Quantum Terra GeoTech AI LLC

POLÍTICA INTEGRAL DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

Documento corporativo alineado a estándares internacionales de cumplimiento:

GDPR (Unión Europea) • CPRA (California) • LFPDPPP (México) • ISO/IEC 27001 • NIST-CSF

Versión del Documento: **1.0**
Fecha de Emisión: **14 de octubre de 2025**
Alcance: **Global – Aplicable a Filiales y Operaciones Asociadas**
Clasificación de Información: **Confidencial – Uso Corporativo Controlado**
Unidad Responsable: **Oficina de Privacidad y Cumplimiento de Datos (DPO Office)**
Contacto Oficial de Privacidad: **privacy@quantumterra.ai**
Canal de Respaldo Operativo: **quantum.terra@outlook.com**
Ubicación Oficial del Documento: **https://quantumterra.ai/privacy**

DECLARACIÓN CORPORATIVA

Quantum Terra GeoTech AI LLC mantiene un compromiso permanente con el cumplimiento normativo en materia de protección de datos personales y privacidad, garantizando un tratamiento legítimo, informado y transparente de la información bajo su responsabilidad. Este documento establece los principios, lineamientos, obligaciones y medidas aplicables al tratamiento de datos personales por parte de Quantum Terra, sus unidades de negocio y proveedores tecnológicos autorizados.

Tabla de contenido

0. DECLARACIÓN CORPORATIVA Y ALCANCE

0.1. Introducción

En **Quantum Terra GeoTech AI LLC** (en adelante, **"Quantum Terra"**), reconocemos que la privacidad es un derecho fundamental y que el tratamiento adecuado de los datos personales es un componente esencial de la ética profesional, la confianza digital y la responsabilidad tecnológica. Somos una consultoría especializada en **inteligencia geoespacial, procesamiento satelital, telemetría IoT aplicada, análisis operativo avanzado y ciencia de datos** para sectores estratégicos como logística, energía, infraestructura, construcción, agricultura de precisión, gestión de recursos naturales y defensa corporativa.

La presente **Política Integral de Privacidad** establece las responsabilidades, principios y reglas que rigen el tratamiento de datos personales en Quantum Terra, incluyendo **datos de localización (geoespaciales) vinculados a personas físicas**, información derivada de análisis operativos y datos generados por plataformas tecnológicas utilizadas o desarrolladas por Quantum Terra.

0.2 Compromiso Corporativo

Quantum Terra opera bajo un modelo de privacidad por diseño y por defecto (privacy by design & default) e incorpora controles éticos y normativos desde la arquitectura de datos hasta la entrega de resultados a clientes. Declaramos formalmente que:

- No comercializar datos personales ni permitir usos no autorizados.
- Tratar únicamente datos adecuados, pertinentes y limitados a las finalidades.
- Establecer bases jurídicas válidas para cada tratamiento (p. ej., ejecución contractual conforme a art. 6(1)(b) GDPR, cumplimiento legal art. 6(1)(c), interés legítimo art. 6(1)(f), o consentimiento cuando corresponda).
- Aplicar salvaguardas reforzadas para datos geoespaciales personales, incluyendo separación lógico-funcional entre identidad y ubicación, reducción de precisión geográfica cuando la finalidad lo permita y anonimización cuando proceda.
- Mantener trazabilidad técnica y documental del ciclo de vida del dato (recopilación, uso, copias de seguridad, acceso, transferencia, retención y eliminación).
- Implementar seguridad razonable y proporcional con base en ISO/IEC 27001, ISO/IEC 27002 y guías NIST, sin ofrecer garantía de seguridad absoluta.

0.2 bis Representación Legal y Domicilios Oficiales

Para efectos de esta Política Integral de Privacidad, Quantum Terra GeoTech AI LLC, constituida conforme a las leyes del Estado de Delaware, Estados Unidos de América, actúa como responsable primario del tratamiento de datos personales en el marco de sus operaciones globales.

Domicilio corporativo principal (Estados Unidos):

8 The Green, Ste R, Dover, Delaware 19901, Estados Unidos de América.

Asimismo, para México y Latinoamérica, Quantum Terra cuenta con representación operativa y administrativa a través de:

Talent & Geoskilled, S. de R.L. de C.V.

RFC HPA1905148K9

Domicilio fiscal: Av. Ciudad Universitaria No. 286, Piso 1, Col. Jardines del Pedregal, Alcaldía Álvaro Obregón, C.P. 01900, Ciudad de México.

Esta entidad funge como representante autorizado y enlace regional para atención a titulares, autoridades competentes y cumplimiento normativo local, en apego a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (México) y demás regulaciones aplicables en la región.

Ambos domicilios se reconocen como oficiales para la recepción de notificaciones, solicitudes de derechos ARCO, requerimientos de autoridades y comunicaciones relacionadas con la protección de datos personales.

Véase también Sección 15.5 (Contacto para cumplimiento en privacidad) para los canales de comunicación complementarios.

0.3 Marco Normativo Aplicable

Quantum Terra actúa conforme a los siguientes marcos regulatorios internacionales:

Jurisdicción	Normativa Aplicable
Unión Europea	Reglamento General de Protección de Datos (GDPR) – Reg. (UE) 2016/679
Estados Unidos – California	Ley de Privacidad del Consumidor de California (CCPA) y Enmienda CPRA
México	Ley Federal de Protección de Datos Personales en Posesión de los Particulares (México) y el marco regulatorio digital aplicable en 2025.
Internacional	Principios de Privacidad de la OCDE
Seguridad	Referencias técnicas ISO/IEC 27001, NIST SP 800-53, OWASP

Quantum Terra incorpora adicionalmente buenas prácticas de responsabilidad proactiva (accountability), conforme al Art. 5.2 del GDPR y principios de evaluación de impacto en tratamiento de alto riesgo.

0.4 Alcance de esta Política

Esta política aplica a todo tratamiento de datos realizado por Quantum Terra, incluyendo:

✓ Datos proporcionados directamente por clientes, proveedores o usuarios

✓ Datos derivados de sistemas de inteligencia geoespacial

✓ Datos recolectados mediante plataformas web, portales y aplicaciones tecnológicas

✓ Datos georreferenciados de telemetría

✓ Datos satelitales vinculados a personas físicas

✓ Datos de usuarios corporativos durante contratos de servicio

✓ Datos conservados para obligaciones legales o de auditoría

0.5 Actividades y Servicios Cubiertos

Esta política cubre todas las operaciones y proyectos de Quantum Terra relacionados con:

- Plataformas GIS empresariales y despliegue de mapas inteligentes
- Procesamiento y análisis de imágenes satelitales
- Seguimiento geoespacial y trazabilidad operativa en tiempo real
- Telemetría IoT aplicada a maquinaria, flotas o infraestructura
- Modelado avanzado, analítica de riesgos y simulación espacial
- Automatización espacial, dashboards y geocercas
- Procesamiento de datos geográficos sensibles
- Implementación de sistemas de monitoreo éticos

0.6 Principios Rectores del Tratamiento de Datos

Quantum Terra adopta los siguientes principios reguladores (GDPR Art. 5):

Principio	Descripción
Licitud	Toda operación de datos tiene base jurídica
Transparencia	El titular conoce cómo y por qué se usan sus datos
Minimización	Solo tratamos datos necesarios para el propósito
Limitación de finalidad	No se usan datos para finalidades no autorizadas
Exactitud	Los datos deben mantenerse actualizados
Seguridad	Medidas técnicas para proteger la información
Integridad	Datos protegidos contra acceso indebido
Responsabilidad	Quantum Terra demuestra cumplimiento

0.7 Categorías de Titulares de Datos

Esta política aplica a los datos personales de las siguientes categorías de personas físicas:

- Clientes y usuarios de servicios tecnológicos
- Representantes legales y contactos comerciales de empresas clientes
- Visitantes de plataformas, sitios web y aplicaciones operadas por Quantum Terra
- Participantes en estudios, pruebas piloto o demostraciones tecnológicas
- Empleados y candidatos a empleo (cuando aplique)
- Proveedores y contratistas independientes
- Personas cuya información geoespacial sea tratada como parte de proyectos de monitoreo, trazabilidad, logística, movilidad, seguridad o infraestructura

0.8 Ámbito de Aplicación Territorial

Esta política aplica a operaciones dentro y fuera de los Estados Unidos cuando Quantum Terra:

- Procesa datos personales de personas ubicadas dentro de México, EE.UU. o la Unión Europea
- Ofrece servicios tecnológicos a entidades dentro de estas jurisdicciones
- Recibe, transfiere o procesa datos alojados en infraestructura multinube con alcance internacional
- Ejecuta proyectos con componente geoespacial o telemetría IoT que impliquen tratamiento de datos personales transfronterizos

Las transferencias internacionales se ejecutarán conforme a mecanismos legales como:

- Standard Contractual Clauses (SCC) de la Unión Europea 2021/914
- Data Processing Agreements (DPA)
- Evaluaciones de Transferencia (TIA – Transfer Impact Assessment) cuando aplique

0.9 Herramientas y Tecnologías Alcanzadas por esta Política

Esta política regula el tratamiento de datos realizado a través de:

Categoría	Ejemplos
Plataformas GIS	ESRI, ArcGIS, QGIS, dashboards espaciales
Telemetría IoT	Sensores, GPS vehicular, dispositivos móviles
Datos satelitales	Sentinel, Landsat, imágenes comerciales o basadas en API
Datos derivados	Modelos predictivos, hotspots de actividad, análisis topológicos
Sistemas Cloud	AWS, Azure, Google Cloud o infraestructura híbrida, ESRI Cloud.

APIs y conectores	REST, WebSocket, ETL geoespacial
Automatización geográfica	GeoAI, detección espacial, flujos automáticos

Cuando alguna de estas herramientas procese datos personales vinculados a personas físicas, se aplicarán las medidas de privacidad por defecto establecidas en este documento.

0.10 Declaración de No Venta de Datos

Quantum Terra no vende ni comercializa datos personales de ninguna forma, ni dentro ni fuera de plataformas digitales. Declaramos explícitamente:

- No vendemos bases de datos
- No lucramos con información personal
- No realizamos perfiles ilícitos o discriminatorios
- Solo tratamos datos con base legal válida

Esta política se encuentra alineada con lo dispuesto en:

- GDPR – Considerando 32 y Art. 5
- CCPA/CPRA – Sección 1798.140 (ad)
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares (México) y el marco regulatorio digital aplicable en 2025.

0.11 Carácter vinculante y relación con otros instrumentos

Esta Política es obligatoria para todo el personal de Quantum Terra, directivos, contratistas, proveedores y subencargados con acceso a datos personales o a infraestructura corporativa. Se integra con (i) la Política Interna de Seguridad de la Información, (ii) el Programa de Cumplimiento y (iii) los documentos contractuales aplicables (términos de servicio, DPA, acuerdos de confidencialidad, anexos de seguridad y guías operativas). En caso de conflicto, prevalecerán las disposiciones legales aplicables y los contratos específicos con el cliente, manteniéndose el mayor nivel de protección al titular.

0.12 Aceptación obligatoria del Aviso de Privacidad y mecanismo de control

El uso de plataformas y servicios digitales de Quantum Terra exige la aceptación expresa y obligatoria del Aviso de Privacidad. El mecanismo de aceptación incorporará:

a) Casilla de consentimiento no pre-marcada y visible;
b) Enlace permanente al texto completo del aviso y de esta Política;
c) Registro de la versión del aviso aceptado, sello de tiempo (timestamp), dirección IP y agente de usuario;
d) Procedimiento para revocar el consentimiento cuando el tratamiento se base en dicha causa.

El aviso integral y sus actualizaciones estarán disponibles en la URL corporativa: https://quantumterra.ai/privacy (dirección provisional sujeta a confirmación y versionado).

0.13 Blindaje jurídico y delimitación de responsabilidades

a) Quantum Terra no será responsable por tratamientos realizados directamente por clientes o terceros fuera de sus instrucciones documentadas, ni por la licitud y calidad de los datos suministrados por éstos.
b) Quantum Terra no responde por usos ilícitos o contrarios a contrato que el cliente o usuario final haga de las plataformas o datos.
c) Quantum Terra no garantiza seguridad absoluta; mantiene medidas de seguridad razonables y proporcionadas a los riesgos y al estado del arte, en consonancia con estándares internacionales.
d) El cliente se obliga a proporcionar instrucciones lícitas y suficientes, acreditar sus propias bases jurídicas y cumplir su normativa local como Responsable del Tratamiento cuando corresponda.

0.14 Bases jurídicas y referencia multinorma

Quantum Terra documenta la base jurídica aplicable en cada operación de tratamiento conforme a:

a) GDPR art. 6(1)(b) ejecución de contrato; art. 6(1)(c) cumplimiento legal; art. 6(1)(f) interés legítimo (cuando prevalezca sobre los intereses y derechos del titular); art. 49 para excepciones en transferencias, cuando aplique; art. 25 privacidad por diseño.
b) CPRA (Secciones 1798.100–1798.199) respecto de derechos, limitaciones y avisos al consumidor.
c) LFPDPPP (México) y demás lineamientos aplicables.

La descripción detallada por finalidad y base jurídica se amplía en la Sección 4 y en el Anexo A.

0.15 Relación con transferencias (remisión a Sección 6)

Cualquier transferencia nacional o internacional se regirá por la Sección 6 de este documento y se realizará bajo garantías adecuadas (p. ej., cláusulas contractuales estándar del GDPR, DPA, acuerdos de confidencialidad, y medidas de seguridad). Este Título 0 constituye el fundamento normativo general al que se refiere expresamente el epígrafe 6.0 (Marco normativo aplicable a transferencias).

0.16 Publicación, versionado y trazabilidad

Quantum Terra mantendrá disponible la versión vigente de esta Política y el historial de cambios relevantes. Toda aceptación del Aviso de Privacidad registrará la versión aplicable. Las modificaciones sustanciales serán comunicadas por medios institucionales razonables y, cuando corresponda, mediante notificación dirigida a titulares o clientes responsables.

