreo y mejora continua como parte del modelo corporativo de gobernanza y confianza digital de la organización.

7. CATEGORIA DE TITULARES

AutenTIC podrá realizar el tratamiento de datos personales de diferentes categorías de titulares, conforme a la naturaleza de sus servicios, relaciones contractuales, actividades corporativas y ecosistemas tecnológicos asociados a identidad digital, validación de identidad, biometría, firma electrónica y demás servicios administrados por la organización.

Las categorías de titulares cuyos datos personales podrán ser objeto de tratamiento incluyen, entre otras, las siguientes:

7.1. Clientes

Personas naturales que adquieren, utilizan o acceden a los productos, plataformas, servicios tecnológicos o servicios digitales ofrecidos por AutenTIC.

7.2. Usuarios

Personas naturales que interactúan con plataformas, aplicativos, portales, APIs, canales digitales o ecosistemas tecnológicos administrados o interoperados por la organización.

7.3. Proveedores

Personas naturales vinculadas a proveedores, contratistas, aliados comerciales o terceros que suministran bienes o servicios a la organización.

7.4. Empleados y Contratistas

Personas naturales vinculadas laboral o contractualmente con AutenTIC, incluyendo colaboradores, contratistas, practicantes, consultores y demás personal autorizado.

7.5. Aspirantes y Participantes de Selección

Personas naturales que participen en procesos de selección, vinculación o evaluación adelantados por la organización.

7.6. Visitantes

Personas naturales que ingresen o interactúen con las instalaciones físicas, plataformas digitales, canales de atención o servicios tecnológicos de AutenTIC.

7.7. Aliados y Terceros

Personas naturales vinculadas a aliados estratégicos, operadores tecnológicos, integradores, clientes corporativos, entidades aliadas o terceros relacionados con la prestación de servicios de la organización.

7.8. Niños, Niñas y Adolescentes

AutenTIC realizará tratamiento de datos personales de niños, niñas y adolescentes únicamente en los casos autorizados por la ley y garantizando la protección de sus

derechos fundamentales, el interés superior del menor y las demás condiciones establecidas en la normatividad aplicable.

Información El gobierno del PIGDP se articulará con el Sistema de Gestión de Seguridad de la Información

8. CATEGORÍAS DE DATOS PERSONALES

AutenTIC podrá realizar el tratamiento de diferentes categorías de datos personales conforme a la naturaleza de sus servicios, finalidades autorizadas, relaciones contractuales, obligaciones legales y ecosistemas tecnológicos asociados a identidad digital, biometría, firma electrónica, interoperabilidad y servicios digitales administrados por la organización.
Las categorías de datos personales objeto de tratamiento podrán incluir, entre otras, las siguientes:

8.1. Datos Públicos

Datos calificados como públicos por la normatividad vigente, incluyendo aquellos contenidos en registros públicos, documentos públicos y demás información que no esté sometida a reserva legal.

8.2. Datos Semiprivados

Datos que no tienen naturaleza íntima, reservada ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a determinado sector o grupo de personas.

8.3. Datos Privados

Datos que por su naturaleza íntima o reservada solo son relevantes para el Titular y cuyo tratamiento requiere autorización conforme a la normatividad aplicable.

8.4. Datos Sensibles

Datos que afectan la intimidad del Titular o cuyo uso indebido puede generar discriminación, incluyendo datos relacionados con salud, origen racial o étnico, orientación política, convicciones religiosas o filosóficas, afiliación sindical, vida sexual y datos biométricos.

8.5. Datos Biométricos

Datos personales sensibles obtenidos a partir de características físicas, fisiológicas o conductuales de una persona natural, utilizados para procesos de autenticación, validación o verificación de identidad.

8.6. Datos Financieros

Datos relacionados con información financiera, crediticia, transaccional, comercial o de comportamiento económico de los titulares.

8.7. Datos de Identidad Digital

Datos utilizados para procesos de identificación, autenticación, validación de identidad, firma electrónica, control de acceso o interacción en entornos digitales.

8.8. Datos de Geolocalización

Datos relacionados con la ubicación geográfica de dispositivos, conexiones, accesos o interacciones realizadas mediante plataformas o servicios digitales administrados por la organización.

8.9. Metadatos y Evidencia Electrónica

Información técnica, registros de auditoría, logs, trazabilidad, eventos, marcas de tiempo y demás evidencias electrónicas generadas durante el uso de plataformas, servicios digitales o mecanismos de autenticación e identidad digital.

8.10. Datos Inferidos y Automatizados

Datos obtenidos mediante procesos de analítica, correlación, automatización, inteligencia artificial o mecanismos tecnológicos utilizados para fortalecer procesos de seguridad, validación, prevención de fraude, monitoreo o prestación de servicios digitales.

9. AUTORIZACIÓN Y CONSENTIMIENTO

AutenTIC realizará el tratamiento de datos personales únicamente cuando cuente con la autorización previa, expresa e informada del Titular, salvo las excepciones previstas en la normatividad vigente. La autorización podrá obtenerse mediante mecanismos físicos, electrónicos, digitales, tecnológicos o cualquier otro medio que permita su posterior consulta y verificación.

