



UANATACA ECUADOR S. A.

POLÍTICA DE PROTECCION DE DATOS

Código:	GES-PO-02
Versión:	0.3
Fecha de la versión:	2026-09-08
Tipo De Documento:	Política
Proceso al que pertenece:	Gestión Estratégica y Compliance
Elaborado por:	Compliance Officer



Firmado por: ELSI MARIANA TAMBACO QUIÑONEZ
Dirección IP: 200.63.106.19
Firmado con eSignAnyWhere

Se puede validar el documento en <https://vol.uanataca.ec>

Revisado y Aprobado por:	Gerente General
--------------------------	-----------------



Firmado por: ELIAS MAURICIO BARZALLO SACOTO
Dirección IP: 186.65.55.227
Firmado con eSignAnyWhere

Se puede validar el documento en <https://vol.uanataca.ec>

Nivel de confidencialidad:	Público
----------------------------	---------

Historial de Modificaciones

Fecha cambio	No. de Versión	Autor del Cambio	Descripción de la modificación
19-10-2023	0.1	Consultora Road Quality - Equipo de Proyecto SGSI	Descripción básica del documento
20/6/2025	0.2	Equipo de Proyecto SGSI	Modificación de Datos de contacto
08/09/2026	0.3	Compliance Officer	Actualización normativa LOPDP/RGLOPDP, SPDP, ARCOTEL e ISO 27001/27017/27018 aplicable; ajuste de bases legitimadoras, transferencias, encargados, seguridad, cloud, incidentes, cookies y resumen público de tratamientos.

Tabla de Contenido

HISTORIAL DE MODIFICACIONES.....	2
TABLA DE CONTENIDO	3
1. OBJETIVO	5
2. ALCANCE Y USUARIOS	5
3. DOCUMENTOS DE REFERENCIA.....	5
4. DEFINICIONES Y ABREVIATURAS.....	5
5. ROLES Y RESPONSABILIDADES.....	8
6. DESARROLLO DEL DOCUMENTO	10
6.1. CONSIDERACIONES GENERALES	10
6.2. OBLIGATORIEDAD	11
6.3. PRINCIPIOS DEL TRATAMIENTO DE DATOS PERSONALES.....	11
6.4. BASES LEGITIMADORAS DEL TRATAMIENTO Y CONSENTIMIENTO DEL TITULAR	13
6.5. TRATAMIENTO DE DATOS PERSONALES SENSIBLES	14
6.6. DERECHOS DE LOS TITULARES DE LOS DATOS.....	14
6.7. INFORMACIÓN A LOS TITULARES DE LOS DATOS PERSONALES	15
6.7.1 FINALIDAD DEL TRATAMIENTO DE LOS DATOS DE LOS CLIENTES	15
6.7.2 FINALIDAD DEL TRATAMIENTO DE LOS DATOS DE LOS TRABAJADORES	15
6.7.3 FINALIDAD DEL TRATAMIENTO DE LOS PROVEEDORES	15
6.7.4 FINALIDAD DEL TRATAMIENTO DE LOS SOCIOS	16
6.8. BASES LEGITIMADORAS APLICABLES AL TRATAMIENTO	17
6.9. CATEGORÍAS DE DATOS PERSONALES Y TITULARES	17
6.9.1 CLIENTES Y USUARIOS.....	17
6.9.2 PROVEEDORES.....	18
6.9.3 TRABAJADORES	18
6.10. TIEMPO DE CONSERVACIÓN	18
6.11. EXISTENCIA DE UNA BASE DE DATOS EN LA QUE CONSTAN SUS DATOS PERSONALES	19
6.12. ORIGEN DE LOS DATOS PERSONALES CUANDO NO SE HAYAN OBTENIDO DIRECTAMENTE DEL TITULAR	19
6.13. OTRAS FINALIDADES Y TRATAMIENTOS ULTERIORES	19
6.14. IDENTIDAD Y DATOS DE CONTACTO DEL RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES	19
6.15. LAS TRANSFERENCIAS O COMUNICACIONES, NACIONALES O INTERNACIONALES, DE DATOS PERSONALES	19
6.16. ENCARGADOS, SUBENCARGADOS Y DESTINATARIOS	20
6.17. CONSECUENCIAS PARA EL TITULAR DE LOS DATOS PERSONALES DE SU ENTREGA O NEGATIVA A ELLO	20
6.18. EFECTO DE SUMINISTRAR DATOS PERSONALES ERRÓNEOS O INEXACTOS	20
6.19. LA POSIBILIDAD DE REVOCAR EL CONSENTIMIENTO	20
6.20. MECANISMOS PARA EJERCER LOS DERECHOS	20
6.21. MEDIOS PARA PARA HACER EFECTIVO SU DERECHO A LA PORTABILIDAD	21
6.22. MEDIOS PARA PRESENTAR RECLAMOS.....	21

6.23.	VALORACIONES Y DECISIONES AUTOMATIZADAS, INCLUIDA LA ELABORACIÓN DE PERFILES.....	21
6.24.	DERECHOS DE LOS TITULARES DE LOS DATOS.....	21
6.24.1	DERECHO DE ACCESO (ARTÍCULO 13 DE LA LOPDP):.....	21
6.24.2	DERECHO DE RECTIFICACIÓN Y ACTUALIZACIÓN (ARTÍCULOS 14 Y 18 DE LA LOPDP):.....	21
6.24.3	DERECHO DE ELIMINACIÓN (ARTÍCULOS 15 Y 18 DE LA LOPDP):.....	22
6.24.4	DERECHO DE OPOSICIÓN (ARTÍCULOS 16 Y 18 DE LA LOPDP):.....	22
6.24.5	DERECHO A LA PORTABILIDAD (ARTÍCULOS 17 Y 18 DE LA LOPDP):	22
6.24.6	DERECHO A LA SUSPENSIÓN DEL TRATAMIENTO (ARTÍCULO 19 DE LA LOPDP):	23
6.24.7	DERECHO A NO SER OBJETO DE UNA DECISIÓN BASADA ÚNICA O PARCIALMENTE EN VALORACIONES AUTOMATIZADAS (ARTÍCULO 20 DE LA LOPDP):	23
6.24.8	DERECHO DE NIÑAS, NIÑOS Y ADOLESCENTES (ARTÍCULO 21 DE LA LOPDP):	24
6.24.9	DERECHO DE CONSULTA (ARTÍCULO 22 DE LA LOPDP):	24
6.24.10	DERECHO A LA EDUCACIÓN DIGITAL (ARTÍCULO 23 DE LA LOPDP):	24
6.25.	DELEGADO DE PROTECCIÓN DE DATOS PERSONALES	25
6.26.	REQUERIMIENTO DIRECTO DEL TITULAR DEL DATO DE CARÁCTER PERSONAL AL RESPONSABLE DEL TRATAMIENTO	25
6.27.	SEGURIDAD EN EL TRATAMIENTO DE DATOS PERSONALES	26
6.28.	SERVICIOS EN LA NUBE Y RESPONSABILIDAD COMPARTIDA	28
6.29.	PROTECCIÓN DE DATOS PERSONALES EN SERVICIOS CLOUD	28
6.30.	REQUISITOS REGULATORIOS APLICABLES A SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA.....	29
6.31.	VIDEOVIGILANCIA.....	29
6.32.	RESPONSABILIDAD DEMOSTRADA Y PROACTIVA FRENTE AL TRATAMIENTO DE DATOS PERSONALES.	30
6.33.	PROCESO DE VERIFICACIÓN Y EVALUACIÓN	30
6.34.	PROTECCIÓN DE DATOS PERSONALES DESDE EL DISEÑO Y POR DEFECTO (PRIVACY BY DESIGN AND BY DEFAULT) Y ESTUDIOS DE IMPACTO DE PRIVACIDAD (PRIVACY IMPACT ASSESSMENT - PIA).	30
6.35.	COOKIES	31
6.35.1	TRATAMIENTO DE COOKIES	31
6.35.2	¿QUIÉN SIRVE ESTAS COOKIES Y POR QUÉ?	32
6.35.3	TUS OPCIONES:	32
6.36.	USO DE LA APLICACIÓN MÓVIL: UANATACA.....	33
6.37.	ANEXO 1. RESUMEN PÚBLICO DE ACTIVIDADES DE TRATAMIENTO	33
7.	VALIDEZ, REVISIÓN Y GESTIÓN DEL DOCUMENTO.....	35

1. Objetivo

Establecer los lineamientos mínimos para el tratamiento lícito, leal, transparente, seguro y proporcional de los datos personales tratados por UANATACA ECUADOR S.A., en calidad de responsable, encargado o corresponsable, según corresponda a cada actividad registrada en el RID/RAT, garantizando el ejercicio de los derechos de los titulares, la protección de la confidencialidad, integridad y disponibilidad de la información, y el cumplimiento de la Ley Orgánica de Protección de Datos Personales, su Reglamento, normativa aplicable de la Superintendencia de Protección de Datos Personales y la ARCOTEL cuando corresponda, y los controles aplicables del SGSI basado en ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018, sin sustituir los contratos, avisos de privacidad, Declaración de Prácticas de Certificación, procedimientos internos ni demás documentos específicos aplicables.