0.17 Interacción con avisos por capas y avisos específicos

Además de esta Política integral, Quantum Terra podrá desplegar avisos de privacidad por capas (aviso corto en formularios o pantallas de alta), con resumen de finalidades, bases jurídicas y enlaces a la versión completa. En proyectos con especificidades regulatorias, se emitirán avisos o anexos técnicos adicionales acordes con el servicio.

0.18 Canales de contacto y ejercicio de derechos

Para ejercer derechos de acceso, rectificación, supresión/cancelación, oposición, limitación, portabilidad o revocación del consentimiento, el titular podrá comunicarse al correo institucional: **privacy@quantumterra.ai** o a **quantum.terra@outlook.com.** El procedimiento, requisitos y plazos se describen en la Sección 10 y en el Anexo D (procedimiento de derechos).

0.19 Estructura documental y lectura recomendada

Esta Política debe leerse conjuntamente con:

a) Sección 4 (Finalidades y bases jurídicas) y Anexo A (desglose por finalidad);
b) Sección 5 (Tratamiento de datos geoespaciales, con salvaguardas reforzadas);
c) Sección 6 (Transferencias nacionales e internacionales);
d) Sección 7 (Subencargados y proveedores tecnológicos) y Anexo I (enlaces a políticas de privacidad de proveedores autorizados, incluidos AWS y Esri);
e) Sección 9 (Seguridad de la información) y Anexo C (medidas técnicas y organizativas).

0.20 Idioma, interpretación y prevalencia

La versión en español de esta Política será la de referencia corporativa salvo que contractualmente se acuerde la prevalencia de otra lengua. En caso de contradicción entre esta Política y un contrato específico suscrito con un cliente, prevalecerá el instrumento que otorgue mayor protección al titular, sin perjuicio de la sujeción al régimen legal obligatorio correspondiente.

0.21 Vigencia y entrada en vigor

Esta Política entra en vigor a partir de su publicación en el canal corporativo habilitado. La Sección 16 detalla reglas de modificaciones, vigencia y jurisdicción aplicable.

1. IDENTIDAD DEL RESPONSABLE Y DATOS DE CONTACTO

1.1 Identidad legal del responsable del tratamiento

El responsable del tratamiento de datos personales es:

- Quantum Terra GeoTech AI LLC
- Entidad privada constituida conforme a las leyes de los Estados Unidos de América.
- Domicilio corporativo de contacto: [Domicilio pendiente de completar – se reservará espacio para actualización corporativa].
- Correo oficial principal para privacidad: privacy@quantumterra.ai (dirección válida y habilitada).
- Correo oficial secundario para privacidad: quantum.terra@outlook.com
- Sitio institucional: https://quantumterra.ai

Quantum Terra actuará como Responsable del Tratamiento cuando determine directamente las finalidades y medios del tratamiento de los datos personales y como Encargado del Tratamiento cuando procese datos por instrucción documentada de un cliente o responsable principal, en términos del artículo 4.8 del GDPR y secciones aplicables de la CPRA.

1.2 Subsidiarias, filiales y entidades relacionadas

Esta Política aplica también a subsidiarias y unidades operativas vinculadas directamente a Quantum Terra que formen parte del mismo grupo corporativo y que participen en operaciones de tratamiento de datos personales como parte de la provisión de servicios tecnológicos, operativos o contractuales. En caso de existir entidad local distinta que funja como responsable legal según la legislación aplicable, dicha entidad será identificada en el contrato o aviso correspondiente.

1.3 Delegado de Protección de Datos (DPO) y contacto oficial

Quantum Terra realizará designación de un Delegado de Protección de Datos (Data Protection Officer – DPO) cuando sea legalmente exigible o contractualmente requerido conforme al artículo 37 del GDPR, o bien contará con un Oficial Interno de Cumplimiento en Privacidad en otras jurisdicciones donde el nombramiento no sea obligatorio. El canal único institucional habilitado para consultas, ejercicio de derechos y comunicaciones oficiales de privacidad es:

- Correo oficial de cumplimiento de privacidad: **privacy@quantumterra.ai** / **quantum.terra@outlook.com.**
- Asunto sugerido: “Ejercicio de derechos de privacidad” / “Notificación de seguridad”

Todos los asuntos relativos a protección de datos, transferencias internacionales, confidencialidad de información y seguridad deben tramitarse exclusivamente a través de este canal.

1.4 Tratamiento efectuado por cuenta de terceros

En proyectos en los que Quantum Terra actúe como Encargado del Tratamiento, el cliente que emita instrucciones será considerado Responsable del Tratamiento y conservará la obligación de:

a) Determinar la base jurídica aplicable para cada tratamiento.
b) Asegurar el cumplimiento de la normativa aplicable al tratamiento de datos.
c) Brindar avisos de privacidad completos a los titulares.
d) Emitir instrucciones lícitas, documentadas y verificables.
e) Garantizar que los datos personales entregados a Quantum Terra hayan sido recopilados de forma legítima.

Quantum Terra no será responsable por instrucciones ilegales o insuficientes del cliente, ni por la licitud del tratamiento original realizado por el cliente como responsable.

1.5 Identificación de corresponsabilidad

Cuando Quantum Terra participe en proyectos donde la determinación de finalidades sea conjunta con un cliente, socio tecnológico o autoridad pública, podrá configurarse una

situación de corresponsabilidad de tratamiento en términos del artículo 26 del GDPR. En estos casos se formalizará un Acuerdo de Corresponsabilidad en el que se documentarán:

- Roles operativos y responsabilidades jurídicas de cada parte
- Medidas de seguridad aplicables
- Proceso para atención de solicitudes de titulares
- Modelo de notificación de incidentes
- Trazabilidad y uso ético de datos

1.6 Continuidad del cumplimiento jurídico internacional

Quantum Terra mantendrá cumplimiento multinorma aplicable en las jurisdicciones donde opere, incluyendo:

- GDPR (Unión Europea)
- CPRA (California, EE.UU.)
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares (México) y el marco regulatorio digital aplicable en 2025LGPD (Brasil) cuando aplique.
- Normativa comercial y de ciberseguridad estadounidense aplicable a servicios digitales
- Principios OCDE de gobernanza de datos

1.7 Protección reforzada para sectores regulados

En caso de colaboración con sectores regulados (p. ej., energía, transporte, geointeligencia, infraestructura crítica, minería, defensa o contratistas gubernamentales), Quantum Terra adoptará términos contractuales y medidas reforzadas de cumplimiento conforme a marcos regulatorios específicos aplicables, sin perjuicio de los estándares mínimos establecidos en esta Política.

2. DEFINICIONES

El presente documento utiliza terminología especializada en materia de protección de datos, regulación aplicable, ingeniería de datos y tratamiento de información geoespacial. Las siguientes definiciones son obligatorias para la correcta interpretación de esta Política Integral de Privacidad.

2.1 Bases legales del tratamiento (catálogo multinorma)

Quantum Terra documenta la base jurídica aplicable a cada finalidad (ver Sección 4 y Anexo A). Conforme al artículo 6 del GDPR:

2.1.1 Ejecución de contrato – art. 6(1)(b) GDPR

El tratamiento es lícito cuando es necesario para ejecutar un contrato en el que el titular es parte o para medidas precontractuales a petición del titular.

Ejemplos en Quantum Terra: provisión de plataformas GIS contratadas, soporte técnico, administración de cuentas, facturación, integración de APIs y mantenimiento correctivo.

2.1.2 Cumplimiento de obligación legal – art. 6(1)(c) GDPR

Tratamientos necesarios para cumplir normas fiscales, laborales, de seguridad o regulatorias.

Ejemplos: conservación contable, atención de requerimientos de autoridades, controles SOX/antifraude cuando aplique.

2.1.3 Interés legítimo – art. 6(1)(f) GDPR

Tratamientos necesarios para los intereses legítimos de Quantum Terra o de un tercero, siempre que no prevalezcan los derechos y libertades del titular. Requiere test de ponderación documentado y controles de minimización.

Ejemplos:

- Seguridad de plataformas y prevención de fraudes;
- Registro de accesos (logs) y telemetría técnica para resiliencia;
- Mejora de rendimiento de servicios y trazabilidad operativa;
- Monitoreo de disponibilidad de sistemas.

No aplicaría, por regla general: marketing directo sin base adicional en ciertas jurisdicciones.

2.1.4 Consentimiento – art. 6(1)(a) GDPR

Cuando no exista otra base válida, se recaba consentimiento libre, específico, informado e inequívoco (casilla no pre-marcada, registro de versión/timestamp/IP, mecanismo de revocación).

Ejemplos: comunicaciones comerciales no esenciales; tratamientos geoespaciales individualizados si no derivan de contrato u obligación legal.

2.1.5 Protección de intereses vitales – art. 6(1)(d) GDPR

Tratamientos necesarios para proteger intereses vitales del titular u otra persona física (supuestos excepcionales).

2.1.6 Interés público o autoridad – art. 6(1)(e) GDPR

Tratamiento necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos (aplicable cuando un cliente autoridad defina tal base y Quantum Terra actúe como encargado).

Nota multinorma

– CPRA (Secc. 1798.100 ss.): exige transparencia, límites de propósito, derechos del consumidor y acuerdos con “service providers”/“contractors”.

– LFPDPPP (México): licitud, consentimiento cuando corresponda, finalidades y transferencia con límites, seguridad y ARCO.

2.2 Criterios para elegir la base legal (metodología de Quantum Terra)

1. Primero contrato (6(1)(b)) cuando la prestación del servicio al titular o a su empleador requiere el tratamiento.
2. Obligación legal (6(1)(c)) si una norma lo exige (fiscal, laboral, seguridad).

3. Interés legítimo (6(1)(f)) cuando sea necesario y proporcionado: se documenta test de ponderación y se aplican controles (minimización, seudonimización, retenciones cortas).
4. Consentimiento (6(1)(a)) cuando no exista otra base válida o para finalidades accesorias (p. ej., marketing o perfilamiento individual).
5. Tratamientos especiales (vitales, interés público) solo si encajan y están documentados.

2.3 Dato Personal

Se entenderá como dato personal toda información concerniente a una persona física identificada o identificable, conforme a lo previsto en el Reglamento General de Protección de Datos (GDPR), artículo 4, apartado 1, y a lo establecido por la California Privacy Rights Act (CPRA), sección 1798.140. Una persona se considera identificable cuando su identidad puede determinarse directa o indirectamente mediante información asociada como identificadores técnicos, referencias operativas o atributos contextuales razonables.

2.4 Dato Personal Sensible

Es cualquier información cuyo tratamiento indebido pueda dar origen a discriminación o afectar gravemente la intimidad del titular. Incluye información de salud, biometría, ideología, origen étnico, religión, orientación sexual o información genética. Quantum Terra no solicita ni trata datos sensibles salvo que sea estrictamente necesario para cumplir una obligación legal o contractual y exista consentimiento explícito del titular.

2.5 Tratamiento de Datos Personales

Se refiere a cualquier operación o conjunto de operaciones realizadas sobre datos personales, por medios automatizados o no, tales como: recopilación, registro, organización, estructuración, almacenamiento, adaptación, uso, transmisión, difusión, interconexión, seudonimización, anonimización o eliminación, conforme al GDPR, artículo 4, apartado 2.

2.6 Responsable del Tratamiento

Persona física o jurídica que decide sobre las finalidades y medios del tratamiento de datos personales. Quantum Terra actúa como Responsable del Tratamiento cuando determina el uso y la finalidad de un conjunto de datos personales, especialmente en proyectos de trazabilidad operativa, monitoreo geoespacial e inteligencia aplicada.

2.7 Encargado del Tratamiento

Persona física o jurídica que trata datos personales por cuenta del Responsable. En proyectos de integración tecnológica, Quantum Terra puede actuar como Encargado del Tratamiento cuando procesa datos proporcionados por un cliente bajo sus instrucciones documentadas (conforme a un Data Processing Agreement – DPA).

2.8 Subencargado del Tratamiento

Proveedor tecnológico que presta servicios de soporte, infraestructura o analítica y realiza operaciones de tratamiento por instrucción del Encargado. Su actuación debe estar autorizada contractualmente y limitada a finalidades explícitas.

2.9 Transferencia y Remisión de Datos

- Transferencia: comunicación de datos personales a un tercero distinto del Responsable o Encargado.
- Remisión: comunicación de datos a un Encargado para tratamiento por instrucción del Responsable.

Quantum Terra realiza únicamente transferencias legítimas conforme a las Standard Contractual Clauses (SCC 2021/914 UE) y mecanismos legales equivalentes aplicables conforme a CPRA y legislación mexicana vigente.

2.10 Seudonimización

Proceso mediante el cual un dato personal deja de estar asociado directamente a un titular mediante el uso de identificadores indirectos. Reduce el riesgo de identificación sin eliminar completamente el carácter personal del dato (GDPR, artículo 4, apartado 5).

2.11 Anonimización

Transformación irreversible de los datos mediante técnicas que impiden la identificación, directa o indirecta, de una persona física. Una vez anonimizado correctamente, el dato deja de ser considerado dato personal. Quantum Terra aplica métodos de anonimización geométrica y estadística, especialmente en el tratamiento de datos geoespaciales.

2.12 Evaluación de Impacto en Privacidad (DPIA/PIA)

Proceso documentado exigido por GDPR, artículo 35, aplicable cuando un tratamiento implique alto riesgo, como monitoreo sistemático de individuos, perfilamiento automatizado o uso de tecnologías de rastreo geoespacial. Quantum Terra utiliza DPIAs como parte de su gobierno de datos.

2.13 Dato Geoespacial Personal

Se entenderá como Dato Geoespacial Personal toda información de localización vinculada a una persona física identificada o identificable, ya sea de forma directa o indirecta, mediante coordenadas geográficas, referencias espaciales, trayectorias de movimiento, zonas de actividad o cualquier representación espacial que permita inferir su posición pasada, presente o futura.