La organización garantizará que el Titular conozca de manera clara las finalidades del tratamiento, los derechos que le asisten, los mecanismos para ejercerlos y las condiciones generales bajo las cuales serán tratados sus datos personales, conforme a los principios de legalidad, libertad, transparencia y responsabilidad demostrada (accountability).

9.1. Autorización General

AutenTIC solicitará la autorización del Titular para el tratamiento de sus datos personales antes de la recolección de la información, informando las finalidades aplicables y las condiciones generales del tratamiento.

9.2. Autorización para Datos Sensibles

El tratamiento de datos sensibles estará sujeto a autorización previa, expresa e informada del Titular, indicando el carácter facultativo de la entrega de este tipo de información.

9.3. Autorización para Datos Biométricos

Cuando el tratamiento involucre datos biométricos, AutenTIC informará al Titular las finalidades específicas asociadas a validación de identidad, autenticación, seguridad, firma electrónica o mecanismos tecnológicos relacionados.

9.4. Autorización para Tratamiento mediante Inteligencia Artificial

Cuando el tratamiento de datos personales involucre herramientas de automatización, analítica avanzada o mecanismos de inteligencia artificial, la organización informará las finalidades generales asociadas al uso de dichas tecnologías.

9.5. Medios de Obtención del Consentimiento

La autorización podrá obtenerse mediante formularios físicos, medios electrónicos, plataformas digitales, mecanismos de autenticación, aceptación de términos y condiciones, validaciones tecnológicas, grabaciones, mensajes de datos u otros mecanismos permitidos por la normatividad aplicable.

9.6. Revocatoria del Consentimiento

El Titular podrá revocar la autorización otorgada para el tratamiento de sus datos personales en los casos permitidos por la normatividad vigente y conforme a los procedimientos definidos por la organización.

9.7. Casos Exceptuados de Autorización

AutenTIC podrá realizar tratamiento de datos personales sin autorización previa del Titular en los casos expresamente previstos por la ley.

10. FINALIDADES DEL TRATAMIENTO

AutenTIC realizará el tratamiento de datos personales conforme a finalidades legítimas, específicas y previamente informadas al Titular, relacionadas con el

desarrollo de sus actividades corporativas, comerciales, tecnológicas, administrativas y de innovación digital.

Las finalidades del tratamiento podrán variar de acuerdo con la naturaleza de la relación entre el Titular y la organización, así como con los servicios asociados a identidad digital, validación de identidad, biometría, firma electrónica, interoperabilidad tecnológica, automatización y demás servicios digitales administrados por AutenTIC.

10.1. Finalidades Generales

AutenTIC podrá realizar el tratamiento de datos personales para el desarrollo de actividades operativas, administrativas, comerciales, contractuales, tecnológicas, de seguridad, cumplimiento legal, atención al cliente, gestión documental, autenticación, validación de identidad, prevención de fraude, trazabilidad y prestación de servicios digitales.

10.2. Finalidades para Clientes

Los datos personales de clientes podrán ser tratados para la prestación de servicios, validación de identidad, autenticación, gestión contractual, soporte, atención de PQRS, gestión comercial, facturación, prevención de fraude, generación de firma electrónica y demás actividades relacionadas con los servicios contratados.

10.3. Finalidades para Proveedores

Los datos personales de proveedores y contratistas podrán ser tratados para procesos de contratación, validación, gestión documental, gestión de pagos, evaluación de servicios, control de acceso y cumplimiento de obligaciones contractuales y legales.

10.4. Finalidades para Empleados y Contratistas

Los datos personales de empleados, colaboradores y contratistas podrán ser tratados para la administración de la relación laboral o contractual, gestión de talento humano, seguridad, control de acceso, afiliaciones, cumplimiento de obligaciones legales y gestión administrativa interna.

10.5. Finalidades Comerciales y de Mercadeo

AutenTIC podrá utilizar datos personales para actividades de contacto, envío de información, campañas comerciales, invitaciones, encuestas, medición de satisfacción, análisis estadístico, ofrecimiento de productos y servicios, siempre conforme a las autorizaciones otorgadas por el Titular.

10.6. Finalidades de Validación de Identidad

La organización podrá realizar procesos de validación, autenticación y verificación de identidad mediante mecanismos físicos, digitales, biométricos o tecnológicos para garantizar la seguridad, trazabilidad y confiabilidad de sus servicios.

10.7. Finalidades Biométricas

Los datos biométricos podrán ser utilizados para procesos de autenticación, validación de identidad, prevención de fraude, controles de seguridad, firma electrónica y mecanismos de confianza digital.

10.8. Finalidades de Firma Electrónica

AutenTIC podrá realizar tratamiento de datos personales relacionados con procesos de firma electrónica, generación de evidencias electrónicas, trazabilidad, autenticación y conservación probatoria asociada a mensajes de datos y transacciones electrónicas.

10.9. Finalidades de Inteligencia Artificial y Automatización

La organización podrá utilizar herramientas de automatización, analítica o inteligencia artificial para fortalecer procesos de validación, seguridad, prevención de fraude, analítica, interoperabilidad tecnológica y mejora de servicios digitales.

10.10. Finalidades de Seguridad y Prevención de Fraude

AutenTIC podrá tratar datos personales para monitoreo, trazabilidad, gestión de incidentes, seguridad de la información, protección de activos digitales, prevención de fraude y cumplimiento de obligaciones legales y regulatorias.