2. Alcance y usuarios

La presente política aplica a todos los procesos, áreas, activos de información, sistemas, plataformas, servicios tecnológicos y servicios en la nube incluidos en el SGSI. Es de cumplimiento obligatorio para colaboradores, directivos, contratistas, proveedores, terceros, partners y usuarios internos o externos que accedan, procesen o gestionen información de la organización.

3. Documentos de referencia

- Constitución de la República del Ecuador, artículos 66 numeral 19 y 92.
- Ley Orgánica de Protección de Datos Personales (LOPDP).
- Reglamento General a la Ley Orgánica de Protección de Datos Personales (RGLOPDP).
- Resoluciones y normativa aplicable de la Superintendencia de Protección de Datos Personales (SPDP).
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- Ley Orgánica de Defensa del Consumidor y normativa aplicable en materia de consumidores y usuarios, en lo que corresponda a la atención de solicitudes, quejas, reclamos, información al consumidor, prestación del servicio, términos y condiciones, canales de atención y relación contractual con clientes y usuarios.
- Normativa ARCOTEL aplicable al servicio.
- Declaración de Prácticas de Certificación (DPC).
- Contratos.
- ISO/IEC 27001:2022; ISO/IEC 27017:2015 e ISO/IEC 27018:2019, cuando aplique.

4. Definiciones y abreviaturas

Para efectos de este documento se tendrán en cuenta las definiciones establecidas en el artículo 4 de la LOPDP. En particular, las siguientes:

- **Autoridad de Protección de Datos Personales:** Autoridad independiente encargada de supervisar la aplicación de la LOPDP, su reglamento y resoluciones que ella dicte, con el fin de proteger los derechos y libertades fundamentales de las personas naturales, en cuanto al tratamiento de sus datos personales.
- **Anonimización:** La aplicación de medidas dirigidas a impedir la identificación o re-identificación de una persona natural, sin esfuerzos desproporcionados.
- **Base de datos o fichero:** Conjunto estructurado de datos cualquiera que fuera la forma, modalidad de creación, almacenamiento, organización, tipo de soporte, tratamiento, procesamiento, localización o acceso, centralizado, descentralizado o repartido de forma funcional o geográfica.
- **Consentimiento:** Manifestación de la voluntad libre, específica, informada e inequívoca, por el que el titular de los datos personales autoriza al responsable del tratamiento de los datos personales a tratar los mismos.
- **Dato biométrico:** Dato personal único, relativo a las características físicas o fisiológicas, o conductas de una persona natural que permita o confirme la identificación única de dicha persona como imágenes faciales o datos dactiloscópicos, entre otros.
- **Dato genético:** Dato personal único relacionado a características genéticas heredadas o adquiridas de una persona natural que proporcionan información única sobre la fisiología o salud de un individuo.
- **Dato personal:** Dato que identifica o hace identificable a una persona natural, directa o indirectamente.
- **Datos personales crediticios:** Datos que integran el comportamiento económico de personas naturales, para analizar su capacidad financiera.
- **Datos relativos a la salud:** datos personales relativos a la salud física o mental de una persona, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.
- **Datos sensibles:** Datos relativos a etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.
- **Delegado de protección de datos:** Persona natural encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la

Autoridad de Protección de Datos Personales, sirviendo como punto de contacto entre esta y la entidad responsable del tratamiento de datos.

- **Destinatario:** Persona natural o jurídica que ha sido comunicada con datos personales.
- **Elaboración de perfiles:** Todo tratamiento de datos personales que permite evaluar, analizar o predecir aspectos de una persona natural para determinar comportamientos o estándares relativos a: rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, ubicación, movimiento físico de una persona, entre otros.
- **Encargado del tratamiento de datos personales:** Persona natural o jurídica, pública o privada, autoridad, u otro organismo que solo o juntamente con otros trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales.
- **Entidad Certificadora:** Entidad reconocida por la Autoridad de Protección de Datos Personales, que podrá, de manera no exclusiva, proporcionar certificaciones en materia de protección de datos personales.
- **Fuente accesible al público:** Bases de datos que pueden ser consultadas por cualquier persona, cuyo acceso es público, incondicional y generalizado.
- **LODPD:** Ley Orgánica de Protección de Datos Personales de la República del Ecuador, publicada en el R.O. 5to S. No.459 del 26 de mayo de 2021.
- **Responsable de tratamiento de datos personales:** persona natural o jurídica, pública o privada, autoridad, u otro organismo, que solo o juntamente con otros decide sobre la finalidad y el tratamiento de datos personales.
- **Sellos de protección de datos personales:** Acreditación que otorga la entidad certificadora al responsable o al encargado del tratamiento de datos personales, de haber implementado mejores prácticas en sus procesos, con el objetivo de promover la confianza del titular, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales.
- **Seudonimización:** Tratamiento de datos personales de manera tal que ya no puedan atribuirse a un titular sin utilizar información adicional, siempre que dicha información adicional, figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

- **Subencargado del tratamiento:** Persona natural o jurídica, pública o privada, autoridad u otro organismo contratado por el encargado del tratamiento para realizar determinadas actividades de tratamiento de datos personales por cuenta del responsable, conforme a instrucciones documentadas y previa autorización contractual cuando corresponda.
- **Titular:** Persona natural cuyos datos son objeto de tratamiento.
- **Transferencia o comunicación:** Manifestación, declaración, entrega, consulta, interconexión, cesión, transmisión, difusión, divulgación o cualquier forma de revelación de datos personales realizada a una persona distinta al titular, responsable o encargado del tratamiento de datos personales. Los datos personales que comuniquen deben ser exactos, completos y actualizados.
- **Tratamiento:** Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recogida, recopilación, obtención, registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión, comunicación o transferencia, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales.
- **Vulneración de la seguridad de los datos personales:** Incidente de seguridad que afecta la confidencialidad, disponibilidad o integridad de los datos personales.

5. Roles y responsabilidades

Rol	Responsabilidades
Gerencia General / Alta Dirección	Aprobar esta política y sus actualizaciones; asignar los recursos necesarios para su implementación; exigir el cumplimiento de las obligaciones legales, regulatorias, contractuales y del SGSI; revisar periódicamente el desempeño y los riesgos relevantes en materia de protección de datos personales.
Compliance Officer / Delegado de Protección de Datos o función de privacidad designada	Coordinar la implementación de esta política; asesorar a las áreas sobre protección de datos personales; mantener o coordinar la actualización del RID/RAT; revisar bases legitimadoras, finalidades, plazos de conservación, transferencias, encargados y subencargados; apoyar la atención de derechos de los titulares; coordinar evaluaciones de impacto cuando correspondan; y servir como punto de contacto interno en materia de privacidad.

Rol	Responsabilidades
Responsable del SGSI / Seguridad de la Información	Definir, implementar, monitorear y mejorar los controles de seguridad aplicables al tratamiento de datos personales; gestionar riesgos de seguridad de la información; coordinar la gestión de incidentes y vulneraciones de seguridad; mantener evidencias del SGSI, SoA, auditorías, controles técnicos y planes de tratamiento de riesgos.
Dueños de proceso / Responsables de área	Asegurar que los tratamientos de datos personales bajo su proceso se realicen conforme al RAT, esta política y los procedimientos internos; validar la necesidad, proporcionalidad, finalidad, base legitimadora, conservación y acceso a los datos; reportar cambios, incidentes, nuevos tratamientos o proveedores que involucren datos personales.
Tecnología / Operaciones	Implementar controles técnicos y operativos autorizados para proteger los datos personales; gestionar accesos, trazabilidad, respaldos, continuidad, seguridad de plataformas, servicios cloud, gestión de cambios, vulnerabilidades y eliminación segura, conforme al SGSI y procedimientos internos.
Legal / Compras / Gestión de proveedores	Incorporar cláusulas de protección de datos, confidencialidad, seguridad, subencargados, retorno, eliminación, auditoría e incidentes en contratos con encargados, proveedores y terceros; verificar que los proveedores que traten datos personales cuenten con garantías proporcionales al riesgo.
Talento Humano	Asegurar que colaboradores y terceros bajo su gestión conozcan sus obligaciones de confidencialidad, protección de datos y seguridad de la información; coordinar capacitaciones, acuerdos de confidencialidad y medidas aplicables al ingreso, cambio o salida del personal.
Colaboradores, contratistas y terceros autorizados	Cumplir esta política, los procedimientos internos y las instrucciones recibidas; tratar datos personales solo para finalidades autorizadas; mantener confidencialidad; usar los accesos asignados de forma responsable; reportar incidentes, accesos indebidos, errores, pérdidas o vulneraciones de seguridad.
Encargados, subencargados y proveedores	Tratar datos personales únicamente conforme a instrucciones documentadas y contrato aplicable; aplicar medidas de seguridad proporcionales al riesgo; mantener confidencialidad; asistir en la atención de derechos e incidentes; y retornar, eliminar o anonimizar los datos al finalizar la relación, según corresponda.

En los servicios en la nube, UANATACA documentará la asignación de responsabilidades entre UANATACA, proveedores cloud, encargados y subencargados, considerando el modelo de responsabilidad compartida, los contratos, acuerdos de nivel de servicio, matriz de riesgos, evaluación de proveedores y Declaración de Aplicabilidad del SGSI.