A diferencia del dato personal tradicional, el dato geoespacial personal incorpora necesariamente un componente de ubicación asociado a contexto, lo cual incrementa su sensibilidad debido a que puede revelar patrones conductuales, hábitos de desplazamiento o incluso aspectos de la vida privada de una persona (domicilio, empleo, lugares visitados). Por esta razón, Quantum Terra lo considera una categoría estratégica con tratamiento reforzado de privacidad.

2.13.1 Formas de Dato Geoespacial Personal

El dato geoespacial personal puede presentarse en distintas formas, entre ellas:

Categoría	Descripción	Ejemplos
Ubicación directa	Coordenada geográfica asociada a una persona física específica	(19.4326, -99.1332), “usuario activo en esta posición”

Ubicación derivada	Inferida de otra información indirecta	Conexión repetida desde misma antena celular, desplazamiento entre puntos
Telemetría asociada	Información generada por sensores IoT que contienen posición	GPS vehicular, reportes CAN/OBD integrados con ubicación
Trayectoria espacio-temporal	Conjunto de puntos geográficos ordenados en el tiempo	Rutas recorridas, historial de movimiento
Área o geocerca asociada	Zonas geográficas vinculadas a comportamiento individual	“Entró a zona restringida”, “salió de perímetro definido”
Clasificación espacial	Perfil generado por análisis geográfico	Zonas de riesgo, frecuencia de visita, proximidad crítica

2.13.2 Riesgo de Reidentificación en Datos Geoespaciales

Incluso cuando los datos geográficos no incluyen el nombre del titular, la combinación de ubicación + tiempo + comportamiento puede permitir su reidentificación. Esto ocurre especialmente cuando:

- Se detecta un domicilio habitual o lugar de trabajo
- La trayectoria se repite regularmente (rutinas de movilidad)
- Se intersecta con otras bases de datos (riesgo de correlación externa)
- Se conocen lugares sensibles visitados por una persona (hospital, sindicato, instalaciones gubernamentales, etc.)

Por lo anterior, Quantum Terra adopta medidas específicas de mitigación como desplazamiento geométrico controlado, precisión degradada, reducción de densidad espacial, cifrado en tránsito y reposo, y hash geográfico cuando aplica.

2.13.3 Técnicas de Protección de Privacidad Geoespacial en Quantum Terra

Para proteger los datos geoespaciales personales, Quantum Terra aplica técnicas de privacidad específicas:

Técnica	**Descripción**
Generalización espacial (Bounding Box)	Sustitución de coordenadas exactas por polígonos aproximados
Hash geográfico	Codificación de ubicación sin revelar coordenadas exactas
Privacidad diferencial espacial	Inyección de ruido controlado para anonimizar movimiento
Enmascaramiento temporal	Eliminación o alteración del orden de tiempo
Geocercas anónimas	Uso de áreas sin ubicación invertible al titular
Cifrado de telemetría	Protección punto a punto de datos IoT/GPS

2.13.4 Diferencia entre Dato Geoespacial Personal y Dato Geográfico No Personal

Categoría	¿Es dato personal?	Ejemplo
Coordenada GPS asociada a un operador de maquinaria	Sí	25.678, -101.334 hora 08:32
Mapa con intensidad térmica de actividad	No (dato agregado)	Heatmap sin identificación
Trayectoria individual de vehículo asignado	Sí	Ruta A–B con ID único
Imagen satelital de terreno agrícola	No	Raster sin vínculo humano

2.13.5 Regla de Quantum Terra

Todo dato espacial que permita inferir actividad humana identificable es considerado dato personal y se protege como tal.

2.14 Perfilamiento o Elaboración de Perfiles (Profiling)

Se entiende por perfilamiento cualquier forma de tratamiento automatizado de datos personales que utilice información personal para evaluar determinados aspectos de una persona física, en particular para analizar o predecir aspectos relacionados con su desempeño laboral, ubicación, fiabilidad, comportamiento, historial de movimiento, preferencias personales o patrones de riesgo. Cuando el perfilamiento incluya componentes geoespaciales, este debe estar respaldado por una base jurídica válida y sujeto a medidas reforzadas de proporcionalidad y transparencia como se trata en la sección 2.1 de Bases Legales.

2.13 Interés Legítimo Tecnológico y Operativo

El interés legítimo es una base jurídica aplicable al tratamiento de datos personales cuando dicho tratamiento es necesario para fines operativos, contractuales o de seguridad tecnológica del responsable, siempre que no prevalezcan los derechos y libertades fundamentales del titular, conforme al artículo 6, apartado 1, inciso f) del GDPR. Quantum Terra utiliza interés legítimo únicamente cuando resulta estrictamente necesario y documenta dicho fundamento en una evaluación interna denominada “Test de Balance de Interés Legítimo”.

Quantum Terra puede tratar datos personales sin pedir permiso (sin consentimiento), siempre que:

- Exista un interés legítimo claro
- Ese interés sea razonable y documentado
- El tratamiento sea necesario para ese fin
- No afecte desproporcionadamente los derechos del titular

Ejemplos de interés legítimo aplicados a Quantum Terra:

- ✓ Registrar accesos a plataforma por seguridad

- ✓ Proteger infraestructura contra fraudes o ataques
- ✓ Analizar uso técnico del sistema para mejorar servicio
- ✓ Telemetría para seguridad operativa de activos

2.14 Brecha de Seguridad de Datos Personales

Es todo evento que resulte o pueda resultar en una destrucción, pérdida, alteración, divulgación no autorizada o acceso no autorizado a datos personales. Las brechas pueden ser de carácter accidental o ilícito y pueden derivar de ataques cibernéticos, errores operativos, accesos internos indebidos o vulnerabilidades tecnológicas. Quantum Terra mantiene un Plan de Respuesta a Incidentes conforme al artículo 33 del GDPR (notificación dentro de las primeras 72 horas cuando aplique).

2.15 Evaluación de No Reidentificación

Es el análisis que determina el riesgo de que un dato aparentemente anónimo pueda volver a asociarse con una persona física a través de la combinación de múltiples fuentes de información. En el contexto geoespacial, Quantum Terra aplicará esta evaluación cada vez que se utilicen datos espaciales derivados o inferidos para garantizar que la anonimización sea efectiva y sostenible.

2.16 Gobernanza de Datos

Es el conjunto de políticas, procedimientos y roles internos implementados para garantizar un tratamiento adecuado de la información durante su ciclo de vida: creación, clasificación, almacenamiento, uso, transferencia y eliminación. Quantum Terra incorpora la gobernanza de datos como parte de su estructura operativa y establece roles responsables para la supervisión de la privacidad y seguridad de los datos procesados.

Véase la **Sección 9 y el Anexo C** para la protección de datos geoespaciales personales y la referencia a medidas aplicables.

3. CATEGORÍAS DE DATOS PERSONALES TRATADOS

Quantum Terra trata únicamente los datos personales que resultan estrictamente necesarios y proporcionales para cumplir con las finalidades legítimas descritas en esta política, en cumplimiento del principio de minimización de datos reconocido por el artículo 5, apartado 1, inciso c) del Reglamento General de Protección de Datos (GDPR). Dependiendo de la relación con el titular y del contexto del proyecto o servicio contratado, Quantum Terra podrá tratar las siguientes categorías de datos personales:

3.1 Datos de Identificación y Contacto

Corresponden a información necesaria para establecer relaciones comerciales o contractuales con clientes, proveedores, aliados tecnológicos o prospectos profesionales. Incluyen nombre completo, correo electrónico, número telefónico, cargo laboral, empresa de afiliación y país de operación. Estos datos se utilizan para fines administrativos, operativos y de comunicación corporativa.

3.2 Datos Profesionales y Contractuales

Se refiere a información asociada con la relación contractual o de prestación de servicios con Quantum Terra. Incluye información de facturación, historial de proyectos, identificadores operativos internos, área de desempeño y datos necesarios para la ejecución legítima de obligaciones contractuales.

3.3 Datos Técnicos y de Interacción Digital

Incluye información derivada del uso de plataformas tecnológicas, portales empresariales y servicios digitales operados o habilitados por Quantum Terra. Comprende dirección IP, identificadores de dispositivo, registros de acceso (logs), configuraciones técnicas, tipo de navegador, zona horaria, interacción con aplicaciones, autenticación por tokens, así como metadatos complementarios necesarios para garantizar la seguridad e integridad de los sistemas.

3.4 Datos Geoespaciales Personales

Se refiere a cualquier información de ubicación asociada a una persona física identificada o identificable, conforme a lo establecido en la Sección 2.11 de esta política. Incluye coordenadas GPS asociadas a una persona o vehículo asignado, trayectorias espacio-temporales, registros de telemetría IoT, zonas de operación en proyectos de monitoreo, patrones de movilidad y ubicación relativa o histórica que permita vincular actividad geográfica con un individuo. Esta categoría recibe un tratamiento reforzado de privacidad y seguridad debido a su naturaleza estratégica.

3.5 Datos Operacionales de Telemetría y Sensores

Información generada por sistemas de supervisión remota, dispositivos IoT, geocercas, rastreo industrial o maquinaria conectada. Incluye información de desempeño vinculada a un dispositivo u operador, tiempos de operación, condiciones de uso y datos derivados que puedan estar asociados directa o indirectamente con una persona física.

3.6 Datos Generados o Inferidos

Quantum Terra puede generar información adicional mediante procesos analíticos legítimos, tales como clasificación operativa, nivel de actividad, riesgo geográfico relativo, patrones de movilidad y otros modelos predictivos derivados del tratamiento autorizado de datos. Aunque estos datos son generados internamente, se consideran datos personales si pueden vincularse a un individuo.

3.7 Datos Financieros Limitados

Quantum Terra únicamente procesa datos financieros o fiscales cuando resulta indispensable para cumplir obligaciones legales o contractuales con clientes o proveedores. Esta categoría puede incluir información de facturación, domicilios fiscales o comprobantes asociados a relaciones comerciales vigentes.

3.8 Exclusión de Datos Sensibles

Quantum Terra no solicita ni trata datos personales sensibles salvo que exista necesidad estricta, base jurídica válida y consentimiento explícito del titular. En los casos excepcionales en los que un proyecto lo requiera, el tratamiento estará sujeto a medidas especiales de protección y evaluación previa de impacto en privacidad.

3.9 Fuentes de Obtención

Los datos personales tratados por Quantum Terra pueden provenir de:

a) información proporcionada directamente por el titular;
b) información proporcionada por clientes responsables del tratamiento;
c) generación interna a partir de datos autorizados;
d) integración legítima con herramientas técnicas u operacionales contratadas.

3.10 Clasificación Interna por Nivel de Sensibilidad

Quantum Terra clasifica los datos personales según su nivel de sensibilidad operativa con el fin de aplicar medidas de seguridad diferenciadas:

4. FINALIDADES DEL TRATAMIENTO Y BASES JURÍDICAS

Quantum Terra trata los datos personales de conformidad con los principios de licitud, lealtad, transparencia, proporcionalidad y responsabilidad previstos en el Reglamento General de Protección de Datos (GDPR), artículo 5, así como la California Privacy Rights Act (CPRA) y la legislación mexicana en materia de protección de datos personales vigente a partir de 2025. Todo tratamiento se realiza con base en una finalidad legítima y sustentado en una base jurídica válida.

4.1 Finalidades del tratamiento

El tratamiento de datos realizado por Quantum Terra se limita a las siguientes finalidades legítimas:

4.1.1 Finalidades primarias (indispensables para la relación contractual)

Estas finalidades son necesarias para la entrega de servicios tecnológicos, implementación de soluciones geoespaciales y cumplimiento operativo con clientes y usuarios. Incluyen:

a) Prestación de servicios en inteligencia geoespacial, análisis satelital, drones, gestión de flotas, seguimiento IoT y visualización de datos
b) Integración, despliegue y soporte de plataformas tecnológicas en entornos cloud o híbridos
c) Administración de acceso a plataformas y autenticación de usuarios
d) Gestión técnica de proyectos, configuración operativa y soporte continuo
e) Cumplimiento de obligaciones contractuales y facturación
f) Seguridad informática y prevención de usos indebidos

4.1.2 Finalidades secundarias (compatibles con la relación principal)

Se refieren a actividades destinadas a la mejora de la calidad del servicio, innovación o análisis interno. Incluyen:

a) Análisis estadístico del rendimiento de plataformas
b) Desarrollo de mejoras funcionales y tecnológicas
c) Evaluación de desempeño de modelos operativos
d) Implementación de mecanismos de calidad de datos
e) Capacitación y auditoría técnica interna
f) Elaboración de reportes de uso empresarial

g) Servicios de localización satelital bajo demanda que generen en consecuencia mapas y datos georreferenciados

4.1.3 Finalidades adicionales sujetas a consentimiento

Estas finalidades solo se ejecutan cuando exista autorización expresa previa del titular:

a) Envío de información comercial o técnica no solicitada
b) Actividades de prospección comercial o marketing empresarial
c) Casos en que se requiera el uso extendido de datos para pruebas avanzadas de análisis
d) Creación y distribución de formularios para levantamiento de datos o registro de información sobre actividades de negocio y empresarial, públicas y privadas

4.2 Bases jurídicas aplicables

El tratamiento de datos personales realizado por Quantum Terra se fundamenta en las siguientes bases jurídicas:

Base jurídica	Aplicación en Quantum Terra
Ejecución de un contrato	Entrega de servicios tecnológicos
Interés legítimo	Seguridad operativa, prevención de abuso
Cumplimiento legal	Obligaciones regulatorias o fiscales
Consentimiento	Marketing o usos no esenciales
Protección de intereses vitales	Casos excepcionales de riesgo
Interés público	Participación en proyectos estratégicos

4.3 Bases jurídicas por región

Jurisdicción	Base jurídica principal
Unión Europea (GDPR)	Art. 6.1 a), b), c) y f)
Estados Unidos (CPRA/CCPA)	Business Purpose y Limited Use
México (Ley 2025)	Finalidad legítima y proporcionalidad

4.4 Finalidades prohibidas

Quantum Terra no realiza tratamiento de datos personales para fines ilícitos ni incompatibles con esta política. Se prohíben expresamente:

a) Tratamiento encubierto mediante técnicas invasivas no transparentes
b) Venta o comercialización de bases de datos
c) Uso de datos sin fundamento jurídico
d) Generación de perfiles discriminatorios
e) Reidentificación intencional en datos anonimizados

4.5 Registro de actividades de tratamiento

Quantum Terra mantiene un Registro Oficial de Actividades de Tratamiento conforme al artículo 30 del GDPR, documentando:

- Sistema o plataforma que ejecuta el tratamiento
- Finalidad asociada
- Categoría de datos procesados
- Base jurídica aplicable
- Alcance geográfico del tratamiento
- Responsable interno asignado
- Plazos de conservación
- Medidas de seguridad aplicadas

5. TRATAMIENTO ESPECÍFICO DE DATOS GEOESPACIALES

Quantum Terra realiza tratamiento de datos geoespaciales únicamente cuando dicho tratamiento es necesario para cumplir obligaciones contractuales, operativas o de soporte tecnológico asociado a sus servicios empresariales. El dato geoespacial vinculado a personas físicas es considerado por Quantum Terra como una categoría de dato que requiere protección reforzada debido a su alta capacidad de inferencia y riesgo de identificación indirecta cuando no se gestionan adecuadamente las medidas de privacidad.