10.11. Finalidades de Analítica y Estadística

Los datos personales podrán ser utilizados para análisis estadísticos, métricas, indicadores, analítica de servicios, inteligencia de negocio y mejora continua de procesos y plataformas digitales.

10.12. Finalidades de Cumplimiento Legal y Contractual

AutenTIC podrá tratar datos personales para dar cumplimiento a obligaciones legales, regulatorias, contractuales, judiciales, administrativas y requerimientos de autoridades competentes.

11. TRATAMIENTO DE DATOS BIOMÉTRICOS

AutenTIC podrá realizar tratamiento de datos biométricos en desarrollo de sus servicios asociados a validación de identidad, autenticación, firma electrónica,

prevención de fraude, seguridad digital y mecanismos de confianza digital, conforme a la normatividad vigente aplicable y a los principios de legalidad, finalidad, proporcionalidad, seguridad y responsabilidad demostrada (accountability).

El tratamiento de datos biométricos será realizado bajo medidas de protección administrativas, técnicas y organizacionales orientadas a garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y uso autorizado de este tipo de información, reconociendo su carácter de dato personal sensible.

11.1. Naturaleza Sensible del Dato Biométrico

Los datos biométricos tratados por AutenTIC serán considerados datos personales sensibles y estarán sujetos a condiciones especiales de protección conforme a la normatividad vigente.

11.2. Finalidad Específica

Los datos biométricos podrán ser utilizados para procesos de validación de identidad, autenticación, mecanismos antifraude, generación de firma electrónica, controles de seguridad y demás servicios digitales autorizados por el Titular.

11.3. Consentimiento Reforzado

AutenTIC solicitará autorización previa, expresa e informada para el tratamiento de datos biométricos, informando al Titular las finalidades aplicables y el carácter facultativo de la entrega de este tipo de información.

11.4. Autenticación y Verificación de Identidad

La organización podrá utilizar tecnologías biométricas para procesos de autenticación, validación y verificación de identidad en entornos físicos o digitales, con el fin de fortalecer la seguridad, trazabilidad y confiabilidad de sus servicios.

11.5. Medidas de Seguridad Biométrica

AutenTIC adoptará medidas de seguridad razonables para la protección de los datos biométricos, incluyendo controles orientados a prevenir acceso no autorizado, pérdida, alteración, divulgación o uso indebido de la información.

11.6. Retención y Eliminación Biométrica

Los datos biométricos serán conservados únicamente durante el tiempo necesario para el cumplimiento de las finalidades autorizadas, obligaciones legales o requerimientos contractuales aplicables, y posteriormente serán eliminados o suprimidos conforme a los lineamientos definidos por la organización.

11.7. Restricciones y Prohibiciones

AutenTIC no realizará tratamiento de datos biométricos para finalidades incompatibles con las autorizadas por el Titular ni para actividades prohibidas por la normatividad vigente.

11.8. Interoperabilidad Biométrica

Cuando los servicios de la organización involucren mecanismos de interoperabilidad tecnológica o integración con terceros autorizados, el tratamiento de datos biométricos se realizará bajo condiciones de seguridad, confidencialidad, trazabilidad y cumplimiento normativo aplicables.

12. TRATAMIENTO DE DATOS MEDIANTE INTELIGENCIA ARTIFICIAL

AutenTIC podrá utilizar herramientas de automatización, analítica avanzada, modelos algorítmicos e inteligencia artificial en el desarrollo de sus servicios digitales, procesos de validación de identidad, seguridad, interoperabilidad tecnológica, prevención de fraude, atención de usuarios y demás actividades relacionadas con su modelo de negocio.
El tratamiento de datos personales mediante mecanismos de inteligencia artificial será realizado bajo principios de legalidad, transparencia, responsabilidad demostrada (accountability), seguridad, privacidad, supervisión humana significativa y gestión de riesgos, procurando un uso responsable, proporcional y ético de las tecnologías implementadas por la organización.

12.1. Uso de Sistemas de Inteligencia Artificial

AutenTIC podrá implementar sistemas de inteligencia artificial y automatización para apoyar procesos tecnológicos, operativos, analíticos y de seguridad relacionados con la prestación de sus servicios digitales.

12.2. Automatización y Asistentes Tecnológicos

La organización podrá utilizar asistentes virtuales, herramientas automatizadas, motores de validación, analítica y demás tecnologías orientadas a optimizar procesos, fortalecer la experiencia del usuario y mejorar la eficiencia operativa.

12.3. Supervisión Humana Significativa

AutenTIC promoverá mecanismos de supervisión, revisión y control humano sobre procesos automatizados o asistidos mediante inteligencia artificial, especialmente cuando puedan generar efectos relevantes sobre los titulares de la información.

12.4. Gestión de Riesgos Algorítmicos

La organización podrá adoptar medidas orientadas a identificar, evaluar y gestionar riesgos asociados al uso de tecnologías de inteligencia artificial, automatización y modelos algorítmicos, incluyendo riesgos relacionados con privacidad, seguridad, sesgos, uso indebido de información y afectación de derechos de los titulares.

12.5. Transparencia y Explicabilidad

AutenTIC procurará promover principios de transparencia y uso responsable en la implementación de tecnologías de inteligencia artificial, conforme a la naturaleza de los servicios y las capacidades tecnológicas aplicables.