6. Desarrollo del documento

6.1. Consideraciones generales

El artículo 92 de la Constitución de la República del Ecuador consagra el derecho de toda persona a “conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo, tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos”. Adicionalmente, establece que “las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley” y que “la persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados”.

La Ley Orgánica de Protección de Datos Personales de la República del Ecuador (en adelante LOPDP), publicada en el R.O. 5to S. No.459 del 26 de mayo de 2021, ordena a los responsables y encargados del tratamiento adecuarse a la misma dentro de los dos años siguientes a su publicación. Adicionalmente, señala que quienes hayan “implementado los preceptos recogidos dentro de esta LOPDP antes de plazo señalado en la Disposición Transitoria Primera obtendrán un reconocimiento por buenas prácticas por parte de la Autoridad de Protección de Datos Personales”.

La LOPDP tiene como finalidad garantizar el ejercicio del derecho a la protección de datos personales. Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela. El artículo 47 señala las obligaciones del responsable y el encargado dentro de las cuales está, entre otras, : “4) Implementar políticas de protección de datos personales afines al tratamiento de datos personales en cada caso en particular;” y “2) Aplicar e implementar requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas, a fin de garantizar y demostrar que el tratamiento de datos personales se ha realizado conforme a lo previsto en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, o normativa sobre la materia;”. El principio de transparencia, por su parte, obliga a que toda información o comunicación relativa al tratamiento de datos sea fácilmente accesible, fácil de entender redactarse en un lenguaje sencillo y claro. Adicionalmente, el artículo 12 de la LOPDP ordena informar a los titulares diferentes aspectos sobre el tratamiento de los datos personales.

UANATACA ECUADOR S.A. está comprometida con el respeto de los derechos de sus clientes, empleados y terceros en general. Por eso, para dar cumplimiento

a la LOPDP, adopta la siguiente política de protección de datos personales de obligatoria aplicación en todas las actividades que involucre el tratamiento de datos personales.

6.2.Obligatoriedad

Esta política es de obligatorio y estricto cumplimiento por parte de todos los empleados de la UANATACA ECUADOR S.A., los contratistas, distribuidores y terceros que obran en nombre de la UANATACA ECUADOR S.A. y los encargados del tratamiento de datos personales que le presten servicios.

Todos los empleados de UANATACA ECUADOR S.A. deben observar y respetar esta política en el cumplimiento de sus funciones. En los casos en que no exista vínculo laboral, se deberá incluir una cláusula contractual para que quienes obren en nombre de UANATACA ECUADOR S.A. se obliguen a cumplir estas políticas.

El incumplimiento de estas originará sanciones de tipo laboral o responsabilidad contractual según el caso. Lo anterior sin perjuicio del deber de responder patrimonialmente por los daños y perjuicios que cause a los titulares de los datos o a UANATACA ECUADOR S.A. por el incumplimiento de esta política o el indebido tratamiento de datos personales.

6.3.Principios del tratamiento de datos personales

El tratamiento de datos personales debe realizarse respetando las normas generales y especiales sobre la materia y para actividades permitidas por la LOPDP. En el desarrollo, interpretación y aplicación de la presente política, se aplicarán de manera armónica e integral los siguientes principios establecidos en el artículo 10 de la LOPDP, a saber:

- **Juridicidad:** Los datos personales deben tratarse con estricto apego y cumplimiento a los principios, derechos y obligaciones establecidas en la Constitución, los instrumentos internacionales, la LOPDP, su Reglamento y la demás normativa y jurisprudencia aplicable.
- **Lealtad:** El tratamiento de datos personales deberá ser leal, por lo que para los titulares debe quedar claro que se están recogiendo, utilizando, consultando o tratando de otra manera, datos personales que les conciernen, así como las formas en que dichos datos son o serán tratados. En ningún caso los datos personales podrán ser tratados a través de medios o para fines, ilícitos o desleales.
- **Transparencia:** El tratamiento de datos personales deberá ser transparente. Por lo que toda información o comunicación relativa a este tratamiento deberá ser fácilmente accesible y fácil de entender y se deberá utilizar un lenguaje sencillo y claro. Las relaciones derivadas del tratamiento de datos personales deben ser transparentes y se rigen en función de las disposiciones contenidas en la LOPDP, su reglamento y demás normativa atinente a la materia.

- **Finalidad:** ¡Las finalidades del tratamiento deberán ser determinadas, explícitas, legítimas y comunicadas al titular; no podrán tratarse datos personales con fines distintos para los cuales fueron recopilados, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en la LOPDP. El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. Para ello, habrá de considerarse el contexto en el que se recogieron los datos, la información facilitada al titular en ese proceso y, en particular, las expectativas razonables del titular basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los titulares del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista.
- **Pertinencia y minimización de datos personales:** Los datos personales deben ser pertinentes y estar limitados a lo estrictamente necesario para el cumplimiento de la finalidad del tratamiento.
- **Proporcionalidad del tratamiento:** El tratamiento debe ser adecuado, necesario, oportuno, relevante y no excesivo con relación a las finalidades para las cuales hayan sido recogidos o a la naturaleza misma, de las categorías especiales de datos.
- **Confidencialidad:** El tratamiento de datos personales debe concebirse sobre la base del debido sigilo y secreto, es decir, no debe tratarse o comunicarse para un fin distinto para el cual fueron recogidos, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en esta ley. Para tal efecto, el responsable del tratamiento deberá adecuar las medidas técnicas organizativas para cumplir con este principio.
- **Calidad y exactitud:** Los datos personales que sean objeto de tratamiento deben ser exactos, íntegros, precisos, completos, comprobables, claros; y, de ser el caso, ¡debidamente actualizados; de tal forma que no se altere su veracidad. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan. En caso de tratamiento por parte de un encargado, la calidad y exactitud será obligación del responsable del tratamiento de datos personales. Siempre que el responsable del tratamiento haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, no le será imputable la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos: a) Hubiesen sido obtenidos por el responsable directamente del titular; b) Hubiesen sido obtenidos por el responsable de un intermediario en caso de que las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establecieran la posibilidad de intervención de un

intermediario que recoja en nombre propio los datos de los afectados para su transmisión al responsable; c) Fuesen obtenidos de un registro público por el responsable.

- **Conservación:** Los datos personales serán conservados durante un tiempo no mayor al necesario para cumplir con la finalidad de su tratamiento. Para garantizar que los datos personales no se conserven más tiempo del necesario, el responsable del tratamiento establecerá plazos para su supresión o revisión periódica. La conservación ampliada de tratamiento de datos personales únicamente se realizará con fines de archivo en interés público, fines de investigación científica, histórica o estadística, siempre y cuando se establezcan las garantías de seguridad y protección de datos personales, oportunas y necesarias, para salvaguardar los derechos previstos en esta norma.
- **Seguridad de datos personales:** Los responsables y encargados de tratamiento de los datos personales deberán implementar todas las medidas de seguridad adecuadas y necesarias, entendiéndose por tales las aceptadas por el estado de la técnica, sean estas organizativas, técnicas o de cualquier otra índole, para proteger los datos personales, frente a cualquier riesgo, amenaza, vulnerabilidad, atendiendo a la naturaleza de los datos de carácter personal, al ámbito y el contexto.
- **Responsabilidad proactiva y demostrada:** El responsable del tratamiento de datos personales deberá acreditar el haber implementado mecanismos para la protección de datos personales; es decir, el cumplimiento de los principios, derechos y obligaciones establecidos en la LOPDP, para lo cual, además de lo establecido en la normativa aplicable, podrá valerse de estándares, mejores prácticas, esquemas de auto y coregulación, códigos de protección, sistemas de certificación, sellos de protección de datos personales o cualquier otro mecanismo que se determine adecuado a los fines, la naturaleza del dato personal o el riesgo del tratamiento. El responsable del tratamiento de datos personales está obligado a rendir cuentas sobre el tratamiento al titular y a la Autoridad de Protección de Datos Personales. El responsable del tratamiento de datos personales deberá evaluar y revisar los mecanismos que adopte para cumplir con el principio de responsabilidad de forma continua y permanente, con el objeto de mejorar su nivel de eficacia en cuanto a la aplicación de la presente Ley.
- **Aplicación favorable al titular:** En caso de duda sobre el alcance de las disposiciones del ordenamiento jurídico o contractuales, aplicables a la protección de datos personales, los funcionarios judiciales y administrativos las interpretarán y aplicarán en el sentido más favorable al titular de dichos datos.

6.4. Bases legitimadoras del tratamiento y consentimiento del titular

El tratamiento de datos personales realizado por UANATACA ECUADOR S.A. se sustentará en la base legitimadora que corresponda a cada actividad de

tratamiento, conforme conste en el Registro de Actividades de Tratamiento — RAT— vigente.

Las bases legitimadoras podrán incluir, según aplique, el consentimiento del titular, la ejecución de medidas precontractuales, la ejecución de una relación contractual, el cumplimiento de obligaciones legales o regulatorias, el cumplimiento de requerimientos de autoridad competente, el interés legítimo documentado u otras bases previstas en la normativa aplicable.

El consentimiento del titular será utilizado únicamente cuando sea la base legitimadora aplicable, especialmente en los casos en que la normativa exija consentimiento expreso o explícito y no se encuentren amparados en una base legitimadora distinta.