5.1 Naturaleza del dato geoespacial personal

Se entiende como dato geoespacial personal toda información que describa una posición, trayectoria u operación en el espacio asociada a una persona física identificada o identificable. Esta información puede encontrarse representada en forma de coordenadas geográficas, referencias espaciales derivadas, trayectorias históricas de movimiento, proximidad geográfica a un punto de interés, datos obtenidos de sensores IoT con componente de ubicación o información cartográfica que vincule movimientos de un individuo con un entorno físico. Este tipo de información requiere un tratamiento jurídicamente responsable considerando que puede revelar patrones de conducta, localización habitual, relaciones sociales o actividad laboral de una persona.

5.2 Casos en los que Quantum Terra trata datos geoespaciales

Quantum Terra puede tratar datos geoespaciales en los siguientes contextos legítimos: despliegue de plataformas GIS empresariales para clientes, administración de flotas y trazabilidad vehicular, supervisión de operaciones industriales mediante sensores IoT, estudios territoriales con componente humano, análisis situacional de riesgo operativo, gestión de geocercas y aplicaciones similares donde la ubicación tiene relevancia funcional.

Este tratamiento se realiza exclusivamente bajo instrucciones contractuales válidas o de conformidad con el consentimiento informado cuando aplique.

5.3 Riesgo de identificación y criterios de protección aplicados

El dato geoespacial posee características que incrementan el riesgo de identificación indirecta, aun cuando no incluya un nombre o identificador directo. La combinación de ubicación con tiempo o patrones de desplazamiento puede permitir deducir la identidad del titular. Por esta razón, Quantum Terra aplica criterios de protección reforzada como minimización espacial, eliminación progresiva de historiales innecesarios, reducción de precisión en coordenadas según el riesgo del tratamiento y separación de datos identificativos respecto de capas espaciales asociadas.

5.4 Principios de tratamiento geoespacial aplicados por Quantum Terra

Además de los principios generales de protección de datos, Quantum Terra aplica principios adicionales para el tratamiento de datos geoespaciales: proporcionalidad operacional, protección contra inferencias no autorizadas, limitación de permanencia en bases operativas, imposibilidad de uso secundario no autorizado y diseño de privacidad preventiva en arquitectura geoespacial para evitar reidentificación no intencional mediante cruces de datos.

5.5 Medidas de privacidad y seguridad geoespacial

Quantum Terra implementa medidas de carácter técnico y organizativo para proteger el dato geoespacial personal, entre ellas: separación lógica de datos espaciales e identificadores personales, enmascaramiento de trayectorias cuando no se requiere exactitud punto a punto, reducción de precisión en coordenadas, aplicación de anonimización progresiva para almacenamiento histórico y cifrado en tránsito y reposo de los datos de telemetría y geolocalización.

5.6 Uso legítimo de datos geoespaciales

Quantum Terra no utiliza datos geoespaciales personales con fines distintos a los autorizados y contractualmente establecidos. El tratamiento se limita a finalidades operativas legítimas, tales como seguridad operacional, integridad logística, análisis de desempeño, planificación territorial y soporte técnico especializado para clientes empresariales. Cualquier uso adicional requiere evaluación de privacidad y fundamento jurídico válido.

5.7 Limitaciones de uso y actividades prohibidas

Queda expresamente prohibido en Quantum Terra el tratamiento de datos de ubicación con fines distintos a los autorizados por el titular o el responsable del tratamiento. No se realizan actividades de vigilancia oculta, reidentificación intencional, elaboración de perfiles sensibles o discriminatorios, monitoreo no autorizado o comercialización de datos de localización.

5.8 Evaluación de impacto previa en proyectos de riesgo

Cuando un tratamiento geoespacial pueda implicar un riesgo elevado para los derechos y libertades del titular, especialmente en casos de monitoreo continuo, análisis predictivo de movimiento o estudios de movilidad humana, Quantum Terra realiza previamente una

Evaluación de Impacto en Privacidad conforme a los criterios internacionales de protección de datos y documenta medidas de mitigación antes de habilitar el proceso.

6. TRANSFERENCIAS DE DATOS PERSONALES

6.0 Marco normativo aplicable

Las transferencias de datos personales realizadas por Quantum Terra se sujetan al marco legal declarado en el Título 0 de esta Política, en cumplimiento con:

- Capítulo V del GDPR (arts. 44–49) – Transferencias internacionales
- Sección 1798.140 de la CPRA (California Privacy Rights Act)
- Artículos 36 y 37 de la LFPDPPP (México)
- Principios OCDE para flujos internacionales de información
- Contrato + DPA (Data Processing Agreement) + Cláusulas Contractuales Estándar (SCC) cuando apliquen

Toda transferencia se realizará solo si existe una base jurídica válida y garantías adecuadas, conforme a lo establecido en el artículo 6, apartado 1, inciso b) o f) del GDPR (ejecución de contrato o interés legítimo documentado) o base equivalente en CPRA/LFPDPPP.

6.1 Tipos de transferencias realizadas

Quantum Terra puede realizar dos tipos de transferencias:

Tipo	Descripción	Alcance
a) Nacionales	A entidades dentro del mismo país para fines operativos o contractuales	Clientes o proveedores locales
b) Internacionales	A entidades en otros países para continuidad operativa	Infraestructura cloud, GIS, análisis, soporte técnico

6.2 Supuestos permitidos de transferencia

Quantum Terra podrá transferir datos personales únicamente cuando:

1. Exista obligación contractual para la prestación del servicio.
2. Exista instrucción legítima del Responsable del Tratamiento.
3. Exista interés legítimo conforme al artículo 6(1)(f) GDPR (operación técnica, estabilidad o seguridad del sistema).
4. Sea necesario para cumplir una obligación legal (autoridades competentes).
5. El titular haya otorgado consentimiento explícito, cuando sea requerido.
6. Exista riesgo operativo o de seguridad que requiera continuidad del servicio (infraestructura redundante o recuperación ante desastres).

6.3 Países y jurisdicciones de destino

Las transferencias internacionales podrán realizarse a:

- Estados Unidos de América (operación cloud, servicios GIS, seguridad, DevOps)
- Canadá y países de la AELC/EEE (si aplica)
- Regiones operativas según infraestructura de proveedor tecnológico (AWS, Azure, Esri Cloud, etc.), conservando trazabilidad y registro de ubicación de datos.

Cuando los países destino no cuenten con decisión de adecuación (art. 45 GDPR), Quantum Terra aplicará Cláusulas Contractuales Estándar (SCC) o garantías alternativas (art. 46 GDPR).

6.4 Medidas y garantías contractuales para transferencias

Toda transferencia estará protegida contractualmente mediante:

- DPA (Data Processing Agreement) con obligaciones claras
- SCC (Standard Contractual Clauses – Comisión Europea) en transferencias internacionales
- Confidencialidad vinculante (NDA corporativo)
- Limitación de propósito – uso solo autorizado
- Retención limitada y supresión obligatoria
- Prohibición de venta de datos (CPRA compliance)
- Prohibición de subtransferencia sin autorización
- Auditoría y supervisión técnica
- Referencia interna: ver también Sección 7 (Subencargados) para conocer cómo se extienden estas mismas obligaciones a proveedores tecnológicos.

6.5 Transferencias con proveedores tecnológicos (cloud/GIS/seguridad)

Quantum Terra podrá transferir datos a proveedores tecnológicos estratégicos cuando sea necesario para ejecutar servicios, siempre bajo contrato, seguridad certificada y trazabilidad operativa. Ejemplos:

Proveedor	Finalidad	Naturaleza
AWS	Cloud hosting / redundancia	Subencargado
Esri	GIS – motor geoespacial	Subencargado
Azure / Oracle Cloud	Infraestructura o almacenamiento	Subencargado
Cloudflare u otro	Seguridad de red	Subencargado

Notas de cumplimiento: Los proveedores tecnológicos no pueden usar datos para sus propios fines. Actúan únicamente bajo instrucciones de Quantum Terra y quedan sujetos a obligaciones contractuales equivalentes a las de Quantum Terra (efecto cascada).

6.6 Transferencias con autoridades o requerimientos legales

Quantum Terra solo transferirá datos a autoridades legítimamente facultadas previa verificación documental del requerimiento.

Cuando la ley lo permita, Quantum Terra notificará al cliente antes de transferirlos. Si está prohibido, cumplirá sin revelar más información que la estrictamente necesaria.

6.7 Transferencias prohibidas

Quantum Terra NO realiza:

- Venta o comercialización de datos personales
- Transferencias no autorizadas a terceros no vinculado
- Transferencias sin base jurídica
- Transferencias con fines publicitarios ilícitos
- Transferencias fuera del control contractual

6.8 Documentación legal aplicable

Toda transferencia quedará documentada en:

- Registro de Transferencias de Quantum Terra (interno)
- DPA firmado con el cliente
- SCC o mecanismos alternos GDPR (si aplica)
- Lista de subencargados autorizados
- Bitácoras o logs técnicos de transferencia

6.9 Derechos del titular frente a transferencias

Todo titular podrá solicitar información sobre destinatarios, razones y base legal de las transferencias relacionadas con sus datos personales. Este derecho se ejerce mediante solicitud formal enviada a:

privacy@quantumterra.ai | quantum.terra@outlook.com

Véase Anexo F (Mecanismos SCC/DPA) y **Anexo I (Políticas de proveedores)**.

7. USO DE SUBENCARGADOS Y PROVEEDORES TECNOLÓGICOS

Quantum Terra podrá apoyarse en terceros que actúen como subencargados del tratamiento de datos personales cuando ello sea estrictamente necesario para la operación de servicios tecnológicos, continuidad operativa, cumplimiento contractual o soporte especializado. Todo subencargado quedará sujeto a obligaciones contractuales equivalentes a las establecidas para Quantum Terra, conforme al artículo 28 del Reglamento General de Protección de Datos (GDPR), la California Privacy Rights Act (CPRA – Sección 1798.140(h)) y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (México) y el marco regulatorio digital 2025 aplicable.

El uso de dichos proveedores no implica cesión, venta ni uso independiente de datos personales. Todos actúan bajo contrato de licenciamiento/servicio con Quantum Terra y están obligados a cumplir instrucciones documentadas y medidas equivalentes de seguridad y privacidad.

7.1 Naturaleza de los subencargados

Se considera subencargado a toda persona física o moral que trate datos personales por cuenta de Quantum Terra y bajo sus instrucciones documentadas, sin adquirir en ningún momento el carácter de Responsable del Tratamiento. Se incluyen dentro de esta categoría:

- Proveedores de computación en la nube (cloud computing),
- Infraestructura de servidores y almacenamiento seguro,
- Plataformas de información geoespacial (GIS), análisis espacial y cartografía digital,
- Servicios de telemetría IoT y redes de geolocalización operativa,
- Herramientas de ciberseguridad, autenticación y gestión de accesos,
- Servicios de continuidad operativa, respaldo y data recovery.

7.2 Subencargados tecnológicos estratégicos

Quantum Terra utiliza proveedores tecnológicos bajo contratos de uso empresarial (licencias comerciales) y condiciones de servicio estándar. El uso de dichos proveedores no implica relación de asociación, joint venture, representación comercial o certificación de alianza estratégica. Se trata únicamente de una relación basada en servicios tecnológicos contratados. Entre los proveedores utilizados se encuentran, entre otros:

Proveedor	Finalidad técnica	Política de privacidad
Amazon Web Services (AWS)	Infraestructura cloud, almacenamiento y despliegue técnico	https://aws.amazon.com/privacy/
Esri (ArcGIS Online / Enterprise)	Motor GIS corporativo y análisis geoespacial	https://www.esri.com/en us/privacy/overview
Microsoft Azure (cuando aplica)	Infraestructura y servicios de identidad	https://privacy.microsoft.com
Oracle Cloud (si aplica)	Bases de datos corporativas	https://www.oracle.com/legal/privacy/

Quantum Terra utiliza estas soluciones únicamente como recursos tecnológicos de soporte; nunca transfieren propiedad ni control de datos a dichos proveedores, ni éstos adquieren derechos de explotación o comercialización sobre los datos tratados.

7.3 Adhesión a políticas de privacidad de proveedores externos

Cualquier tratamiento realizado a través de los servicios de estos proveedores estará sujeto también a sus respectivas políticas de privacidad y términos de uso. Esto no libera a Quantum Terra de sus responsabilidades legales, pero deja claro que ciertos aspectos técnicos del procesamiento se rigen por los marcos normativos propios de dichos proveedores. Quantum Terra exige que todo subencargado cumpla estándares equivalentes o superiores de cumplimiento normativo (GDPR, CPRA, CCPA, LFPDPPP, ISO 27001, NIST).