12.6. Restricciones de Uso

La organización no utilizará herramientas de inteligencia artificial para finalidades contrarias a la ley, incompatibles con las autorizaciones otorgadas por los titulares o que vulneren derechos y libertades fundamentales.

12.7. Calidad y Minimización de Datos

AutenTIC promoverá el tratamiento adecuado, pertinente y proporcional de los datos personales utilizados en procesos automatizados o mecanismos de inteligencia artificial.

12.8. Inteligencia Artificial Generativa

Cuando la organización utilice tecnologías de inteligencia artificial generativa, adoptará medidas razonables orientadas a proteger la confidencialidad, seguridad y uso adecuado de la información tratada mediante dichas herramientas.

12.9. Evaluaciones de Impacto y Mejora Continua

AutenTIC podrá desarrollar actividades de evaluación, monitoreo y mejora continúa relacionadas con el uso de tecnologías de inteligencia artificial, privacidad, seguridad de la información y gestión de riesgos asociados al tratamiento de datos personales.

13. FIRMA ELECTRÓNICA, IDENTIDAD DIGITAL Y EVIDENCIA ELECTRÓNICA

AutenTIC podrá realizar tratamiento de datos personales en el marco de servicios asociados a firma electrónica, identidad digital, autenticación, validación de identidad, generación de evidencia electrónica y mecanismos de confianza digital, conforme a la normatividad vigente y a los principios de seguridad, trazabilidad, confidencialidad, integridad y responsabilidad demostrada (accountability).
La organización adoptará medidas razonables orientadas a garantizar la autenticidad, confiabilidad, trazabilidad y conservación de la información asociada a procesos

electrónicos, mensajes de datos, mecanismos de autenticación y evidencias digitales generadas durante la prestación de sus servicios tecnológicos y plataformas digitales.

13.1. Servicios de Firma Electrónica

AutenTIC podrá realizar tratamiento de datos personales relacionados con servicios de firma electrónica, aceptación electrónica, validación documental y demás mecanismos digitales utilizados para la manifestación de voluntad en medios electrónicos.

13.2. Validación de Identidad

La organización podrá utilizar mecanismos físicos, digitales, biométricos o tecnológicos para procesos de autenticación, validación y verificación de identidad de usuarios, clientes, proveedores y demás titulares de información.

13.3. OTP y Factores de Autenticación

AutenTIC podrá implementar mecanismos de autenticación, validación transaccional, códigos OTP, autenticación multifactor y demás controles tecnológicos orientados a fortalecer la seguridad y confiabilidad de sus servicios digitales.

13.4. Evidencia Electrónica

La organización podrá generar, almacenar, conservar y gestionar evidencias electrónicas relacionadas con transacciones, autenticaciones, validaciones, accesos, firmas electrónicas y demás eventos asociados a sus plataformas y servicios digitales.

13.5. Registros de Auditoría y Logs

AutenTIC podrá administrar registros de auditoría, trazabilidad técnica, logs, eventos de seguridad, marcas de tiempo y demás mecanismos orientados a monitoreo, control, seguridad y soporte probatorio de las operaciones realizadas en sus sistemas y plataformas tecnológicas.

13.6. Trazabilidad y Conservación Probatoria

La organización adoptará medidas orientadas a garantizar la trazabilidad, integridad, conservación y disponibilidad de la información electrónica y evidencias digitales generadas durante la prestación de sus servicios, conforme a las obligaciones legales, regulatorias y contractuales aplicables.

14. TRANSMISIÓN, TRANSFERENCIA DE DATOS

AutenTIC podrá realizar transmisión y transferencia de datos personales en desarrollo de sus actividades corporativas, contractuales, tecnológicas y operacionales, conforme a las finalidades autorizadas por los titulares, la normatividad vigente y los principios de seguridad, confidencialidad, trazabilidad y responsabilidad demostrada (accountability).

La organización adoptará medidas razonables orientadas a garantizar que las transmisiones y transferencias de datos personales realizadas con terceros, aliados, proveedores tecnológicos, operadores cloud, integradores, clientes corporativos y demás entidades relacionadas, se efectúen bajo condiciones adecuadas de protección de la información y cumplimiento normativo.

14.1. Transmisión Nacional

AutenTIC podrá realizar transmisión de datos personales dentro del territorio nacional con Encargados del Tratamiento, proveedores, operadores tecnológicos o terceros autorizados para el desarrollo de actividades relacionadas con la prestación de servicios y operación de la organización.

14.2. Transferencia Internacional

La organización podrá realizar transferencia internacional de datos personales cuando ello sea necesario para la prestación de servicios, operación de plataformas tecnológicas, interoperabilidad, almacenamiento, procesamiento o cumplimiento de obligaciones contractuales y legales, conforme a las condiciones establecidas en la normatividad aplicable.

14.3. Transmisión con Encargados

Los Encargados del Tratamiento que reciban datos personales por cuenta de AutenTIC deberán cumplir las obligaciones de confidencialidad, seguridad, protección de la información y demás condiciones definidas por la organización y la normatividad vigente.