Cuando el tratamiento se base en el consentimiento, este deberá ser libre, específico, informado e inequívoco. UANATACA conservará evidencia verificable de la base legitimadora aplicable a cada tratamiento, incluyendo, cuando corresponda, la evidencia del consentimiento otorgado por el titular.

6.5.Tratamiento de datos personales sensibles

De conformidad con el artículo 26 de la LOPDP, se podrán tratar datos personales sensibles únicamente cuando concurra alguna de las siguientes circunstancias: a) El titular haya dado su consentimiento explícito para el tratamiento de sus datos personales, especificándose claramente sus fines.; b) El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del titular en el ámbito del Derecho laboral y de la seguridad y protección social; c) El tratamiento es necesario para proteger intereses vitales del titular o de otra persona natural, en el supuesto de que el titular no esté capacitado, física o jurídicamente, para dar su consentimiento; d) El tratamiento se refiere a datos personales que el titular ha hecho manifiestamente públicos; e) El tratamiento se realiza por orden de autoridad judicial. f) El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular; g) Cuando el tratamiento de los datos de salud se sujete a las disposiciones contenidas en la LOPDP.

6.6.Derechos de los titulares de los datos

Las personas obligadas cumplir estas políticas deben respetar y garantizar los siguientes derechos de los titulares de los datos previstos en el capítulo III de la LOPDP. A continuación, se enuncian dichos derechos y la norma respectiva en el cual se encuentra el alcance y excepciones de estos:

- Derecho a la información (artículo 12 de la LOPDP)
- Derecho de acceso (artículo 13 de la LOPDP)
- Derecho de rectificación y actualización (artículos 14 y 18 de la LOPDP)

- Derecho de eliminación (artículos 15 y 18 de la LOPDP)
- Derecho de oposición (artículos 16 y 18 de la LOPDP)
- Derecho a la portabilidad (artículos 17 y 18 de la LOPDP)
- Derecho a la suspensión del tratamiento (artículo 19 de la LOPDP)
- Derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas (artículo 20 de la LOPDP)
- Derecho de niñas, niños y adolescentes a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas (artículo 21 de la LOPDP)
- Derecho de consulta (artículo 22 de la LOPDP)
- Derecho a la educación digital (artículo 23 de la LOPDP)

6.7. Información a los titulares de los datos personales

En virtud del artículo 12 de la LOPDP, se informa lo siguiente a los titulares de los datos personales:

Fines del tratamiento: UANATACA ECUADOR S.A. recolectará, usará y tratará los datos personales de manera leal y lícita para cumplir las actividades propias de su objeto social en especial las siguientes:

6.7.1 Finalidad del tratamiento de los datos de los clientes

- Validar la identidad de la persona que pide la firma electrónica
- Emitir la firma electrónica
- Asistir para poder adquirir la firma electrónica
- Realizar facturación electrónica y validación de pagos
- Recopilar información técnica en caso de problemas tecnológicos con la firma electrónica

6.7.2 Finalidad del tratamiento de los datos de los trabajadores

Los datos que se recolectan o almacenen sobre los empleados mediante el diligenciamiento de formatos, redes sociales digitales, contratos, vía telefónica, correo electrónico o con la entrega de documentos (hojas de vida, anexos) serán tratados para todo lo relacionado con cuestiones laborales de orden legal o contractual según el caso. En particular, para los siguientes fines:

- Ingresar información en el SISTEMA SUT del Ministerio de Trabajo
- Ingresar la información para afiliación y pago de la seguridad social
- Realizar pago de remuneraciones
- Elaborar contratos de trabajo
- Realizar pago de utilidades
- Gestionar la atención de salud y seguridad ocupacional

6.7.3 Finalidad del tratamiento de los proveedores

- Elaborar contratos

- Ejecución de contratos
- Para temas de facturación
- Realizar el pago por la prestación del servicio o entrega del producto.

6.7.4 Finalidad del tratamiento de los socios

El tratamiento de los datos de los accionistas tendrá como finalidad cumplir los deberes legales pertinentes como, entre otros, llevar los libros y papeles sociales.

De igual forma, la información se utilizará para efectuar todas las actividades relacionadas con los derechos económicos y políticos administrativos de los socios o accionistas. Adicionalmente, sus datos se emplearán para mantener comunicación con los mismos y elaborar las actas de junta.

UANATACA ECUADOR S.A. también podrá tratar los datos personales para los siguientes fines:

- Implementar estrategias de CRM (customer relationship management), que comprende, entre otras, (i) un modelo de gestión de toda la organización, basada en la orientación al cliente y marketing relacional; (ii) Crear bases de datos o sistemas informáticos de apoyo a la gestión de las relaciones con los clientes, a la venta y al marketing.
- Realizar invitaciones a eventos, mejorar productos y servicios u ofertar nuevos productos, y todas aquellas actividades asociadas a la relación comercial o vínculo existente con UANATACA ECUADOR S.A., o aquel que llegare a tener.
- Gestionar trámites (solicitudes, quejas, reclamos), efectuar encuestas de satisfacción respecto de los bienes y servicios de UANATACA ECUADOR S.A. o empresas vinculadas, como las que forman parte de UANATACA ECUADOR S.A. y los aliados comerciales de UANATACA ECUADOR S.A.;
- Suministrar información de contacto y documentos pertinentes a la fuerza comercial y/o red de distribución, telemarketing, y terceros afines al servicio de certificación electrónica, seguridad de la información o servicio tecnológico con los cuales UANATACA ECUADOR S.A. posea un vínculo contractual; para información específica, puede consultar en atencionlodp@uanataca.ec.

Los datos que se recolecten o almacenen sobre los empleados de UANATACA ECUADOR S.A. mediante el diligenciamiento de formatos, vía telefónica, o con la entrega de documentos (hojas de vida, anexos) serán tratados para todo lo relacionado con cuestiones laborales de orden legal o contractual. En virtud de lo anterior, UANATACA ECUADOR S.A. utilizará los datos personales para los siguientes fines: (1) Dar cumplimiento a las leyes como, entre otras, de derecho laboral, seguridad social, pensiones, riesgos profesionales, Sistema Integral de Seguridad Social e impuestos; (2) Cumplir las instrucciones de las autoridades judiciales y administrativas competentes; (3) Implementar las políticas y estrategias laborales y organizacionales de la casa matriz.

Respecto de los datos (i) recolectados directamente en los puntos de seguridad, (ii) tomados de los documentos que suministran las personas al personal de seguridad y (iii) obtenidos de las videograbaciones que se realizan dentro o fuera de las instalaciones de UANATACA ECUADOR S.A., éstos se utilizarán para fines de seguridad de las personas, los bienes e instalaciones de UANATACA ECUADOR S.A. y podrán ser utilizados como prueba en cualquier tipo de proceso o investigación.

6.8. Bases legitimadoras aplicables al tratamiento

El tratamiento legítimo de los datos personales se realizará con base en la condición de licitud que corresponda a cada actividad de tratamiento registrada en el RAT vigente. Según la finalidad, categoría de datos, tipo de titular y contexto del tratamiento, la base legitimadora podrá ser una o varias de las previstas en la LOPDP, incluyendo consentimiento, obligación legal, orden judicial, ejecución contractual o precontractual, interés legítimo documentado u otras aplicables. En suma, dependiendo del caso particular para los cuales se trata el dato, el fundamento de legitimación o licitud del tratamiento de los datos podrá ser cualquiera de los siguientes: 1) El consentimiento del titular del dato; 2) Tratamiento de datos necesario para cumplir una obligación legal; 3) Tratamiento realizado para cumplir una orden judicial; 4) Tratamiento sustentado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, derivados de una competencia atribuida por una norma con rango de ley, sujeto al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de la LOPDP y a los criterios de legalidad, proporcionalidad y necesidad; 5) Para la ejecución de medidas precontractuales a petición del titular o para el cumplimiento de obligaciones contractuales perseguidas por el responsable del tratamiento de datos personales, encargado del tratamiento de datos personales o por un tercero legalmente habilitado; 6) Para proteger intereses vitales, del interesado o de otra persona natural, como su vida, salud o integridad; 7) Para tratamiento de datos personales que consten en bases de datos de acceso público; u, 8) Para satisfacer un interés legítimo del responsable de tratamiento o de tercero, siempre que no prevalezca el interés o derechos fundamentales de los titulares al amparo de lo dispuesto en esta norma.

6.9. Categorías de datos personales y titulares

Los datos personales serán tratados de manera manual y automatizada según el caso.

6.9.1 Clientes y usuarios

Datos identificativos: Nombre y apellidos, número de cédula de identidad o número de pasaporte, nacionalidad, fecha de nacimiento, lugar, sexo, estado civil, código dactilar, nombre de los padres.

Datos de identificación fiscal: Registro Único de Contribuyentes

Datos de contacto: dirección, teléfonos y correo electrónico.

Datos de imagen y biométricos, cuando aplique: fotografía de rostro, video de rostro, reconocimiento facial u otros datos necesarios para validación de identidad.

Datos económicos crediticios: información bancaria, crediticia y transaccional de pago.

Datos web: Dirección IP, datos del navegador y datos de trazabilidad.

6.9.2 Proveedores

Datos identificativos: Nombre y apellidos, cédula de identidad o registro único de contribuyentes, dirección, representante legal, correo electrónico, teléfono.