7.4 Obligaciones contractuales de los subencargados

Todo subencargado deberá formalizar un Acuerdo de Procesamiento de Datos (DPA) con Quantum Terra, el cual incluye como mínimo:

- Confidencialidad permanente,
- Prohibición absoluta de uso de datos para fines propios,
- Implementación obligatoria de medidas de seguridad y cifrado,
- Trazabilidad y registro de acceso (logs y auditoría),
- Notificación oportuna de incidentes de seguridad,
- Supresión o devolución segura de datos al término de la relación contractual.

7.5 Supervisión y verificación de cumplimiento

Quantum Terra podrá supervisar el desempeño de los subencargados y solicitar evidencia de cumplimiento. Si se detecta incumplimiento o riesgo operativo, Quantum Terra podrá suspender o revocar acceso inmediato a los datos.

7.6 Subcontratación en cadena prohibida

Ningún subencargado podrá a su vez subcontratar a otro subencargado (“subprocesamiento en cadena”) sin aprobación previa y por escrito de Quantum Terra. En caso de autorizarse, deberán trasladarse íntegramente las mismas obligaciones contractuales.

7.7 Lista de subencargados autorizados

Quantum Terra mantiene una lista interna actualizada de subencargados autorizados, disponible para clientes o titulares que lo soliciten formalmente mediante el canal de privacidad.

Consulta formal disponible vía:

privacy@quantumterra.ai | quantum.terra@outlook.com

7.8 Blindaje legal

Quantum Terra implementa controles preventivos y contratos con obligaciones equivalentes a las propias. No obstante, Quantum Terra no será responsable por incumplimientos

atribuibles directamente a un subencargado cuando dicho riesgo haya sido mitigado mediante control contractual razonable y selección diligente del proveedor.

7.9 Relación con otras secciones de la Política

Esta sección se complementa con:

- Sección 6 – Transferencias de datos personales,
- Anexo F – Mecanismos de transferencia internacional (SCC/DPA),
- Anexo I – Enlaces de políticas de proveedores tecnológicos,
- Sección 9 – Seguridad de datos.

Los proveedores tecnológicos mencionados no adquieren derechos de explotación ni de uso independiente sobre los datos personales tratados. El uso de dichas plataformas no implica cesión ni venta de datos; actúan exclusivamente bajo contrato de licenciamiento/servicio con Quantum Terra y quedan obligados a cumplir las instrucciones documentadas y medidas equivalentes de seguridad y privacidad. Véanse Anexos G e I.

8. CONSERVACIÓN Y ELIMINACIÓN DE DATOS PERSONALES

Quantum Terra conserva los datos personales únicamente durante el tiempo que sea necesario para cumplir con las finalidades legítimas del tratamiento y conforme a obligaciones contractuales, operativas o legales aplicables. Una vez que la información deja de ser necesaria para dichos fines, será eliminada o sometida a un proceso de anonimización irreversible.

8.1 Criterios de conservación

Los plazos de conservación aplicados por Quantum Terra se determinan conforme a los siguientes criterios:

- Cumplimiento de finalidades del tratamiento
- Obligaciones contractuales con clientes o proveedores
- Cumplimiento de disposiciones legales o regulatorias
- Preservación de evidencias en caso de auditorías o controversias
- Seguridad operativa y defensa de intereses legítimos

8.2 Plazos de conservación por categoría de datos

Quantum Terra aplica plazos diferenciados de retención según la naturaleza de la información tratada:

Categoría de datos	Plazo de conservación	Justificación
Datos de identificación y contacto	Mientras exista relación comercial	Necesidad contractual
Datos contractuales y administrativos	Vigencia del contrato + 5 años	Obligaciones legales y auditorías
Datos técnicos (registros de acceso y logs)	6 a 24 meses	Seguridad operativa

Datos geoespaciales personales	De 12 a 36 meses según finalidad	Necesidad operativa y trazabilidad
Telemetría IoT asociada a operación	12 meses, prorrogables según contrato	Continuidad operacional
Información fiscal y contable	5 años	Legislación aplicable
Datos anonimizados	Indefinido	No son datos personales

8.3 Eliminación y supresión de datos

Una vez concluida la finalidad del tratamiento, Quantum Terra procederá a eliminar los datos personales mediante mecanismos seguros que impidan su recuperación. El proceso de eliminación podrá realizarse mediante:

- Eliminación lógica en sistemas de producción
- Eliminación física en repositorios locales cuando corresponda
- Anonimización irreversible cuando se requiera conservar datos estadísticos o históricos

8.4 Bloqueo temporal

En casos en los que exista una obligación legal o contractual que impida la eliminación inmediata de datos, Quantum Terra podrá aplicar un período de bloqueo temporal, durante el cual los datos serán restringidos y únicamente accesibles para cumplimiento legal o auditoría.

8.5 Anonimización

Cuando resulte necesario conservar información para fines estadísticos, de aprendizaje tecnológico o estudios operacionales, Quantum Terra podrá aplicar técnicas de anonimización irreversible, eliminando toda capacidad de vincular los datos con una persona física.

8.6 Registro y trazabilidad de eliminación

Quantum Terra mantiene registros internos que acreditan la aplicación de políticas de eliminación y depuración de datos conforme a procedimientos auditables y verificables.

Véase **Anexo B (Conservación y eliminación).**

9. SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS

Quantum Terra implementa medidas **técnicas, administrativas y organizativas** destinadas a garantizar la **confidencialidad, integridad y disponibilidad** de los datos personales bajo su tratamiento. Estas medidas se aplican conforme al principio de **seguridad basada en riesgo**, responsabilidad proactiva (accountability) y **privacidad por diseño**. Quantum Terra reconoce que ningún sistema es técnicamente invulnerable; sin embargo, mantiene un marco de **seguridad razonable y proporcional**, alineado a

estándares internacionales, aplicable tanto a infraestructura propia como a servicios tecnológicos de terceros utilizados para la operación.

9.1 Principio de seguridad en Quantum Terra

Quantum Terra implementa seguridad **por diseño y por defecto** en todas sus operaciones, integrando controles preventivos desde la arquitectura de soluciones tecnológicas hasta el despliegue operativo. La seguridad se aplica tanto al tratamiento de datos personales como a información estratégica y operativa de clientes.

9.2 Marco normativo, arquitectura de seguridad aplicada y proveedores tecnológicos habilitados

Quantum Terra opera bajo un **modelo de gestión de seguridad híbrido**, soportado en infraestructura controlada y plataformas tecnológicas certificadas como **Amazon Web Services (AWS)** y **Esri ArcGIS**, utilizadas bajo **licencia empresarial**. Estas plataformas proveen servicios tecnológicos, pero **no adquieren derechos sobre los datos procesados**. El tratamiento permanece bajo control de Quantum Terra.

Infraestructura tecnológica utilizada:

- AWS Cloud – infraestructura segura y redundante:
  https://aws.amazon.com/privacy/
- Esri ArcGIS Platform – gestión geoespacial profesional:
  https://www.esri.com/en-us/privacy/overview
- Otros proveedores estratégicos certificados (si aplica):
  Microsoft Azure (https://privacy.microsoft.com)
  Oracle Cloud (https://www.oracle.com/legal/privacy/)

El uso de estos proveedores **no implica alianza empresarial ni transferencia de responsabilidad**, sino únicamente procesamiento técnico bajo contrato y controles de seguridad.

Adicionalmente, Quantum Terra adopta formalmente los siguientes estándares:

- **ISO/IEC 27001** – Sistema de Gestión de Seguridad de Información
- **ISO/IEC 27002** – Controles de ciberseguridad
- **NIST SP 800-53** – Seguridad en infraestructura tecnológica
- **NIST Cybersecurity Framework (CSF)** – Gobernanza de riesgo
- **Modelo Zero Trust** – Control de acceso estricto y segmentación

Véase **Anexo C (MTO).**

9.3 Política interna de seguridad

Quantum Terra mantiene una Política Interna de Seguridad de Información que es obligatoria para empleados, contratistas, proveedores y subencargados. Incluye administración de privilegios, uso aceptable, protección de infraestructura, clasificación de activos y gestión disciplinaria por incumplimientos.

9.4 Controles de seguridad implementados

La seguridad se ejecuta siguiendo una estrategia de defensa en profundidad con controles como:

- Control de acceso basado en roles (RBAC) y privilegio mínimo
- Autenticación multifactor (MFA)
- Segmentación de red y aislamiento de entornos críticos
- Supervisión y monitoreo continuo de actividad
- Escaneo de vulnerabilidades y actualizaciones periódicas

9.5 Seguridad en infraestructura tecnológica

Quantum Terra asegura la protección de servidores dedicados o plataformas cloud mediante:

- Hardening de sistemas
- Firewalls de aplicación
- Protección contra amenazas (IDS/IPS)
- Gestión de certificados
- Monitoreo y respuesta ante eventos (SIEM)

9.6 Protección de datos geoespaciales e información sensible

Quantum Terra aplica controles adicionales a datos geoespaciales personales:

- Separación lógica entre identidad y ubicación
- Reducción de precisión geográfica según finalidad
- Enmascaramiento georreferencial operativo
- Auditoría obligatoria de consultas sensibles
- Anonimización para modelos de análisis cuando sea viable

9.7 Gestión de vulnerabilidades y monitoreo

La infraestructura técnica está sujeta a escaneos de vulnerabilidad, pruebas de resiliencia y monitoreo permanente. Planes de remediación rápida son ejecutados ante riesgo detectado.

9.8 Cifrado y resguardo seguro de información

Quantum Terra cifra datos:

- **En tránsito:** TLS/HTTPS
- **En reposo:** AES-256 u otro algoritmo estándar equivalente
- **En uso:** aislamiento operacional restringido

9.9 Registro y trazabilidad de operaciones

Se conservan **logs de acceso, modificación, consulta y eliminación** de datos. Todo evento relevante es rastreado y archivado siguiendo políticas internas de conservación.

9.10 Continuidad operativa y recuperación ante incidentes

Planes de continuidad e infraestructura resiliente garantizan disponibilidad razonable. Se emplean redundancia en nube, alta disponibilidad, replicación operativa y backups programados. El Plan de Respuesta a Incidentes se detalla en el Anexo C.

9.11 Responsabilidad limitada en materia de seguridad de la información

Quantum Terra implementa medidas de seguridad razonables, proporcionales al riesgo y acordes con el estado del arte tecnológico para proteger los datos personales y la infraestructura bajo su control. No obstante, el titular y/o cliente reconoce y acepta que ningún sistema, red, infraestructura tecnológica, plataforma en la nube o servicio digital es completamente inmune a vulneraciones o incidentes de seguridad derivados de factores externos. En consecuencia:

a) Quantum Terra **no será responsable** por brechas de seguridad, accesos no autorizados, pérdida de información o cualquier daño derivado de:

- Ataques cibernéticos de carácter externo, incluyendo hacking, ransomware, denegación de servicio (DoS o DDoS), intrusiones avanzadas (APT) u otros eventos similares;
- Fallas o interrupciones en servicios de infraestructura asociados a terceros proveedores de telecomunicaciones, centros de datos, servicios cloud o redes satelitales;
- Errores u omisiones atribuibles exclusivamente al cliente, incluyendo configuraciones inseguras, uso indebido de accesos o falta de cumplimiento de políticas operativas;
- Supuestos de fuerza mayor o caso fortuito, como eventos naturales, conflictos sociales o crisis ajenas al control razonable de Quantum Terra.

b) Quantum Terra asumirá responsabilidad únicamente cuando se acredite **falta grave o incumplimiento directo** a sus obligaciones contractuales de seguridad, y siempre dentro de los límites de responsabilidad establecidos en el contrato marco y acuerdos legales aplicables con el cliente.

c) En caso de un incidente de seguridad confirmando riesgo para los titulares o terceros, Quantum Terra activará su **Plan Corporativo de Respuesta a Incidentes** conforme al Anexo C y notificará al cliente o autoridad competente cuando proceda legalmente.

Quantum Terra aplica medidas de seguridad razonables y proporcionales al riesgo. No obstante, ningún sistema es invulnerable. Quantum Terra no será responsable por incidentes atribuibles a ataques externos, fallas de terceros, configuraciones indebidas del cliente o fuerza mayor, salvo incumplimiento grave directamente imputable a Quantum Terra. Ante un incidente, se activará el Plan de Respuesta (Anexo C) y se notificará conforme a ley.

10. DERECHOS DE LOS TITULARES DE DATOS

Quantum Terra reconoce y garantiza el ejercicio de los derechos de protección de datos personales conforme a los principios de autodeterminación informativa, transparencia y legalidad. Todo titular tiene derecho a conocer cómo se recopila, utiliza, conserva, comparte o elimina su información personal, así como a solicitar el ejercicio de sus derechos de privacidad de manera efectiva y gratuita.

10.1 Principio general de autodeterminación informativa

Quantum Terra respeta el derecho de las personas a decidir sobre el uso legítimo de sus datos personales. Este principio se encuentra respaldado por el marco internacional de protección de datos, incluyendo el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, la California Privacy Rights Act (CPRA) y la legislación mexicana vigente en materia de datos personales.

10.2 Derechos reconocidos a los titulares

Dependiendo de la jurisdicción aplicable, Quantum Terra reconoce y habilita los siguientes derechos para los titulares de datos personales:

- Derecho de acceso: conocer qué datos personales se tratan.
- Derecho de rectificación: solicitar la corrección de información inexacta o incompleta.
- Derecho de supresión o cancelación: solicitar la eliminación de datos cuando ya no sean necesarios o se haya retirado el consentimiento.
- Derecho de oposición: oponerse al tratamiento cuando no exista obligación legal o contractual que lo justifique.
- Derecho a la limitación del tratamiento: restringir temporalmente el uso de los datos en determinados supuestos.
- Derecho a la portabilidad: solicitar el envío de los datos a otro responsable cuando sea técnicamente posible.
- Derecho a retirar el consentimiento: en tratamientos basados en consentimiento previo.
- Derecho a no ser objeto de decisiones automatizadas: especialmente en casos de perfilamiento que produzca efectos legales directos.
- Estos derechos se atenderán conforme a lo establecido en el GDPR (artículos 15 a 21), CPRA (sección 1798.100 y siguientes) y legislación mexicana aplicable.