14.4. Proveedores Cloud y SaaS

AutenTIC podrá utilizar servicios cloud, plataformas SaaS, infraestructura tecnológica y servicios especializados prestados por terceros nacionales o internacionales para el desarrollo de sus actividades y servicios digitales, adoptando medidas razonables de protección de la información y gestión de riesgos.

14.5. APIs e Interoperabilidad

La organización podrá implementar mecanismos de interoperabilidad, integraciones tecnológicas, APIs y servicios digitales interconectados para facilitar procesos de validación, autenticación, firma electrónica, intercambio de información y prestación de servicios tecnológicos.

14.6. Autoridades Competentes

AutenTIC podrá suministrar o compartir datos personales cuando exista obligación legal, requerimiento judicial, administrativo o solicitud válida de autoridad competente conforme a la normatividad aplicable.

14.7. Garantías Contractuales

La organización promoverá la incorporación de cláusulas, acuerdos, obligaciones de confidencialidad y demás mecanismos contractuales orientados a garantizar la protección de los datos personales tratados por terceros, aliados, proveedores y Encargados del Tratamiento.

15. DERECHOS DE LOS TITULARES

AutenTIC garantizará a los titulares de los datos personales el ejercicio de los derechos previstos en la normatividad vigente aplicable en materia de protección de datos personales y habeas data, conforme a los principios de legalidad, transparencia, acceso, confidencialidad y responsabilidad demostrada (accountability).

Los titulares de los datos personales podrán ejercer, entre otros, los siguientes derechos:

15.1. Derecho de Acceso

Conocer y acceder a los datos personales que sean objeto de tratamiento por parte de AutenTIC.

15.2. Derecho de Actualización

Solicitar la actualización de sus datos personales cuando estos hayan sufrido modificaciones o cambios.

15.3. Derecho de Rectificación

Solicitar la corrección o rectificación de datos personales cuando resulten inexactos, incompletos o induzcan a error.

15.4. Derecho de Supresión

Solicitar la supresión de los datos personales cuando resulte procedente conforme a la normatividad vigente y siempre que no exista obligación legal o contractual que impida su eliminación.

15.5. Derecho de Revocatoria

Revocar la autorización otorgada para el tratamiento de datos personales en los casos permitidos por la ley.

15.6. Derecho de Información

Solicitar información relacionada con el uso, tratamiento y finalidades aplicables a sus datos personales.

15.7. Derecho de Queja ante la SIC

Presentar quejas ante la Superintendencia de Industria y Comercio (SIC) por presuntas infracciones relacionadas con el tratamiento de datos personales, una vez agotado el trámite de consulta o reclamo ante AutenTIC cuando ello resulte aplicable.

15.8. Derechos frente a IA y Automatización

Los titulares podrán solicitar información general relacionada con el uso de mecanismos automatizados, tecnologías de validación, biometría, autenticación o herramientas de inteligencia artificial utilizadas por la organización, conforme a la naturaleza de los servicios prestados y las disposiciones aplicables.

16. PROCEDIMIENTO GENERAL PARA EL EJERCICIO DE DERECHOS

AutenTIC establecerá mecanismos y procedimientos orientados a garantizar el ejercicio de los derechos de los titulares de los datos personales, conforme a la normatividad vigente aplicable y a los principios de transparencia, acceso, confidencialidad, trazabilidad y responsabilidad demostrada (accountability).

Los titulares podrán presentar consultas, solicitudes, reclamos o requerimientos relacionados con el tratamiento de sus datos personales mediante los canales definidos por la organización.

16.1. Canales de Atención

AutenTIC dispondrá de canales físicos, electrónicos y digitales para la recepción y atención de consultas, solicitudes y reclamos relacionados con el tratamiento de datos personales.

Canales oficiales para el ejercicio de los derechos de los titulares del tratamiento de personales:

- Envío de petición escrita en medio físico a la dirección Calle 93B # 13-30 oficina 202, Bogotá D.C.
- Enviar un correo manifestando de manera expresa su solicitud (conocer, actualizar, rectificar o suprimir sus datos personales) al correo privacidad@autentic.com.co.

16.2. Consultas

Los titulares podrán presentar consultas relacionadas con la existencia, acceso, uso o tratamiento de sus datos personales conforme a los mecanismos definidos por la organización y la normatividad vigente.

16.3. Reclamos

Los titulares podrán presentar reclamos cuando consideren que la información tratada por AutenTIC deba ser corregida, actualizada, suprimida o cuando adviertan presuntos incumplimientos relacionados con el tratamiento de datos personales.

16.4. Validación de Identidad del Solicitante

La organización podrá implementar mecanismos de validación y autenticación orientados a verificar la identidad del titular o de su representante antes de suministrar información o atender solicitudes relacionadas con datos personales.

16.5. Términos de Respuesta

AutenTIC atenderá las consultas, solicitudes y reclamos dentro de los términos establecidos en la normatividad vigente aplicable.

16.6. Escalamiento

La organización podrá establecer mecanismos internos de revisión, seguimiento y escalamiento para la adecuada atención de solicitudes relacionadas con protección de datos personales.

16.7. Casos Especiales

AutenTIC podrá aplicar validaciones, controles o procedimientos adicionales cuando las solicitudes involucren datos sensibles, información biométrica, evidencias electrónicas, validación de identidad, representación legal, requerimientos de autoridad competente o situaciones que requieran medidas reforzadas de seguridad y verificación.

17. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

AutenTIC adoptará medidas administrativas, técnicas, humanas, organizacionales y tecnológicas orientadas a proteger la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los datos personales bajo su responsabilidad, conforme a la naturaleza de la información, los riesgos asociados al tratamiento y la normatividad vigente aplicable.

La organización promoverá la integración de controles de privacidad y seguridad de la información como parte de su modelo corporativo de gobernanza digital, gestión de riesgos y mejora continua, articulando el Programa Integral de Gestión de Datos Personales (PIGDP) con el Sistema de Gestión de Seguridad de la Información (SGSI).

17.1. Integración con el SGSI

El Programa Integral de Gestión de Datos Personales (PIGDP) se articulará con el Sistema de Gestión de Seguridad de la Información (SGSI) de AutenTIC para fortalecer la protección de los activos de información, la gestión de riesgos y los controles de seguridad aplicables al tratamiento de datos personales.

17.2. Controles de Seguridad

La organización podrá implementar controles de seguridad físicos, lógicos, tecnológicos y organizacionales orientados a prevenir acceso no autorizado, pérdida, alteración, divulgación, uso indebido o tratamiento no autorizado de los datos personales.

17.3. Gestión de Riesgos de Privacidad

AutenTIC podrá desarrollar actividades de identificación, análisis, evaluación y tratamiento de riesgos relacionados con privacidad, seguridad de la información, biometría, identidad digital, inteligencia artificial y demás tecnologías utilizadas por la organización.

17.4. Monitoreo y Trazabilidad

La organización podrá implementar mecanismos de monitoreo, registros de auditoría, logs, trazabilidad técnica y controles de seguimiento orientados a fortalecer la seguridad, integridad y control de las operaciones realizadas sobre los datos personales.

17.5. Gestión de Incidentes

AutenTIC podrá establecer mecanismos de detección, atención, gestión y respuesta frente a incidentes que puedan afectar la seguridad, privacidad o protección de los datos personales tratados por la organización.

17.6. Continuidad y Respaldo de la Información

La organización podrá implementar medidas de respaldo, recuperación, continuidad operativa y protección de información orientadas a garantizar la disponibilidad y resiliencia de los servicios y datos personales tratados.

17.7. Desarrollo Seguro y Tecnologías Digitales

AutenTIC promoverá la adopción de buenas prácticas de seguridad y privacidad en el diseño, desarrollo, implementación y operación de plataformas, aplicaciones, servicios digitales y mecanismos tecnológicos utilizados por la organización.

18. GESTIÓN DE INCIDENTES DE PRIVACIDAD Y SEGURIDAD

AutenTIC establecerá mecanismos orientados a la identificación, reporte, atención y gestión de incidentes que puedan afectar la privacidad, confidencialidad, integridad, disponibilidad o tratamiento adecuado de los datos personales bajo su responsabilidad.

La organización promoverá una cultura de reporte oportuno, gestión de riesgos y mejora continua frente a eventos relacionados con fuga de información, acceso no autorizado, pérdida, alteración, divulgación indebida, incidentes tecnológicos y demás situaciones que puedan comprometer la protección de los datos personales y la seguridad de la información.

La gestión de incidentes de privacidad y seguridad de la información será abordada de manera integral y articulada con el Sistema de Gestión de Seguridad de la Información (SGSI), el Plan de Respuesta a Incidentes de Seguridad de la Información y los procedimientos internos definidos por la organización para la gestión, tratamiento, notificación y seguimiento de incidentes.

AUTENTIC LATAM S.A.S. podrá adoptar medidas administrativas, técnicas, organizacionales y operacionales orientadas a prevenir, contener, mitigar y gestionar incidentes relacionados con privacidad y seguridad de la información, conforme a la naturaleza del evento, los riesgos identificados y las obligaciones legales o regulatorias aplicables.

19. RETENCIÓN, CONSERVACIÓN Y SUPRESIÓN DE DATOS

AutenTIC realizará la retención, conservación, almacenamiento, supresión y disposición de datos personales conforme a la naturaleza de la información, las finalidades autorizadas, las obligaciones legales, regulatorias, contractuales y los principios de necesidad, proporcionalidad, seguridad, confidencialidad y responsabilidad demostrada (accountability).

La organización adoptará medidas razonables orientadas a garantizar la adecuada conservación, protección, disponibilidad, trazabilidad y eliminación segura de los datos personales y evidencias electrónicas bajo su responsabilidad.

19.1. Criterios de Retención

AutenTIC conservará los datos personales únicamente durante el tiempo necesario para cumplir las finalidades del tratamiento, obligaciones legales, regulatorias, contractuales, probatorias, de seguridad o requerimientos de autoridades competentes.

19.2. Conservación Probatoria

La organización podrá conservar información, registros, evidencias electrónicas, trazabilidad, logs, autenticaciones, validaciones y demás elementos relacionados con servicios digitales, firma electrónica, identidad digital y seguridad de la información, cuando ello resulte necesario para fines probatorios, contractuales, legales, regulatorios o de auditoría.

19.3. Eliminación Segura

AutenTIC podrá implementar mecanismos orientados a la eliminación, destrucción o disposición segura de datos personales cuando finalicen las finalidades del tratamiento o cuando resulte procedente conforme a la normatividad aplicable.