Datos económicos crediticios: información bancaria, crediticia y transaccional de pago.

6.9.3 Trabajadores

Datos identificativos: Nombre y apellidos, cédula de identidad, dirección, correo electrónico, teléfono nacionalidad, fecha de nacimiento, lugar, sexo, estado civil, código dactilar, nombre de los padres.

Datos de imagen y biométricos: fotografía de rostro, reconocimiento facial, huellas digitales.

Datos económicos crediticios: información bancaria y transaccional de pago.

Datos de Salud: expedientes médicos ocupacionales, exámenes médicos y de laboratorio ocupacionales, historia clínica.

Datos situación personal y familiar: datos de estado civil, cargas familiares, discapacidad, datos de personas con discapacidad a su cargo (sustituto), datos de cargas familiares y dependientes, incluyendo, cuando aplique, nombres y apellidos, número de identificación o documento equivalente, fecha de nacimiento o edad, parentesco, condición de dependencia, discapacidad, calidad de sustituto u otra información estrictamente necesaria para cumplir obligaciones laborales, de seguridad social, beneficios legales, tributarios o requerimientos de autoridad competente.

Datos situación profesional: Hojas de vida profesional, historia laboral y documentación académica.

6.10. Tiempo de conservación

Los datos personales serán conservados únicamente durante el tiempo necesario para cumplir con las finalidades para las cuales fueron recopilados y tratados. Cuando la normativa aplicable establezca un período específico de conservación, los datos se mantendrán durante dicho plazo.

Una vez cumplida la finalidad del tratamiento, los datos podrán conservarse durante los plazos de prescripción aplicables cuando ello resulte necesario para la formulación, ejercicio o defensa de reclamaciones, así como para atender eventuales responsabilidades legales, administrativas o contractuales. Transcurridos dichos plazos, los datos serán eliminados, anonimizados o sometidos a los mecanismos de supresión que correspondan, de conformidad con la normativa aplicable.

6.11. Existencia de una base de datos en la que constan sus datos personales

Según el caso, UANATACA deposita la información en diferentes bases de datos de la empresa.

6.12. Origen de los datos personales cuando no se hayan obtenido directamente del titular

Algunos datos personales son recolectados de fuentes de acceso público o bases de datos de naturaleza pública o de entidades estatales.

6.13. Otras finalidades y tratamientos ulteriores

Los datos no serán utilizados para fines diferentes a los recolectados o autorizados por la ley. Los datos personales no serán utilizados para finalidades distintas a las informadas al titular o autorizadas por la normativa aplicable. Cuando, para la prestación del servicio, sea necesario comunicar, transferir o permitir el tratamiento de datos por terceros, UANATACA documentará la finalidad, categorías de datos, destinatario o encargado, país u organización, base legitimadora, mecanismo jurídico y garantías aplicables, conforme al RAT vigente.

6.14. Identidad y datos de contacto del responsable del tratamiento de datos personales

Nombre del responsable: UANATACA ECUADOR S.A.

Dirección del domicilio legal: Av. 12 de octubre N24-739 y Av. Colón, edificio Torre Boreal, oficina 905.

Número de teléfono: +593968720200

Dirección de correo electrónico: atenciónlodp@uanataca.ec

6.15. Las transferencias o comunicaciones, nacionales o internacionales, de datos personales

Las transferencias o comunicaciones nacionales o internacionales de datos personales se realizarán únicamente cuando exista una base legitimadora aplicable, una finalidad determinada y garantías adecuadas conforme a la normativa vigente. UANATACA documentará, según corresponda, el destinatario, país u organización de destino, categorías de datos, finalidad, mecanismo jurídico aplicable y medidas de seguridad.

El tratamiento realizado por encargados o subencargados que actúen por cuenta e instrucciones documentadas de UANATACA no será considerado transferencia o comunicación de datos personales, sin perjuicio de las obligaciones contractuales, de seguridad, confidencialidad, trazabilidad, retorno, eliminación o anonimización que correspondan.

En caso de transferencias internacionales hacia jurisdicciones que no cuenten con un nivel adecuado de protección, UANATACA aplicará los mecanismos jurídicos y garantías exigibles conforme a la normativa aplicable

6.16.Encargados, subencargados y destinatarios

UANATACA ECUADOR S.A. podrá contratar encargados del tratamiento para la prestación de servicios que impliquen tratamiento de datos personales por cuenta e instrucciones de UANATACA. Dichos encargados deberán tratar los datos únicamente para las finalidades autorizadas, mantener confidencialidad, aplicar medidas de seguridad proporcionales al riesgo, asistir en la atención de derechos de los titulares, notificar incidentes de seguridad cuando corresponda y retornar, eliminar o anonimizar los datos al finalizar la relación contractual.

Cuando un encargado requiera apoyarse en subencargados, deberá contar con autorización contractual o documentada, según corresponda. Los destinatarios que reciban datos personales para sus propios fines serán responsables del tratamiento que realicen sobre dichos datos y deberán cumplir la normativa aplicable.

6.17.Consecuencias para el titular de los datos personales de su entrega o negativa a ello

El no suministro de los datos personales requeridos o la entrega parcial de los mismos nos impedirá prestar un servicio de calidad o el servicio de validación al titular del dato.

6.18.Efecto de suministrar datos personales erróneos o inexactos

El suministro de datos erróneo o inexactos nos impedirá prestar un servicio adecuado al titular del dato y las decisiones que se adopten con fundamento dicha información pueden ser erróneas e inexactas debido a las deficiencias en la calidad de la información suministrada.

6.19.La posibilidad de revocar el consentimiento

El consentimiento puede ser revocado en los casos permitidos en la LOPDP o sus normas reglamentarias.

6.20.Mecanismos para ejercer los derechos

El titular puede utilizar los siguientes medios para hacer efectivos los derechos de acceso, eliminación, rectificación y actualización, oposición, anulación, limitación del tratamiento y a no ser objeto de una decisión basada únicamente en valoraciones automatizadas

Realizar la solicitud mediante correo electrónico a la siguiente dirección: atenciónlodp@uanataca.ec

Utilizar los canales previstos en nuestra página web www.uanataca.ec

6.21. Medios para hacer efectivo su derecho a la portabilidad

Estas son las alternativas para que el titular puede solicitar el derecho de portabilidad:

Realizar la solicitud mediante correo electrónico a la siguiente dirección: atenciónlodp@uanataca.ec

Utilizar los canales previstos en nuestra página web www.uanataca.ec

6.22. Medios para presentar reclamos

El titular puede utilizar los siguientes medios para presentar reclamos:
Realizar la solicitud mediante correo electrónico a la siguiente dirección: atenciónlodp@uanataca.ec.

Utilizar los canales previstos en nuestra página web www.uanataca.ec

Igualmente, podrá hacer lo mismo ante la Autoridad de Protección de Datos Personales, recurriendo a los canales dispuestos por esa entidad para dicho efecto.

6.23. Valoraciones y decisiones automatizadas, incluida la elaboración de perfiles

Nuestra empresa podrá utilizar mecanismos automatizados de verificación biométrica o validación de identidad, cuando aplique. La compañía no elabora perfiles sobre los titulares de los datos.

6.24. Derechos de los titulares de los datos

6.24.1 Derecho de acceso (artículo 13 de la LOPDP):

El titular tiene derecho a conocer y a obtener, gratuitamente acceso a todos sus datos personales y a la información detallada en el artículo 12 de la LOPDP sin necesidad de presentar justificación alguna. La respuesta a la solicitud se emitirá a más tardar dentro del plazo de quince (15) días siguientes a la fecha de la solicitud.

6.24.2 Derecho de rectificación y actualización (artículos 14 y 18 de la LOPDP):

El titular tiene el derecho a obtener la rectificación y actualización de sus datos personales inexactos o incompletos. Para tal efecto, el titular deberá presentar los justificativos del caso, cuando sea pertinente. La solicitud se atenderá dentro de los quince (15) días siguientes a la fecha de la solicitud.

Estos derechos no proceden en los casos señalados en el artículo 18 de la LOPDP.

6.24.3 Derecho de eliminación (artículos 15 y 18 de la LOPDP):

El titular del dato podrá solicitar la supresión de sus datos, la cual es procedente cuando: 1) El tratamiento no cumpla con los principios establecidos en la LOPDP; 2) El tratamiento no sea necesario o pertinente para el cumplimiento de la finalidad; 3) Los datos personales hayan cumplido con la finalidad para la cual fueron recogidos o tratados; 4) Haya vencido el plazo de conservación de los datos personales; 5) El tratamiento afecte derechos fundamentales o libertades individuales; 6) Revoque el consentimiento prestado o señale no haberlo otorgado para uno o varios fines específicos, ¡sin necesidad de que medie justificación alguna; o, 7) Exista obligación legal.

La eliminación será gratuita y se efectuará en el plazo de quince (15) días de recibida la solicitud por parte del titular.

Este derecho no procede en los casos señalados en el artículo 18 de la LOPDP.