10.3 Procedimiento para ejercer derechos

El titular podrá ejercer sus derechos enviando una solicitud formal al correo institucional designado para este fin:

- Correo de contacto para ejercicio de derechos: **privacy@quantumterra.ai**

La solicitud deberá contener como mínimo:

- Nombre completo del titular
- Medio para comunicar la respuesta
- Descripción clara del derecho que desea ejercer
- Identificación oficial o medio que acredite identidad
- Documentos adicionales si ejerce en representación de un tercero

10.4 Verificación de identidad y respuesta

Quantum Terra podrá solicitar información o documentación adicional cuando sea necesario verificar la identidad del solicitante y prevenir fraudes o accesos no autorizados. Las solicitudes serán atendidas dentro de un plazo razonable a partir de su recepción, sujeto a la normativa aplicable en cada jurisdicción.

10.5 Derecho a limitar el tratamiento geoespacial

Dado que Quantum Terra realiza actividades de procesamiento geoespacial, se reconoce expresamente el derecho del titular a solicitar la limitación parcial o total del tratamiento de datos geoespaciales personales cuando considere que dicho tratamiento afecta su privacidad o seguridad personal, excepto en casos en los que exista obligación legal o contractual vigente que lo impida.

10.6 Restricciones al ejercicio de derechos

Los derechos descritos podrán negarse total o parcialmente cuando:

- Exista obligación legal que impida atender la solicitud.
- Se comprometa información de terceros.
- Se afecten investigaciones internas o requerimientos de autoridad.
- Se ponga en riesgo la seguridad de infraestructura crítica.
- El solicitante no acredite su identidad correctamente.

En todos los casos, Quantum Terra comunicará las razones de la determinación correspondiente.

10.7 Registro y trazabilidad de solicitudes

Quantum Terra mantiene un control interno de solicitudes de derechos ejercidos por los titulares, con objeto de garantizar trazabilidad, transparencia y cumplimiento normativo. Dicho registro se conserva conforme a los plazos de conservación definidos en esta política.

Véase **Anexo D (Procedimiento de derechos)**

11. CONSENTIMIENTO Y BASES JURÍDICAS DEL TRATAMIENTO

Quantum Terra realiza el tratamiento de datos personales únicamente cuando existe una base jurídica válida que legitima dicho tratamiento. El consentimiento del titular es uno de los fundamentos legales reconocidos, pero no es el único aplicable. Dependiendo del tipo de tratamiento, de la relación con el titular y de la legislación vigente, podrán aplicarse bases jurídicas alternativas cuando corresponda.

11.1 Consentimiento del titular

Cuando el tratamiento de datos personales no se base en otra causa de legitimación, Quantum Terra podrá solicitar el consentimiento del titular de forma previa, expresa e informada. El consentimiento podrá recabarse por medios electrónicos o documentales y deberá ser verificable. En todo momento se respetará el derecho del titular a retirar su consentimiento de forma posterior, sin efectos retroactivos sobre tratamientos ya realizados legítimamente.

11.2 Casos en los que el consentimiento no es requerido

Quantum Terra podrá tratar datos personales sin necesidad de obtener consentimiento cuando exista otra base legal aplicable conforme a la normativa vigente, entre ellas:

- Cuando el tratamiento sea necesario para la ejecución de un contrato con el titular o con la entidad que represente.

- Cuando el tratamiento se realice en cumplimiento de una obligación legal aplicable.
- Cuando el tratamiento se base en un interés legítimo documentado y no vulnera los derechos del titular.
- Cuando el tratamiento sea necesario para la seguridad de la información o la prevención de usos indebidos.
- Cuando exista una obligación derivada de una autoridad competente o un mandato legal.

11.3 Base jurídica por tipo de finalidad

Las bases jurídicas utilizadas por Quantum Terra para el tratamiento de datos son consistentes con:

- Artículo 6 del Reglamento General de Protección de Datos (GDPR).
- Sección 1798.100 de la California Privacy Rights Act (CPRA).
- Legislación mexicana aplicable en materia de protección de datos personales en posesión de particulares que se encuentre vigente.

11.4 Consentimiento para tratamiento geoespacial

Cuando se requiera tratar datos geoespaciales personales asociados a individuos identificados, el consentimiento podrá solicitarse de manera diferenciada cuando el tipo de proyecto así lo exija, especialmente en escenarios de monitoreo individual continuo o trazabilidad personalizada. Este consentimiento podrá formar parte del contrato de servicios, declaración corporativa o acuerdo digital de aceptación informado.

11.5 Revocación del consentimiento

Los titulares podrán revocar en cualquier momento el consentimiento otorgado para el tratamiento de sus datos personales. Esta revocación deberá solicitarse de forma expresa mediante solicitud formal a través de los medios oficiales definidos en esta política. La revocación no tendrá efectos retroactivos respecto de tratamientos realizados con base en consentimiento previamente otorgado.

11.6 Limitación del consentimiento en ciertos casos

Quantum Terra podrá continuar el tratamiento de datos personales aun cuando el consentimiento haya sido revocado cuando exista una base jurídica alternativa que lo permita, como obligación legal o contractual vigente. En todos los casos se respetarán los principios de proporcionalidad y necesidad.

Véase **Anexo H (Aceptación obligatoria)**

12. DECISIONES AUTOMATIZADAS Y PERFILAMIENTO

Quantum Terra realiza actividades de análisis avanzados que pueden incluir modelado predictivo, clasificación operativa, segmentación técnica y analítica aplicada para optimizar procesos de negocio de sus clientes. Sin embargo, Quantum Terra no toma decisiones que produzcan efectos legales o que afecten significativamente al titular de forma automática sin intervención humana responsable.

12.1 Definición de decisiones automatizadas

Se considera decisión automatizada aquella que es generada exclusivamente mediante procesamiento automático de datos sin intervención humana significativa. Este tipo de decisiones se encuentra regulado internacionalmente debido al impacto que podría generar sobre los derechos de los titulares. Quantum Terra no aplica decisiones automatizadas sin supervisión humana y mantiene siempre revisión técnica responsable antes de ejecutar conclusiones que involucren datos personales.

12.2 Alcance del perfilamiento

El perfilamiento consiste en el análisis automatizado de datos personales para evaluar aspectos relacionados con el desempeño laboral, preferencias, ubicación, movimiento geoespacial, comportamiento operacional u otros patrones asociados con la actividad del titular. Quantum Terra utiliza técnicas de análisis bajo principios de proporcionalidad y respeto a la privacidad, y únicamente en contextos legítimos previamente autorizados contractualmente.

12.3 Perfilamiento geoespacial

En los casos en los que se realicen análisis derivados de datos geoespaciales personales, Quantum Terra aplicará restricciones específicas para evitar uso indebido o inferencias abusivas. El tratamiento geoespacial se limita a finalidades operativas, logísticas, de continuidad de negocio o seguridad operativa. Quantum Terra no utiliza análisis geoespacial para fines invasivos de monitoreo personal ni para perfilamiento conductual no autorizado.

12.4 Transparencia en procesos analíticos

Los análisis que se generen como parte de los servicios tecnológicos prestados por Quantum Terra no tienen por objeto generar acciones discriminatorias, invasivas o desproporcionadas. Cuando un proyecto requiera la implementación de modelos predictivos, inteligencia operativa o clasificación automática, Quantum Terra documentará el propósito del modelo y su impacto previsto sobre los titulares antes de su implementación.

12.5 Derechos del titular ante decisiones automatizadas

El titular podrá oponerse al uso de perfilamiento que involucre tratamiento injustificado de datos personales o solicitar información clara acerca de la lógica aplicada en procesos automatizados que puedan afectarlo directamente. Quantum Terra asegura la posibilidad de revisión humana en todos los casos que lo requieran y garantiza un canal accesible para que el titular pueda manifestar oposición razonada.

13. GESTIÓN DE INCIDENTES Y NOTIFICACIÓN DE BRECHAS DE SEGURIDAD

Quantum Terra mantiene procedimientos internos para detectar, analizar y responder a incidentes de seguridad que puedan comprometer la integridad, confidencialidad o disponibilidad de los datos personales bajo su custodia. Estos procedimientos forman parte de su modelo operativo de seguridad y se realizan conforme al deber de responsabilidad proactiva.

13.1 Definición de brecha de seguridad

Se considera brecha de seguridad cualquier evento que derive en acceso no autorizado, pérdida, alteración, destrucción o divulgación indebida de datos personales, ya sea de

forma accidental o ilícita. Las brechas pueden originarse por ciberataques, fallas técnicas, errores humanos o comportamiento negligente de terceros con acceso autorizado a información.

13.2 Modelo de gestión de incidentes

Quantum Terra dispone de un Modelo de Gestión de Incidentes que integra detección temprana, análisis de causa raíz, contención del incidente, mitigación del impacto y medidas correctivas. Este modelo incluye registro documental de incidentes, coordinación con equipos técnicos internos y, cuando procede, participación de subencargados tecnológicos involucrados en el tratamiento.

13.3 Notificación de brechas

Cuando una brecha de seguridad represente un riesgo para los derechos de los titulares, Quantum Terra notificará el incidente al responsable del tratamiento o autoridad competente, según sea aplicable. Las notificaciones se realizarán en un plazo razonable y conforme a los criterios establecidos por la normativa vigente. Cuando corresponda, también se informará a los titulares afectados de forma clara y verificable.

13.4 Coordinación con terceros

Cuando un incidente de seguridad involucre a subencargados, proveedores tecnológicos o aliados operativos, Quantum Terra exigirá colaboración inmediata para la investigación del evento y la implementación de medidas de contención. Toda empresa tercera con acceso a datos deberá asumir responsabilidades contractuales de notificación oportuna de incidentes de seguridad.

13.5 Prevención y mejora continua

Quantum Terra realiza evaluaciones periódicas de vulnerabilidades y simulaciones de incidentes para fortalecer su preparación operativa. Asimismo, incorpora controles de aprendizaje continuo para prevenir recurrencia mediante ajustes técnicos, actualizaciones de seguridad y prácticas internas de concientización corporativa.

14. TRANSFERENCIAS INTERNACIONALES Y CUMPLIMIENTO MULTINORMA

Quantum Terra realiza operaciones con alcance internacional que pueden implicar el tratamiento y transferencia de datos personales fuera del país de origen del titular. Toda transferencia internacional se realiza conforme a marcos regulatorios vigentes y bajo mecanismos que garantizan la protección adecuada de la información, sin importar el país de destino.

14.1 Principio de continuidad de protección

En toda transferencia internacional de datos personales, Quantum Terra garantiza que el nivel de protección conferido a la información no se verá reducido como consecuencia de dicha transferencia. Esto significa que, aun cuando los datos sean trasladados a países con normativa distinta en materia de privacidad, deberán mantenerse bajo estándares equivalentes a los establecidos en esta política.

14.2 Fundamento jurídico internacional

Quantum Terra cumple con los marcos internacionales de protección de datos aplicables según el territorio de operación del cliente o titular, entre ellos:

- Reglamento General de Protección de Datos (GDPR) de la Unión Europea.
- California Privacy Rights Act (CPRA) y normativa estatal aplicable en Estados Unidos.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares (México) y el marco regulatorio digital aplicable en 2025.
- Principios de privacidad de la Organización para la Cooperación y el Desarrollo Económicos (OCDE).

14.3 Mecanismos contractuales de transferencia

Cuando la transferencia de datos personales se realice hacia países que no cuenten con una decisión de adecuación en materia de protección de datos, Quantum Terra aplicará garantías contractuales adecuados, entre ellas:

- Cláusulas contractuales estándar para transferencia de datos.
- Acuerdos de procesamiento de datos (DPA).
- Obligaciones de confidencialidad para todos los participantes del tratamiento.
- Limitación estricta de finalidad y retención de datos.
- Reglas de cooperación en materia de seguridad y cumplimiento.

14.4 Transferencias intragrupo o con aliados estratégicos

Quantum Terra podrá realizar transferencias de datos entre entidades vinculadas o aliados estratégicos únicamente cuando sea necesario para cumplir obligaciones contractuales o entregar servicios corporativos especializados. En estos casos, la transferencia estará sujeta a obligaciones de protección y confidencialidad equivalentes a las establecidas en esta política.

14.5 Transferencias derivadas de obligaciones legales

En circunstancias excepcionales, Quantum Terra podrá transferir datos personales cuando exista un requerimiento legal de una autoridad competente, siempre que dicho requerimiento sea legítimo y se encuentre debidamente fundamentado. En estos casos, Quantum Terra evaluará la legalidad de la solicitud y limitará la transferencia a la información estrictamente necesaria para cumplir la obligación.

15. DELEGADO DE PROTECCIÓN DE DATOS Y CUMPLIMIENTO CORPORATIVO

Quantum Terra mantiene un modelo de cumplimiento interno en materia de protección de datos y privacidad corporativa basado en responsabilidades claramente definidas y supervisión continua. Dicho modelo forma parte de su estructura de gobernanza y constituye un componente esencial de sus operaciones internacionales.

15.1 Responsabilidad en materia de privacidad

La responsabilidad general del cumplimiento de esta política recae en la alta dirección de Quantum Terra, quien garantiza la disponibilidad de recursos adecuados para mantener

controles de privacidad, seguridad y legalidad en el tratamiento de datos personales. Toda persona que trate datos bajo responsabilidad de Quantum Terra deberá observar esta política y actuar conforme a los principios y marcos normativos aplicables.

15.2 Delegado de Protección de Datos (DPO)

Quantum Terra podrá designar un Delegado de Protección de Datos (DPO, por sus siglas en inglés) o Responsable de Privacidad cuando así lo exijan las leyes aplicables o cuando la naturaleza de los proyectos lo requiera por su complejidad, escala o riesgos asociados al tratamiento de datos personales. El DPO o figura equivalente supervisará el cumplimiento, asesorará en evaluaciones de impacto y fungirá como punto de contacto con autoridades y titulares.