19.4. Anonimización y Seudoanonimización

La organización podrá aplicar mecanismos de anonimización, seudoanonimización, disociación u otras técnicas orientadas a reducir riesgos de identificación y fortalecer la protección de la información personal.

19.5. Retención de Logs y Evidencias

AutenTIC podrá conservar registros de auditoría, logs, eventos, evidencias electrónicas, trazabilidad técnica y demás información relacionada con seguridad, autenticación, validación de identidad, biometría, firma electrónica y operación de plataformas digitales, conforme a necesidades operativas, de seguridad, cumplimiento y soporte probatorio.

20. TRATAMIENTO DE DATOS DE NIÑOS, NIÑAS Y ADOLESCENTES

AutenTIC realizará el tratamiento de datos personales de niños, niñas y adolescentes únicamente en los casos permitidos por la normatividad vigente y garantizando el respeto de sus derechos fundamentales, el interés superior del menor y las medidas reforzadas de protección aplicables.

La organización adoptará medidas razonables orientadas a prevenir el uso inadecuado de información de menores de edad y promoverá criterios de necesidad, proporcionalidad, seguridad y protección reforzada en el tratamiento de este tipo de información.

20.1. Principios Aplicables

El tratamiento de datos personales de niños, niñas y adolescentes se realizará bajo criterios de protección reforzada, interés superior del menor, respeto de sus derechos fundamentales, confidencialidad y seguridad de la información.

20.2. Consentimiento del Representante Legal

AutenTIC solicitará autorización previa del representante legal o persona facultada cuando el tratamiento de datos personales de menores de edad así lo requiera conforme a la normatividad aplicable.

20.3. Restricciones Especiales

La organización podrá limitar, restringir o abstenerse de realizar determinados tratamientos de datos personales de menores de edad cuando ello resulte necesario para garantizar la protección de sus derechos o prevenir riesgos asociados al uso de tecnologías digitales.

20.4. Limitaciones Biométricas y Automatizadas

AutenTIC podrá adoptar restricciones o controles reforzados frente al uso de tecnologías biométricas, automatizadas o mecanismos de inteligencia artificial relacionados con datos personales de niños, niñas y adolescentes, conforme a criterios de protección reforzada y gestión de riesgos.

21. INTEGRACIÓN DEL PIGDP CON EL SISTEMA INTEGRADO DE GESTIÓN (SIG)

AutenTIC reconoce la protección de datos personales, la privacidad y la seguridad de la información como componentes integrados dentro de su Sistema Integrado de Gestión (SIG), promoviendo un enfoque articulado de cumplimiento, gestión de riesgos, seguridad, mejora continua y confianza digital.

El Programa Integral de Gestión de Datos Personales (PIGDP) se desarrolla de manera coordinada con los demás sistemas, políticas, procesos y controles corporativos implementados por la organización, especialmente aquellos relacionados con seguridad de la información, gestión de riesgos, continuidad, cumplimiento, gestión documental, tecnologías digitales y mejora continua.

21.1. Articulación Estratégica

El PIGDP se integra con el Sistema Integrado de Gestión (SIG) como parte del modelo corporativo de gobernanza, fortaleciendo capacidades relacionadas con privacidad, seguridad, cumplimiento, monitoreo, trazabilidad y protección de la información.

21.2. Relación con el SGSI ISO/IEC 27001:2022

El Programa Integral de Gestión de Datos Personales (PIGDP) se articula con el Sistema de Gestión de Seguridad de la Información (SGSI) alineado con la norma ISO/IEC 27001:2022, permitiendo fortalecer la protección de activos de información, la gestión de riesgos y los controles aplicables al tratamiento de datos personales.

21.3. Controles Integrados y Gestión de Riesgos

AutenTIC podrá aplicar controles administrativos, técnicos, organizacionales y de seguridad definidos dentro de sus sistemas de gestión para apoyar la protección, confidencialidad, integridad, disponibilidad y trazabilidad de los datos personales tratados por la organización.

21.4. Evidencias y Accountability

La organización promoverá mecanismos de documentación, monitoreo, trazabilidad, conservación de evidencias y registros orientados a demostrar el cumplimiento de las obligaciones aplicables en materia de protección de datos personales, privacidad y seguridad de la información.

21.5. Auditoría y Mejora Continua

AutenTIC podrá desarrollar actividades de seguimiento, auditoría, evaluación y mejora continua relacionadas con el PIGDP y los sistemas de gestión asociados, con el fin de fortalecer los controles de privacidad, seguridad, cumplimiento y gestión integral de riesgos.

22. CAPACITACIÓN, CONCIENTIZACIÓN Y CULTURA

AutenTIC promoverá actividades de capacitación, sensibilización y fortalecimiento de cultura organizacional orientadas a la protección de datos personales, privacidad,

seguridad de la información, gestión de riesgos y uso responsable de tecnologías digitales.

La organización fomentará el desarrollo de competencias y buenas prácticas relacionadas con el tratamiento adecuado de datos personales, conforme a las responsabilidades aplicables a colaboradores, contratistas, terceros y demás personas que intervengan en actividades relacionadas con el Programa Integral de Gestión de Datos Personales (PIGDP).