6.24.4 Derecho de oposición (artículos 16 y 18 de la LOPDP):

El titular tiene el derecho a oponerse o negarse al tratamiento de sus datos personales, en los siguientes casos: 1) No se afecten derechos y libertades fundamentales de terceros, la ley se lo permita y no se trate de información pública, de interés público o cuyo tratamiento está ordenado por la ley; 2) El tratamiento de datos personales tenga por objeto la mercadotecnia directa; el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles; en cuyo caso los datos personales dejarán de ser tratados para dichos fines; 3) Cuando no sea necesario su consentimiento para el tratamiento como consecuencia de la concurrencia de un interés legítimo, previsto en el artículo 7 de la LOPDP, y se justifique en una situación concreta personal del titular, siempre que una ley no disponga lo contrario.

La solicitud será atendida dentro de los 15 días a la fecha de la misma. De ser procedente, se dejará de tratar los datos personales, salvo que se acredite motivos legítimos e imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del titular, o para la formulación, el ejercicio o la defensa de reclamaciones.

Este derecho no procede en los casos señalados en el artículo 18 de la LOPDP.

6.24.5 Derecho a la portabilidad (artículos 17 y 18 de la LOPDP):

El titular tiene el derecho a recibir sus datos personales en un formato compatible, actualizado, estructurado, común, interoperable y de lectura mecánica, preservando sus características o a transmitirlos a otros responsables en los términos que establezca la Autoridad de Protección de Datos Personales.

El titular podrá solicitar que se realice la transferencia o comunicación de sus datos personales a otro responsable del tratamiento en cuanto fuera técnicamente posible y sin que el responsable pueda aducir impedimento de cualquier orden con el fin de garantizar el acceso, la transmisión o reutilización de datos por parte

del titular o de otro responsable del tratamiento. Luego de completada la transferencia de datos, el responsable que lo haga procederá a su eliminación, salvo que el titular disponga su conservación o mandato legal. El responsable que ha recibido la información asumirá las responsabilidades contempladas en la LOPDP.

Para que proceda el derecho a la portabilidad de datos es necesario que se produzca al menos una de las siguientes condiciones: 1) Que el titular haya otorgado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. La transferencia o comunicación se hará entre responsables del tratamiento de datos personales cuando la operación sea técnicamente posible, caso contrario los datos deberán ser transmitidos directamente al titular; 2) Que el tratamiento se efectúe por medios automatizados; 3) Que se trate de un volumen relevante de datos personales, según los parámetros definidos en el reglamento de la LOPDP; o, 4) Que el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos del responsable o encargado del tratamiento de datos personales, o del titular en el ámbito del derecho laboral y seguridad social

No procederá este derecho cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable del tratamiento de datos personales con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles. Tampoco procede este derecho en los casos señalados en el artículo 18 de la LOPDP.

6.24.6 Derecho a la suspensión del tratamiento (artículo 19 de la LOPDP):

El titular tendrá derecho a obtener la suspensión del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes: 1) Cuando el titular impugne la exactitud de los datos personales, mientras el responsable de tratamiento verifica la exactitud de estos; 2) El tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso; 3) El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones; y 4) Cuando el interesado se haya opuesto al tratamiento en virtud del artículo 31 de la presente LOPDP; mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

Cuando el titular impugne la exactitud de los datos personales, mientras el responsable de tratamiento verifica la exactitud de los mismos, deberá colocarse en la base de datos, en donde conste la información impugnada, que ésta ha sido objeto de inconformidad por parte del titular.

Se podrá tratar los datos personales, que han sido objeto del ejercicio del derecho de suspensión cuando sean necesarios para la formulación, el ejercicio o la defensa de reclamaciones; con el objeto de proteger los derechos de otra persona natural o jurídica o por razones de interés público importante.

6.24.7 Derecho a no ser objeto de una decisión basada única o

parcialmente en valoraciones automatizadas (artículo 20 de la LOPDP):

El titular tiene derecho a no ser sometido a una decisión basada única o parcialmente en valoraciones que sean producto de procesos automatizados, incluida la elaboración de perfiles, que produzcan efectos jurídicos en el o que atenten contra sus derechos y libertades fundamentales, para lo cual podrá: a) Solicitar al responsable del tratamiento una explicación motivada sobre la decisión tomada por el responsable o encargado del tratamiento de datos personales; b) Presentar observaciones; c) Solicitar los criterios de valoración sobre el programa automatizado; o, d) Solicitar al responsable información sobre los tipos de datos utilizados y la fuente de la cual han sido obtenidos los mismos; y e) Impugnar la decisión ante el responsable o encargado del tratamiento

No se aplicará este derecho cuando: 1) La decisión es necesaria para la celebración o ejecución de un contrato entre el titular y el responsable o encargado del tratamiento de datos personales; 2). Está autorizada por la normativa aplicable, orden judicial, resolución o mandato motivado de autoridad técnica competente, para lo cual se deberá establecer medidas adecuadas para salvaguardar los derechos fundamentales y libertades del titular; o, 3) Se base en el consentimiento explícito del titular; 4) La decisión no conlleve impactos graves o riesgos verificables para el titular.

6.24.8 Derecho de niñas, niños y adolescentes (artículo 21 de la LOPDP):

En adición a lo señalado en el título no se podrán tratar datos sensibles o datos de niñas, niños y adolescentes a menos que se cuente con la autorización expresa del titular o de su representante legal; o, cuando, dicho tratamiento esté destinado a salvaguardar un interés público esencial, el cual se evalúe en atención a los estándares internacionales de derechos humanos, y como mínimo satisfaga los criterios de legalidad, proporcionalidad y necesidad, y además incluya salvaguardas específicas para proteger los derechos fundamentales de los interesados.

Los adolescentes, en ejercicio progresivo de sus derechos, a partir de los 15 años, podrán otorgar, en calidad de titulares, su consentimiento explícito para el tratamiento de sus datos personales, siempre que se les especifique con claridad sus fines.

Los adolescentes mayores de doce (12) años y menores de quince (15) años, así como las niñas y niños, para el ejercicio de sus derechos necesitarán de su representante legal. Los adolescentes mayores de quince (15) años y menores de dieciocho (18) años, podrán ejercitarlos de forma directa ante la Autoridad de Protección de Datos Personales o ante el responsable de la base de datos personales del tratamiento.

6.24.9 Derecho de consulta (artículo 22 de la LOPDP):

Las personas tienen derecho a la consulta pública y gratuita ante el Registro Nacional de Protección de Datos Personales, de conformidad con la LOPDP.

6.24.10 Derecho a la educación digital (artículo 23 de la LOPDP):

Las personas tienen derecho al acceso y disponibilidad del conocimiento, aprendizaje, preparación, estudio, formación; capacitación, enseñanza e instrucción relacionados con el uso y manejo adecuado, sano, constructivo, seguro y responsable de las tecnologías de la información y comunicación, en estricto apego a la dignidad e integridad humana, los derechos fundamentales y libertades individuales con especial énfasis en la intimidad, la vida privada, autodeterminación informativa, identidad y reputación en línea, ciudadanía digital y el derecho a la protección de datos personales, así como promover una cultura sensibilizada en el derecho de protección de datos personales.

6.25. Delegado de protección de datos personales

La compañía UANATACA ECUADOR S.A. ha designado un Delegado de Protección de Datos Personales conforme a la normativa aplicable.

El delegado cumplirá las funciones señaladas en el artículo 49 de la LOPDP y para el cumplimiento de sus funciones se dará cumplimiento a lo señalado en el artículo 50 de la precitada ley.

Para dicho efecto, se ponen a disposición del titular los siguientes medios de contacto al delegado de protección de datos personales:

Correo electrónico: atenciónlodp@uanataca.ec

Número de teléfono: +593968720200

Dirección: Av. 12 de octubre N24-739 y Av. Colón, edificio Torre Boreal, Piso 9, oficina 905.

6.26. Requerimiento directo del titular del dato de carácter personal al responsable del tratamiento

De conformidad con el artículo 62 de la LOPDP, el titular podrá en cualquier momento, de forma gratuita, presentar requerimientos, peticiones, quejas o reclamaciones directamente al responsable del tratamiento, relacionadas con el ejercicio de sus derechos, la aplicación de principios y el cumplimiento de obligaciones por parte del responsable del tratamiento, siempre que tengan relación con él titular y se cumpla lo dispuesto en el artículo 13 del RGLOPDP.

Para dicho efecto, se ponen a disposición del titular los siguientes medios:

Realizar la solicitud cumpliendo lo estipulado en el artículo 13 del RGLOPDP mediante correo electrónico a la siguiente dirección: atenciónlodp@uanataca.ec

Utilizar los canales previstos en nuestra página web www.uanataca.ec

El requerimiento se responderá hasta dentro el plazo de (15) días siguientes a la solicitud.

En el caso de que no se conteste el requerimiento, o éste fuere negado, el titular podrá presentar el correspondiente reclamo administrativo ante la Autoridad de Protección de Datos Personales.

6.27. Seguridad en el tratamiento de datos personales

Proteger la información es una condición crucial del tratamiento de datos personales.

La seguridad es un proceso dinámico en constante evolución y prueba. Garantizamos un nivel de seguridad apropiado en las diferentes etapas del tratamiento de datos personales en donde las medidas de seguridad son objeto de evaluación y revisión.

Dichas medidas están enfocadas para mitigar los siguientes riesgos: acceso no autorizado a los datos personales, pérdida, destrucción (accidental o no autorizada), contaminación (por virus informático) uso fraudulento, consulta, copia, modificación, adulteración, revelación, comunicación, o difusión no autorizados.