15.3 Funciones del delegado o responsable de privacidad

Las funciones del DPO o responsable designado podrán incluir:

- Supervisión del cumplimiento de esta política
- Coordinación de evaluaciones de impacto de privacidad cuando corresponda
- Revisión de contratos y acuerdos de procesamiento de datos
- Capacitación en privacidad para personal y equipos operativos
- Atención de consultas de titulares y autoridades
- Gestión de incidentes relacionados con datos personales

15.4 Independencia y confidencialidad

El responsable designado para supervisar privacidad actuará con independencia funcional y contará con autoridad suficiente para supervisar el cumplimiento de las obligaciones en materia de protección de datos. Asimismo, deberá actuar con confidencialidad respecto a la información a la que tenga acceso durante sus funciones.

15.5 Contacto para cumplimiento en privacidad

Para cualquier asunto relacionado con el cumplimiento de esta política o protección de datos personales, Quantum Terra pone a disposición el siguiente medio de contacto:

Correo institucional de cumplimiento y privacidad: **privacy@quantumterra.ai** | **quantum.terra@outlook.com**

Para efectos de contacto o ejercicio de derechos ARCO, el titular podrá dirigirse a cualquiera de los domicilios señalados en la Sección 0.2 bre “Representación Legal y Domicilios Oficiales”.

16. MODIFICACIONES DE LA POLÍTICA, VIGENCIA Y JURISDICCIÓN APLICABLE

Quantum Terra se reserva el derecho de actualizar o modificar esta Política Integral de Privacidad en cualquier momento con el fin de reflejar cambios regulatorios, operativos, contractuales, tecnológicos o de seguridad que resulten necesarios para mantener su cumplimiento y alineación con mejores prácticas internacionales.

16.1 Modificaciones de la política

Cualquier modificación sustancial a esta política será comunicada a través de los medios institucionales de Quantum Terra o, en su caso, mediante notificación directa a los titulares

o responsables involucrados cuando así lo exija la normativa aplicable. Versiones anteriores podrán ser conservadas para fines de trazabilidad documental o cumplimiento.

16.2 Entrada en vigor, vigencia y control de versiones

La presente Política Integral de Privacidad entra en vigor a partir del 14 de octubre de 2025, identificada como Versión 1.0, y permanecerá vigente hasta que sea sustituida o modificada formalmente mediante una nueva publicación aprobada por la Dirección Ejecutiva y el Comité de Cumplimiento de Quantum Terra GeoTech AI LLC.

Quantum Terra mantiene un sistema de gestión documental y control de versiones aplicable a esta Política, conforme a buenas prácticas de cumplimiento (accountability – GDPR art. 5.2). Dicho sistema incluye:

a) Versionado progresivo documental bajo esquema 1.0, 2.0, 3.0…, con registro de cambios sustantivos.
b) b) Historial de versiones disponible para auditoría, conservación normativa y trazabilidad interna.
c) c) Modelo de mejora continua, que permite actualizar este documento para reflejar:

- Reformas legales o regulatorias aplicables;
- Cambios operativos o tecnológicos significativos;
- Nuevas medidas de seguridad o control;
- Ajustes derivados de recomendaciones internas de cumplimiento o auditoría externa certificada.
- d) Revisión periódica mínima anual o en menor plazo si lo exige un cambio normativo o tecnológico relevante.
- e) Notificación institucional a clientes y titulares de datos cuando existan modificaciones sustanciales que afecten el alcance del tratamiento o los derechos del titular, conforme al principio de transparencia.

Quantum Terra se reserva el derecho de modificar esta Política para mantener coherencia con estándares internacionales de cumplimiento, incluyendo GDPR, CPRA, LFPDPPP México y demás normativa aplicable en las jurisdicciones donde opera, sin perjuicio de los derechos adquiridos por los titulares.

16.3 Subsistencia del tratamiento

La revocación del consentimiento o la terminación de la relación contractual no afecta la legitimidad de tratamientos realizados con anterioridad ni impide la conservación de datos cuando exista obligación legal o contractual que lo requiera, conforme a lo dispuesto en esta política.

16.4 Jurisdicción aplicable

En caso de controversia, interpretación o ejecución derivada de este documento, será aplicable la legislación correspondiente a la jurisdicción en la que opere la entidad de Quantum Terra que actúe como responsable del tratamiento. Cuando exista conflicto internacional de leyes, se aplicarán principios de cooperación regulatoria y solución racional de conflictos conforme a buenas prácticas de protección de datos.

ANEXO A

MATRIZ DE FINALIDADES Y BASES JURÍDICAS DEL TRATAMIENTO

El presente Anexo forma parte integral de la Política Integral de Privacidad de **Quantum Terra GeoTech AI LLC** y detalla las **finalidades específicas del tratamiento de datos personales**, así como la **base jurídica aplicable** para cada operación de tratamiento, conforme al artículo 6 del **GDPR**, Sección 1798.100 de la **CPRA** y marco jurídico mexicano aplicable.

Nota de autoridad legal: Quantum Terra no realiza tratamientos sin fundamento jurídico válido y documentado. Ninguna finalidad se ejecuta sin base legal. *(Ver Sección 2 de esta Política).*

TABLA DETALLADA DE FINALIDADES Y BASES DE TRATAMIENTO

Nº	Finalidad del Tratamiento	Base Jurídica (GDPR)	Equivalente CPRA	Justificación Operativa
1	Gestión de relación contractual con clientes corporativos	Art. 6(1)(b) – Ejecución de contrato	Business Purpose	Necesario para ejecutar servicios contratados
2	Administración de cuentas, facturación y cobranza	Art. 6(1)(b) / 6(1)(c)	Service Provider Exception	Obligación derivada de contrato
3	Validación de identidad y autenticación en plataformas	Art. 6(1)(f) – Interés legítimo	Security & Fraud Prevention	Seguridad operativa
4	Soporte técnico y resolución de incidentes	Art. 6(1)(b)	Business Operations	Necesario para continuidad de servicio
5	Operación de infraestructura cloud y GIS	Art. 6(1)(f)	Service Provider Use	Necesidad técnica
6	Registro y trazabilidad operativa (logs)	Art. 6(1)(f)	Security Monitoring	Seguridad por diseño
7	Prevención de fraude o accesos no autorizados	Art. 6(1)(f)	Cybersecurity Protection	Obligación de seguridad
8	Comunicación con clientes sobre servicio contratado	Art. 6(1)(b)	Business Communication	Relación empresarial
9	Cumplimiento de obligaciones legales o regulatorias	Art. 6(1)(c)	Legal Compliance	Requerimientos fiscales o de autoridad
10	Gestión de proveedores y subcontratistas	Art. 6(1)(f)	Contract Execution	Relaciones operativas
11	Operaciones internas estadísticas o de mejora	Art. 6(1)(f)	Internal Analytics	Optimización de calidad

12	Tratamiento de datos geoespaciales para proyectos	Art. 6(1)(b) / 6(1)(f)	Contractual / Service Provider	Finalidad contractual
13	Evaluación de candidatos y reclutamiento	Art. 6(1)(b) / 6(1)(a)	Employment Purpose	Procesos de talento
14	Cumplimiento de solicitudes ARCO / GDPR	Art. 6(1)(c)	Consumer Rights Response	Obligación legal
15	Notificaciones de cambios de política	Art. 6(1)(c) / 6(1)(f)	Regulatory Transparency	Cumplimiento de información
16	Marketing legítimo no intrusivo	Art. 6(1)(a) – Consentimiento	Opt-in Required	Solo con autorización
17	Uso de datos anonimizados para analítica	Fuera de GDPR (Recital 26)	No Personal Data	Sin impacto en privacidad

CATEGORÍAS DE DATOS UTILIZADOS POR FINALIDAD

Finalidad	Categorías de Datos Utilizados
Gestión operativa	Identificación, contacto, empresa, puesto
Plataforma	Datos técnicos, registros de acceso
GIS/geoespacial	Datos de ubicación vinculados bajo contrato
Facturación	Datos fiscales, financieros corporativos
Soporte técnico	Logs, telemetría, ID de usuario
Seguridad	Identificadores y registros de actividad
Reclutamiento	CV, trayectoria profesional, contacto
Marketing	Solo correo corporativo (si aplica y con consentimiento)

LEGITIMIDAD POR INTERÉS LEGÍTIMO (DOCUMENTO CONEXO)

Para finalidades basadas en **interés legítimo**, Quantum Terra realiza un **Test de Interés Legítimo (LIA)** documentado conforme a criterio GDPR.

El Test de Interés Legítimo está disponible para revisión en caso de auditoría o solicitud legal fundada (ver Sección 2.3 y Anexo F).

REGLAS DE CONSENTIMIENTO

- El consentimiento solo se solicita cuando **no aplica otra base jurídica válida**.
- En operaciones de contrato **NO se pide consentimiento**.
- Para marketing opcional, se requiere **opt-in**.
- Consentimiento registrado con: IP, timestamp, versión, hash legal.

Contacto para dudas sobre bases legales:

privacy@quantumterra.ai | quantum.terra@outlook.com

ANEXO B

POLÍTICA DE CONSERVACIÓN Y ELIMINACIÓN DE DATOS

El presente Anexo establece los **plazos de conservación** y **criterios de eliminación segura** aplicables a los datos personales tratados por **Quantum Terra GeoTech AI LLC**, conforme a los principios de **limitación temporal**, **minimización** y **responsabilidad proactiva**, establecidos en:

- Art. 5.1(e) del **GDPR** (limitación del plazo de conservación)
- Sección 1798.105 de la **CPRA** (derecho de supresión)
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares (México) y el marco regulatorio digital aplicable en 2025

Quantum Terra retendrá datos personales únicamente durante el tiempo necesario para cumplir con las **finalidades legítimas** informadas y **obligaciones contractuales o legales** correspondientes.

B.1 Principios de conservación aplicados

Quantum Terra conserva los datos conforme a los siguientes principios:

Principio	Aplicación
Necesidad	Se conserva solo lo estrictamente requerido
Proporcionalidad	Se limita por finalidad específica
Legalidad	Se conserva cuando existe obligación legal
Seguridad	Durante conservación se aplican controles técnicos
Documentación	Se mantiene registro de supresión y retención

Eliminación efectiva	Supresión segura al concluir finalidad

B.2 Plazos generales de conservación

Los siguientes plazos aplican como guía corporativa estándar, salvo que exista contrato específico o disposición legal que establezca un término diferente:

Tipo de datos	Plazo de conservación	Fundamento
Datos de clientes corporativos (contacto, relación comercial)	Mientras dure la relación contractual + 5 años	Cumplimiento legal/defensa de reclamaciones
Facturación e información fiscal	5 a 10 años	Obligación fiscal/contable
Logs técnicos y telemetría de sistemas	6 a 24 meses	Seguridad y continuidad operativa
Datos de soporte técnico	Hasta resolución del caso + 6 meses	Finalidad estrictamente operativa
Datos geoespaciales personales	Conservación mínima necesaria según proyecto	Minimización reforzada (Sección 5)
Información contractual y legal	Vigencia contractual + 5 años	Defensa jurídica
Reclutamiento (candidatos)	12 meses	Base legítima – procesos internos
Comunicación comercial opcional	Hasta revocación del consentimiento	Derecho de oposición/cancelación

B.3 Criterios especiales para datos geoespaciales

Dado que Quantum Terra trata **datos geoespaciales personales** en algunos proyectos, aplica medidas reforzadas:

- Retención limitada al **tiempo estrictamente necesario** para análisis operativo
- Enmascaramiento geográfico y reducción de precisión cuando aplique
- Eliminación temprana o anonimización inmediata cuando ya no sea requerido
- Prohibición de almacenamiento indefinido sin justificación documental
- Supervisión del Oficial de Protección de Datos para excepciones

B.4 Métodos de eliminación segura

Quantum Terra aplica procesos auditables de supresión:

Método	Aplicación
Eliminación lógica	Bloqueo + depuración controlada de registros internos
Eliminación física	Destrucción total de dispositivos que contengan información
Anonimización	Eliminación irreversible de vínculo identificable
Sobrescritura segura	Procedimiento técnico (overwrite) en repositorios
Eliminación certificada	Bajo lineamientos NIST SP 800-88

B.5 Conservación para efectos legales

Quantum Terra podrá conservar información más allá del plazo operativo cuando:

- Exista **obligación legal** de conservación
- Sea necesaria para defensa de derechos legales ante controversia
- Se encuentre bajo **requerimiento de autoridad competente**

B.6 Suspensión de eliminación en caso de investigación

Cualquier solicitud de supresión se suspenderá temporalmente cuando:

- Los datos sean necesarios para **cumplimiento legal**
- Sean parte de **auditoría o controversia activa**
- Su eliminación implique incumplimiento de contrato o ley

B.7 Documentación de supresiones

Quantum Terra mantiene evidencia documental de procesos de eliminación, anonimización y depuración conforme a requerimientos de trazabilidad interna (**logs de supresión**).

Consultas relacionadas con conservación de datos:

privacy@quantumterra.ai | quantum.terra@outlook.com

ANEXO C

MEDIDAS TÉCNICAS Y ORGANIZATIVAS DE SEGURIDAD (MTO)

El presente Anexo forma parte integral de la **Política Integral de Privacidad de Quantum Terra GeoTech AI LLC** y establece las **medidas de seguridad técnicas, administrativas**

y organizativas adoptadas para proteger los datos personales tratados en el marco de sus operaciones corporativas, tecnológicas y de cumplimiento.

Estas medidas se aplican conforme a los principios de seguridad establecidos en los artículos 5 y 32 del **GDPR**, Sección 1798.150 de la **CPRA**, la **Ley Federal de Protección de Datos Personales en Posesión de los Particulares (México)** y el marco regulatorio digital vigente. Las medidas están alineadas con estándares internacionales incluyendo **ISO/IEC 27001, ISO/IEC 27002 y NIST Cybersecurity Framework (CSF)**.