22.1. Sensibilización

AutenTIC podrá desarrollar actividades de sensibilización orientadas a fortalecer la cultura de privacidad, confidencialidad, protección de datos personales y seguridad de la información dentro de la organización.

22.2. Formación Interna

La organización podrá implementar programas de formación interna relacionados con protección de datos personales, tratamiento adecuado de información, seguridad digital, gestión de riesgos y cumplimiento de obligaciones aplicables.

22.3. Capacitación Especializada

AutenTIC podrá promover capacitaciones especializadas para roles, procesos o actividades que involucren tratamiento de datos sensibles, biometría, inteligencia artificial, identidad digital, firma electrónica, seguridad de la información o tecnologías emergentes.

22.4. Responsabilidad del Personal

Todos los colaboradores, contratistas, proveedores y terceros que intervengan en actividades relacionadas con el tratamiento de datos personales deberán cumplir las políticas, lineamientos y controles definidos por la organización en materia de privacidad, seguridad de la información y protección de datos personales.

23. AUDITORÍA, MONITOREO Y MEJORA CONTINUA

AutenTIC promoverá actividades de seguimiento, monitoreo, evaluación y mejora continua orientadas a fortalecer la efectividad del Programa Integral de Gestión de Datos Personales (PIGDP), la protección de datos personales, la privacidad y la seguridad de la información.

La organización podrá implementar mecanismos de control, revisión y evaluación periódica relacionados con cumplimiento normativo, gestión de riesgos, controles de

seguridad, tratamiento de datos personales, tecnologías digitales y demás componentes asociados al PIGDP y al Sistema Integrado de Gestión (SIG).

23.1. Seguimiento

AutenTIC podrá desarrollar actividades de seguimiento relacionadas con la implementación, cumplimiento y efectividad de los lineamientos, controles y medidas asociadas al tratamiento de datos personales.

23.2. Indicadores

La organización podrá definir indicadores, métricas o mecanismos de medición orientados a evaluar el desempeño, cumplimiento y madurez de las actividades relacionadas con privacidad, protección de datos personales y seguridad de la información.

23.3. Auditorías

AutenTIC podrá realizar actividades de auditoría, revisión o verificación relacionadas con el cumplimiento de las disposiciones aplicables en materia de protección de datos personales, privacidad y seguridad de la información.

23.4. Revisión y Actualización

La presente política podrá ser revisada y actualizada por la organización cuando existan cambios normativos, regulatorios, tecnológicos, organizacionales o de riesgos que así lo requieran.

23.5. Mejora Continua

La organización promoverá actividades de mejora continúa orientadas al fortalecimiento del Programa Integral de Gestión de Datos Personales (PIGDP), los controles de privacidad, la seguridad de la información y la gestión integral de riesgos asociados al tratamiento de datos personales.

24. VIGENCIA Y ACTUALIZACIÓN DE LA POLÍTICA

La presente Política Integral de Tratamiento de Datos Personales de AutenTIC entra en vigencia a partir de su aprobación y publicación por parte de la organización, y permanecerá aplicable mientras se desarrollen actividades relacionadas con el tratamiento de datos personales bajo responsabilidad de la compañía.

La organización podrá realizar modificaciones, actualizaciones o ajustes a la presente política cuando existan cambios normativos, regulatorios, tecnológicos, organizacionales, contractuales, operacionales o asociados a riesgos que así lo requieran.

24.1. Vigencia

La presente política tendrá vigencia indefinida a partir de su entrada en aplicación, sin perjuicio de las actualizaciones que pueda realizar la organización conforme a sus necesidades de cumplimiento y mejora continua.

24.2. Actualizaciones

AutenTIC podrá actualizar, modificar o complementar la presente política cuando resulte necesario para fortalecer la protección de datos personales, privacidad, seguridad de la información, gestión de riesgos o cumplimiento de obligaciones legales y regulatorias aplicables.

24.3. Comunicación de Cambios Sustanciales

Cuando se realicen cambios sustanciales en la presente política que puedan afectar las finalidades del tratamiento o los derechos de los titulares, la organización podrá comunicar dichas modificaciones mediante sus canales institucionales, plataformas digitales, avisos de privacidad u otros mecanismos que considere pertinentes.

La presente Política rige a partir de su firma y complementa las políticas asociadas, con vigencia indefinida.

Esta política será revisada y actualizada periódicamente para asegurar su vigencia y adecuación a la legislación aplicable. Cualquier cambio significativo será comunicado a los titulares de los datos.

LUIS MIGUEL GONZALEZ ULLOA
Director General

CONTROL DE VERSIONES Y CAMBIOS

Versión	Fecha aprobación	Nota de cambio
1	30/07/2024	Versión Inicial
2	11/03/2025	Se modifico el numeral 4 de autorización vinculando el nuevo formato de Autorización de Tratamiento de Datos Personales.
3	01/06/2026	Actualización integral de la Política de Tratamiento de Datos Personales para su alineación con el Programa Integral de Gestión de Datos Personales (PIGDP), incorporando nuevos capítulos relacionados con gobierno y responsabilidades, categorías de titulares y datos personales, tratamiento biométrico, inteligencia artificial, firma electrónica, identidad digital, transmisión y transferencia de datos, integración con el Sistema Integrado de Gestión (SIG), seguridad de la información, gestión de incidentes, conservación probatoria, accountability y mejora continua.