Para establecer las medidas se tienen en cuenta, entre otras, las técnicas de seguridad existentes en general y para sectores específicos, los riesgos que presente el tratamiento y la naturaleza de los datos que deban protegerse, la probabilidad y severidad del daño obtenido, la sensibilidad de la información y el contexto en el que es realizado el tratamiento y las eventuales consecuencias negativas para los titulares de los datos.

Varios factores son cruciales para garantizar la seguridad de la información. Ninguno es suficiente por sí sólo, razón por la cual es necesario que todos confluyan para otorgar seguridad a la información evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Estos pilares sintetizan los elementos fundamentales de la seguridad en nuestra organización:



- **Enfoque preventivo de incidentes de seguridad:** Todos los esfuerzos tendrán como meta evitar que situaciones que comprometan la seguridad de la información. En caso de presentarse incidentes de seguridad se dará respuesta a los mismos y a partir de las vulnerabilidades detectadas se efectuarán mejoras en la seguridad de la información.

En caso de una vulneración de seguridad que afecte datos personales, UANATACA activará el procedimiento interno de gestión de incidentes del SGSI, evaluará la naturaleza del incidente, categorías de datos comprometidos, titulares afectados, posibles consecuencias y medidas de contención, mitigación y recuperación. Cuando legalmente corresponda, UANATACA notificará a la SPDP, a ARCOTEL y/o a los titulares afectados, conforme a los plazos, condiciones y canales previstos en la normativa.

- **Medidas humanas:** Se trabajará para generar una cultura de seguridad de la información mediante capacitación y concientización del equipo humano de nuestra empresa con miras a que conozcan la importancia de mantener la información segura y su responsabilidad personal para que en nuestra organización no ocurran incidentes de seguridad.
- **Pautas técnicas y físicas:** Se utilizarán equipos, muebles, software y procesos razonables y acordes para garantizar la seguridad de la información.

- **Oficial de seguridad y medidas administrativas:** Se asignará a una persona o dependencia la responsabilidad de velar por garantizar la seguridad de la información.
- **Herramientas contractuales:** En los contratos se incluirá cláusulas exigiendo el respeto de las medidas de seguridad, la confidencialidad y uso lícito de la información.
- **Revisión periódica:** Todas las medidas de seguridad serán objeto de evaluación anual con miras a establecer el nivel de utilidad de estas y, en caso de ser necesario, implementar estrategias adicionales para mejorar el nivel de seguridad de la información.

UANATACA protegerá los datos personales mediante medidas técnicas, organizativas, jurídicas y administrativas proporcionales al riesgo, naturaleza de los datos, finalidad del tratamiento y contexto operativo. Dichas medidas podrán incluir, según aplique, control de acceso, autenticación segura, gestión de privilegios, segregación de funciones, trazabilidad, registros de actividad, protección contra software malicioso, respaldo, continuidad, cifrado, eliminación segura, gestión de vulnerabilidades, gestión de proveedores, capacitación y verificación periódica de controles.

El detalle técnico, responsables, periodicidad, evidencias y estado de implementación de los controles se mantendrá en los documentos internos del SGSI, matriz de riesgos, Declaración de Aplicabilidad, procedimientos de seguridad y registros de auditoría, evitando exponer configuraciones o información operativa sensible en esta política pública

6.28.Servicios en la nube y responsabilidad compartida

Cuando UANATACA utilice servicios en la nube para el tratamiento, almacenamiento, respaldo, transmisión o soporte de datos personales, se aplicará un modelo de responsabilidad compartida entre UANATACA y el proveedor cloud, conforme al rol que cada parte desempeñe. UANATACA validará, según aplique, las responsabilidades contractuales, ubicación o posibles ubicaciones de tratamiento, segregación de información, control de accesos, registros, continuidad, respaldo, gestión de cambios, eliminación segura y salida del servicio.

Los controles específicos de seguridad cloud se documentarán en la matriz de riesgos, evaluación de proveedores, contratos, acuerdos de nivel de servicio, Declaración de Aplicabilidad y demás documentos internos del SGSI.

6.29.Protección de datos personales en servicios cloud

Cuando UANATACA actúe como encargado del tratamiento o utilice proveedores cloud que traten datos personales por cuenta de UANATACA o de sus clientes,

se exigirán, según aplique, instrucciones documentadas, deber de confidencialidad, medidas de seguridad, información sobre subencargados, países o posibles países de tratamiento, asistencia para atención de derechos, notificación de incidentes, trazabilidad, retorno, eliminación o anonimización de datos personales al finalizar la relación contractual.

La aplicación de controles asociados a ISO/IEC 27018 se realizará únicamente cuando corresponda al tratamiento de información personal identificable en servicios cloud que actúen como procesadores o encargados, sin extender su aplicación a tratamientos donde no resulte pertinente.

6.30.Requisitos regulatorios aplicables a servicios de certificación electrónica

En los tratamientos asociados a la emisión, gestión, suspensión, revocación, validación, sellado de tiempo, conservación de evidencias y soporte de certificados de firma electrónica, UANATACA aplicará las obligaciones legales, regulatorias, contractuales y técnicas que correspondan a su calidad de entidad vinculada o regulada, conforme a la normativa aplicable, la Declaración de Prácticas de Certificación, políticas internas, contratos y requerimientos de ARCOTEL.

UANATACA conservará las evidencias necesarias para demostrar la trazabilidad, integridad, autenticidad, disponibilidad, gestión de revocación o suspensión, atención de requerimientos de autoridad y cumplimiento de los controles aplicables, sin publicar en esta política información técnica, operativa o de seguridad que pueda comprometer la prestación del servicio.

Adicionalmente, contamos con una política de seguridad de información y datos personales de obligatorio cumplimiento.

6.31.Videovigilancia

UANATACA ECUADOR S.A. podrá utilizar sistemas de videovigilancia en sus instalaciones, oficinas y áreas de acceso, con la finalidad de proteger la seguridad de las personas, bienes, instalaciones, activos de información y continuidad operativa.

La existencia de estos sistemas será informada mediante avisos visibles en las zonas correspondientes. Las imágenes captadas serán tratadas únicamente para fines de seguridad, control de accesos, investigación de incidentes y atención de requerimientos de autoridad competente, cuando corresponda.

El acceso a las imágenes estará limitado al personal autorizado y su conservación se realizará durante el tiempo necesario para cumplir la finalidad del tratamiento, salvo que deban conservarse por incidentes, requerimientos legales, regulatorios o defensa de derechos.

6.32.Responsabilidad demostrada y proactiva frente al tratamiento de datos personales.

UANATACA ECUADOR S.A. adoptará las medidas útiles, oportunas y eficientes para demostrar que ha implementado medidas apropiadas y efectivas para cumplir con sus obligaciones legales en todo lo relacionado con el tratamiento de datos personales.

En adición a lo dispuesto en esta política, se aplicarán e implementarán requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas, a fin de garantizar y demostrar que el tratamiento de datos personales se ha realizado conforme a lo previsto en la LOPDP, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales o normativa sobre la materia.

Adicionalmente, UANATACA ECUADOR S.A. podrá valerse de estándares, mejores prácticas, esquemas de auto y correulación, códigos de protección, sistemas de certificación, sellos de protección de datos personales o cualquier otro mecanismo que se determine adecuado a los fines, la naturaleza del dato personal o el riesgo del tratamiento.

6.33.Proceso de verificación y evaluación

UANATACA ECUADOR S.A. realizará auditorías internas o externas con miras a verificar, evaluar o valorar periódicamente la eficiencia, eficacia y efectividad de los requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas implementadas para dar cumplimiento a la LOPDP.

Se evaluarán y revisarán los mecanismos que adopte la empresa para cumplir con el principio de responsabilidad de forma continua y permanente, con el objeto de mejorar su nivel de eficacia en cuanto a la aplicación de la LOPDP.

6.34.Protección de datos personales desde el diseño y por defecto (Privacy by Design and by Default) y estudios de impacto de privacidad (Privacy Impact Assessment - PIA).

Para garantizar el tratamiento lícito de los datos personales y evitar vulneraciones a los derechos de los titulares de esa información se hará uso de la privacidad desde el diseño y por defecto (Privacy by Design and by Default)

El debido tratamiento de datos es un elemento fundamental en nuestra organización. Por eso, desde antes de recolectar información y durante todo el ciclo de vida de esta, adoptarán medidas preventivas de diversa naturaleza (tecnológica, organizacional, humana, ética y procedimental, entre otras) con el objeto de evitar vulneraciones a los derechos de las personas, así como fallas de seguridad o indebidos Tratamientos de Datos Personales.

En el evento que surjan nuevos proyectos o actividades que involucre tratamiento de datos personales se aplicaran desde el inicio de los mismos medidas técnicas,

organizativas y de cualquier otra índole, con miras a garantizar el tratamiento de datos personales conforme a la LOPDP.

Se implementarán medidas técnicas y organizativas adecuadas con miras a que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines del tratamiento, en los términos del reglamento.

Previo al diseño y desarrollo de proyectos o actividades que involucren tratamiento de datos personales, y en la medida en que sea probable que el mismo entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los Titulares, se efectuará una evaluación de impacto en la privacidad (Privacy Impact Assessment - PIA por sus siglas en inglés).

Se realizarán esa evaluación con el fin de poner en funcionamiento un sistema efectivo de manejo de riesgos y controles internos, para garantizar que los datos se tratarán debidamente y conforme con la regulación existente.

Dicha evaluación debería incluir, como mínimo, lo siguiente:

- Una descripción detallada de las operaciones de Tratamiento de datos personales que involucra el proyecto o actividad.
- Una evaluación de los riesgos específicos para los derechos y libertades de los Titulares de los datos personales. Se desarrollará y pondrá en marcha un sistema de administración de riesgos asociados al tratamiento de datos personales que les permita identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos en desarrollo del cumplimiento de las normas de protección de datos personales.
- Las medidas previstas para afrontar los riesgos, incluidas garantías; medidas de seguridad; diseño de software; tecnologías y mecanismos que garanticen la protección de datos personales, teniendo en cuenta los derechos e intereses legítimos de los Titulares de los datos y de otras personas eventualmente afectadas.

Los resultados de este estudio, junto con las medidas para mitigar los riesgos, hacen parte de la aplicación del principio de privacidad desde el diseño y por defecto.

6.35. Cookies

6.35.1 Tratamiento de Cookies

Las cookies son pequeños fragmentos de texto, que los sitios web que el cliente visita, envían al navegador del cliente. Permiten que los sitios web recuerden información sobre su visita, lo que puede hacer que sea más fácil volver a visitar los sitios y hacer que estos le resulten más útiles. Las tecnologías similares, como

los identificadores únicos que se usan para identificar una aplicación o dispositivo, las etiquetas de píxel y el almacenamiento local, pueden realizar la misma función. UANATACA podrá utilizar cookies técnicas o necesarias para permitir el funcionamiento del sitio web y, cuando corresponda, cookies analíticas, de medición o publicitarias, únicamente conforme a las preferencias gestionadas por el usuario y la normativa aplicable.

Las cookies no necesarias no serán obligatorias para la prestación del servicio principal y el usuario podrá aceptarlas, rechazarlas o configurarlas. La información sobre herramientas utilizadas, finalidad, proveedor, plazo de conservación y mecanismo de gestión de preferencias estará disponible en el banner o panel de configuración de cookies del sitio web.

UANATACA no utilizará herramientas de rastreo de comportamiento avanzado, grabación de sesión, movimientos del cursor o clics, salvo que dicha funcionalidad haya sido previamente validada por Legal, TI/Seguridad y Protección de Datos, se informe de forma clara al titular y se cuente con la base legitimadora aplicable.

6.35.2 ¿Quién sirve estas cookies y por qué?

Las cookies que podríamos utilizar o servicios que utilizamos en nuestros sitios:

- Google Analytics

Recoge datos basados en eventos tanto de sitios web como de aplicaciones. Es una herramienta gratuita que permite recopilar datos de sitios web y aplicaciones para generar informes estadísticos. Esto ayuda a comprender el rendimiento de los sitios y aplicaciones, y a mejorar la estrategia digital.

- Píxel de META

Agrega un fragmento de código a un sitio web que permite medir, optimizar y crear públicos para campañas publicitarias.

6.35.3 Tus Opciones:

Tienes derecho a decidir si aceptas o rechazas las cookies que no sean esenciales. El usuario puede configurar sus preferencias de cookies siguiendo las indicaciones a continuación.

En la mayoría de los navegadores web, encontrará una sección de "ayuda" en la barra de herramientas. Consulte esta sección para obtener información sobre cómo recibir una notificación cuando reciba una nueva cookie y cómo desactivarlas. Consulte los enlaces a continuación para obtener instrucciones sobre cómo modificar la configuración de su navegador web en los navegadores más populares:

Internet Explorer: <https://windows.microsoft.com/en-gb/internet-explorer/delete-manage-cookies#ie=ie-11>

Mozilla Firefox: <https://support.mozilla.org/en-US/kb/enable-and-disable-cookies->

website-preferences?esab=a&s=cookies&r=6&as=s

Google Chrome: <https://support.google.com/accounts/answer/61416?hl=en>
Safari de Apple: <https://support.apple.com/guide/safari/manage-cookies-sfri11471/mac>

Estas opciones son específicas del navegador que utiliza. Si accede a nuestros servicios desde otros dispositivos o navegadores, realice estas acciones desde esos sistemas para garantizar que sus opciones se apliquen a los datos recopilados al utilizarlos.

Tenga en cuenta que, si rechaza las cookies o las desactiva, es posible que no pueda acceder a ciertas partes del Sitio o del Servicio y que no pueda beneficiarse de la funcionalidad completa del Sitio o del Servicio.

En muchos casos, otras tecnologías de seguimiento (como las etiquetas de píxeles) dependen de las cookies para funcionar correctamente, por lo que pueden volverse ineficaces si rechaza todas las cookies o modifica la configuración de su navegador para notificarle cada vez que se envía una cookie y permitirle aceptar o rechazar las cookies de forma individual.

6.36. Uso de la Aplicación Móvil: Uanataca

El uso de la aplicación móvil de Uanataca (en adelante, la “Aplicación”) es completamente facultativo y no constituye un requisito obligatorio para la utilización de los servicios prestados por Uanataca Ecuador S.A. La Aplicación es desarrollada y gestionada por Uanataca S.A., una entidad constituida conforme a la legislación del Reino de España, siendo el responsable del tratamiento de los datos personales que se recopilen, almacenen o traten a través de dicha plataforma.

En tal virtud, al optar por utilizar la Aplicación, el usuario deberá consultar las condiciones legales donde está su política de protección de datos personales aplicable a dicha herramienta tecnológica, la cual es gestionada y emitida directamente por Uanataca S.A. (España). Dicha política contiene la información detallada sobre las finalidades del tratamiento, los derechos del titular de los datos, y los mecanismos para su ejercicio, entre otros aspectos relevantes. Se recomienda a los usuarios leer detenidamente la política de protección de datos personales de la Aplicación antes de utilizarla, a fin de que puedan tomar una decisión informada sobre su uso.

6.37. Anexo 1. Resumen público de actividades de tratamiento

El presente anexo contiene un resumen público de las principales actividades de tratamiento de datos personales realizadas por UANATACA ECUADOR S.A. El detalle operativo, técnico, contractual y de seguridad se mantiene en el Registro de Actividades de Tratamiento —RAT— vigente, matriz de riesgos, contratos, procedimientos internos y demás documentos del SGSI. Este resumen no incluye información sensible de arquitectura tecnológica, proveedores críticos,

configuraciones de seguridad ni detalles que puedan comprometer la operación o seguridad de la organización.

Actividad de tratamiento	Titulares	Finalidad	Categorías de datos	Base legitimadora	Destinatarios / encargados	Conservación
Emisión y gestión de certificados de firma electrónica	Clientes, solicitantes, representantes legales	Validar identidad, emitir, gestionar, suspender o revocar certificados y prestar soporte asociado	Identificación, contacto, contractuales, técnicos y, cuando aplique, biométricos	Ejecución contractual, obligación legal/regulatoria y consentimiento cuando aplique	Autoridades competentes, proveedores tecnológicos o encargados autorizados	Según normativa aplicable, DPC, contrato y RAT vigente
Atención al cliente y soporte	Clientes, usuarios, prospectos	Gestionar solicitudes, soporte, incidentes, reclamos y consultas	Identificación, contacto, registros de interacción, información técnica necesaria	Ejecución contractual, medidas precontractuales y obligación legal cuando aplique	Proveedores de soporte, herramientas tecnológicas autorizadas y autoridades cuando corresponda	Según RAT vigente y necesidad de atención o defensa
Gestión comercial	Clientes, prospectos, contactos comerciales	Gestionar cotizaciones, comunicaciones comerciales, campañas y relación comercial	Identificación, contacto, información comercial	Interés legítimo, medidas precontractuales y consentimiento cuando aplique	Proveedores tecnológicos y canales comerciales autorizados	Según RAT vigente o hasta oposición/revocatoria cuando aplique
Gestión laboral	Trabajadores, postulantes, ex trabajadores	Administración laboral, contractual, seguridad social, salud ocupacional y cumplimiento legal	Identificación, contacto, laborales, financieros, cargas familiares y salud ocupacional cuando aplique	Ejecución contractual y obligación legal	Autoridades laborales, IESS, bancos y proveedores laborales autorizados	Según normativa laboral, tributaria, seguridad social y RAT vigente
Gestión de proveedores	Proveedores, representantes y contactos	Contratación, ejecución contractual, pagos, facturación y cumplimiento	Identificación, contacto, financieros, tributarios y contractuales	Ejecución contractual y obligación legal	Autoridades, bancos, asesores y proveedores tecnológicos autorizados	Según normativa tributaria, contractual y RAT vigente
Videovigilancia y seguridad física	Visitantes, colaboradores y terceros	Seguridad de personas, bienes e instalaciones	Imagen, fecha, hora, ubicación e información incidental captada por cámaras	Interés legítimo, seguridad y cumplimiento de obligaciones aplicables y órdenes judiciales	Autoridades competentes cuando corresponda	Según política de retención y RAT vigente

7. Validez, revisión y gestión del documento

Este documento es válido hasta **8 de septiembre del 2027**