C.1 Modelo de gestión de seguridad

Quantum Terra opera bajo un Sistema de Gestión de Seguridad de Información (SGSI) basado en riesgo, alineado a ISO/IEC 27001. Este modelo se estructura en:

1. Política de seguridad documentada y aprobada por dirección.
2. Evaluación de riesgos permanentes sobre información y sistemas.
3. Controles de seguridad diseñados bajo el principio de defensa en profundidad.
4. Gestión de vulnerabilidades y respuesta a incidentes.
5. Planes de continuidad operativa.
6. Supervisión continua y auditoría interna.

C.2 Medidas técnicas aplicadas

Las siguientes medidas son implementadas de forma obligatoria en entornos de operación de Quantum Terra:

Categoría	**Medidas aplicadas**
Protección de acceso	Autenticación multifactor (MFA), contraseñas seguras, bloqueo antiabuso
Gestión de identidades	Control de acceso basado en roles (RBAC), privilegio mínimo
Cifrado	Cifrado en tránsito (TLS/HTTPS) y en reposo (AES-256)
Redes	Firewalls, segmentación de entornos, aislamiento GIS sensible
Monitorización	Detección de intrusiones (IDS/IPS) y monitoreo SIEM
Desarrollo seguro	Revisión de código, pruebas estáticas y dinámicas
Seguridad en APIs	Tokens cifrados, protección anti inyección y rate limiting
Backups seguros	Replicación distribuida y restauración probada
Trazabilidad	Bitácoras de acceso e intervención técnica

C.3 Seguridad aplicada a proveedores tecnológicos (ESRI, AWS y otros)

Quantum Terra utiliza infraestructura tecnológica de proveedores certificados para garantizar resiliencia operativa y seguridad de datos. Estos proveedores actúan como **subencargados tecnológicos**, bajo contrato y supervisión conforme al artículo 28 del GDPR.

Infraestructura utilizada según proyecto:

Proveedor	Propósito técnico	Política de seguridad/privacidad
Amazon Web Services (AWS)	Infraestructura cloud, redes seguras	https://aws.amazon.com/security/
Esri (ArcGIS Enterprise/Online)	Gestión y análisis geoespacial	https://trust.arcgis.com
Microsoft Azure (si aplica)	Servicios de identidad, contenedores	https://learn.microsoft.com/security
Oracle Cloud (si aplica)	Bases de datos empresariales	https://www.oracle.com/cloud/security

El uso de estas plataformas:

- No implica transferencia de propiedad o explotación de datos.
- Se realiza bajo contratos de seguridad y protección de datos (DPA y SCC cuando aplique).
- Está sujeto a las medidas de confianza, seguridad y privacidad publicadas en los portales oficiales de cada proveedor.
- Se realiza bajo supervisión de cumplimiento de Quantum Terra, sin cesión de control.

C.4 Medidas organizativas y administrativas

Quantum Terra aplica controles organizacionales para reforzar la seguridad operacional:

- Capacitación obligatoria en protección de datos y ciberseguridad.
- Política de uso aceptable de recursos tecnológicos.
- Código interno de conducta y confidencialidad.
- Gestión de accesos basada en funciones autorizadas.
- Revisión periódica de roles y permisos.
- Procedimientos disciplinarios ante violaciones de seguridad.

C.5 Gestión de incidentes de seguridad

Quantum Terra mantiene un **Plan Corporativo de Respuesta a Incidentes** que incluye:

- Clasificación de incidentes por nivel de criticidad.
- Contención técnica inmediata.

- Mitigación de impacto.
- Notificación a clientes cuando proceda legalmente.
- En caso aplicable, notificación a autoridad conforme al GDPR art. 33.
- Trazabilidad y documentación del incidente.

C.6 Auditoría y supervisión

El cumplimiento del presente Anexo es verificable mediante auditorías internas y, cuando aplique contractualmente, auditorías externas. Quantum Terra podrá compartir evidencia de cumplimiento con clientes o autoridades cuando exista base jurídica o contrato que lo exija.

Contacto para asuntos de seguridad operativa:

privacy@quantumterra.ai | quantum.terra@outlook.com

ANEXO D

PROCEDIMIENTO PARA EJERCICIO DE DERECHOS DEL TITULAR (ARCO/GDPR/CPRA)

El presente Anexo describe el procedimiento mediante el cual los titulares de datos personales podrán ejercer sus derechos relacionados con el tratamiento de su información por parte de **Quantum Terra GeoTech AI LLC**, de conformidad con lo establecido en:

- Artículos 12 a 22 del **GDPR** (Derechos del interesado),
- Secciones 1798.100 a 1798.130 de la **California Privacy Rights Act (CPRA)**,
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares (México) y el marco regulatorio digital aplicable en 2025,
- Principios de transparencia y responsabilidad proactiva.

D.1 Derechos que pueden ejercerse

Todo titular podrá ejercer los siguientes derechos:

Derecho	Descripción
Acceso	Obtención de confirmación sobre si Quantum Terra trata sus datos personales y acceso a dicha información.
Rectificación	Corrección de datos inexactos o incompletos.
Supresión/Cancelación	Eliminación de datos cuando ya no sean necesarios o cuando proceda legalmente.
Oposición	Solicitud de cese de tratamiento por causa legítima.

Limitación del tratamiento	Restricción temporal del uso de datos.
Portabilidad	Solicitud de transferencia de datos a otro responsable en formato estructurado (cuando aplique).
Revocación de consentimiento	Cuando el tratamiento se base en consentimiento.
No ser objeto de decisiones automatizadas	Derecho a revisión humana cuando proceda legalmente.

D.2 Medios para ejercer derechos

Las solicitudes deberán enviarse mediante cualquiera de los siguientes medios oficiales:

Correo institucional de privacidad:

- privacy@quantumterra.ai

Copia operacional de respaldo:

- quantum.terra@outlook.com

Se deberá indicar en el asunto: **"Ejercicio de Derechos de Privacidad"**.

D.3 Contenido mínimo de la solicitud

Toda solicitud deberá contener lo siguiente:

1. Nombre completo del titular y datos de contacto.
2. Descripción clara del derecho que desea ejercer.
3. Identificación oficial o método de verificación de identidad.
4. En su caso, documentos que apoyen la procedencia de la solicitud.
5. Indicación del medio para recibir respuesta (correo electrónico).

Si la solicitud resulta incompleta, Quantum Terra podrá requerir información adicional en un plazo de **máximo 10 días hábiles**.

D.4 Plazos de respuesta

Requisito	Plazo
Acuse de recibo	Dentro de 5 días hábiles
Solicitudes incompletas, requerimiento de aclaración	Dentro de 10 días hábiles
Tiempo máximo de respuesta al titular	**30 días hábiles** a partir de solicitud completa
Posible extensión por complejidad	**15 días hábiles adicionales** (con aviso al titular)
Tiempo para ejecución de derecho aprobado	Hasta 15 días posteriores a resolución

Quantum Terra notificará la resolución por medio electrónico oficial. Cuando no proceda la solicitud, se informarán los motivos legales.

D.5 Procedencia y límites del ejercicio de derechos

Las solicitudes podrán **no proceder** cuando:

- El titular no acredite identidad;
- Exista obligación legal de conservación;
- El tratamiento sea necesario para defensa de derechos de Quantum Terra;
- La eliminación afecte intereses legítimos de terceros;
- Existan procesos legales pendientes que exijan conservación.

D.6 Costos

El ejercicio de derechos será gratuito. Sin embargo, en caso de solicitudes excesivas o injustificadas, Quantum Terra podrá aplicar un costo administrativo razonable permitido por ley.

D.7 Medios de respuesta

- Respuesta directa vía correo electrónico institucional.
- Adjuntos con datos portables en CSV, JSON o PDF cuando aplique.
- Acreditación documental en caso de rectificación o cancelación.

D.8 Autoridad competente

En caso de discrepancia, el titular podrá acudir ante:

- Autoridad de protección de datos de la Unión Europea (si aplica),
- **California Privacy Protection Agency (CPPA)**,
- **Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos (INAI) – México**.

D.9 Transparencia

Quantum Terra mantiene registro documental de cada solicitud recibida, su análisis, resolución y acciones ejecutadas, conforme al principio de responsabilidad proactiva.

Correos oficiales para ejercicio de derechos:

privacy@quantumterra.ai | quantum.terra@outlook.com

ANEXO E

AVISOS DE PRIVACIDAD POR CAPAS (MULTICAPA)

El presente Anexo establece la estructura de avisos de privacidad por capas utilizada por Quantum Terra GeoTech AI LLC, conforme al principio de transparencia y comunicación

progresiva previsto en los artículos 12 y 13 del GDPR, así como en la CPRA y la legislación mexicana.

Quantum Terra utiliza un modelo de aviso de privacidad en tres niveles (“multicapa”), el cual permite informar de forma adecuada y gradual a los titulares dependiendo del contexto de tratamiento.

E.1 Objetivo del modelo de transparencia por capas

Capa	Finalidad
Capa 1 – Aviso Corto	Información esencial durante la recolección inicial
Capa 2 – Aviso Intermedio	Contexto ampliado para decisiones informadas
Capa 3 – Aviso Integral	Texto completo con cláusulas legales (esta política)

E.2 Capa 1 – Aviso de Privacidad Breve (pantallas de formulario / web / app)

Uso: páginas de contacto, registro de cuenta, alta de usuarios en plataforma o demos corporativos.

Ejemplo oficial de Quantum Terra (texto editable):

Quantum Terra recopila datos personales para finalidades operativas, de soporte técnico y administración de cuentas. El tratamiento se realiza conforme a nuestra Política Integral de Privacidad disponible en **https://quantumterra.ai/privacy**. Para más información o ejercer sus derechos de acceso, rectificación, oposición o portabilidad, escriba a privacy@quantumterra.ai. Al continuar, usted acepta el tratamiento conforme a las finalidades descritas.

E.3 Capa 2 – Aviso de Interacción Operativa (modal de aceptación con registro)

Uso: despliegue obligatorio en plataformas tecnológicas internas o acceso a servicios protegidos.

Ejemplo oficial de aviso operativo:

Al continuar utilizando esta plataforma, usted acepta el tratamiento de sus datos personales para administración de acceso, trazabilidad operativa, seguridad de sistemas y cumplimiento contractual. Quantum Terra podrá hacer uso de subencargados tecnológicos (incluyendo AWS y Esri) bajo cláusulas de privacidad y seguridad equivalentes. Más información en: **https://quantumterra.ai/privacy.**

Debe marcar para continuar:

[ ] He leído y acepto el Aviso de Privacidad.

E.4 Capa 3 – Aviso Integral

Corresponde al contenido completo de este documento denominado “Política Integral de Privacidad de Quantum Terra GeoTech AI LLC” y describe los principios, obligaciones, finalidades, bases legales, transferencias internacionales, medidas de seguridad, derechos del titular y anexos vinculados.

E.5 Reglas de despliegue obligatorio

Quantum Terra aplica las siguientes reglas estándar de visibilidad en todos los canales digitales:

Obligación	Aplicación
Aviso visible permanente	Pie de página de sitios y plataformas
Acceso a política completa	Enlace directo obligatorio
Aceptación obligatoria	Formularios, registros, inicios de sesión
Prueba de aceptación	Registro de timestamp, IP, hash de consentimiento
Mecanismo de revocación	Enlace/solicitud disponible para titulares

E.6 Evidencia de consentimiento

El consentimiento se documenta mediante:

- Registro digital de aceptación
- Versionamiento del aviso aceptado
- Registro de huella técnica (IP, timestamp)
- Prueba legal admisible (hash documental)

Estos registros forman parte del expediente digital de cumplimiento y pueden ser solicitados para auditoría o defensa jurídica.

E.7 Conexión de cumplimiento

Este Anexo se articula con:

- Sección 0.8 – Aceptación obligatoria del aviso
- Sección 11 – Consentimiento y revocación
- Anexo H – Texto formal de aceptación del aviso

Para ajustes operativos o integración en frontend web/app:

privacy@quantumterra.ai | quantum.terra@outlook.com

ANEXO F

MECANISMOS DE TRANSFERENCIA INTERNACIONAL Y GARANTÍAS CONTRACTUALES (SCC/DPA)

Este Anexo establece los mecanismos que **Quantum Terra GeoTech AI LLC** aplica para realizar **transferencias internacionales de datos personales** de forma legal, segura y conforme al marco jurídico internacional aplicable, incluyendo:

- **GDPR (arts. 44–49)** para transferencias fuera del Espacio Económico Europeo
- **CPRA (Sección 1798.185)** – transferencia bajo obligaciones contractuales equivalentes
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares (México) y el marco regulatorio digital aplicable en 2025 además de las disposiciones sobre transferencia internacional
- **Principios de privacidad OCDE**

F.1 Formas de transferencia aplicadas por Quantum Terra

Tipo	Descripción
Transferencia controlada	Entre entidades del mismo grupo o proveedores tecnológicos autorizados
Transferencia funcional	Para ejecutar contratos con clientes o servicios operativos
Transferencia legal	Solicitada por autoridad competente conforme a ley aplicable

F.2 Fundamento de transferencia y legitimidad

Toda transferencia internacional realizada por Quantum Terra debe:

1. Tener **base jurídica válida** documentada (Art. 6 GDPR y equivalentes en CPRA y México).
2. Estar **justificada por finalidad contractual o de servicio**.
3. **Garantizar nivel adecuado de protección** para el titular.
4. Usar mecanismos legales aceptados internacionalmente.

F.3 Garantías utilizadas para transferencias internacionales

Quantum Terra aplica uno o más de los siguientes mecanismos según el caso:

Escenario	Garantía de transferencia aplicada
Transferencias UE–USA	**Cláusulas Contractuales Estándar (SCC) – Comisión Europea**

Transferencias América–UE	**DPA + Contrato de transferencia**
Transferencias Latinoamérica	**Consentimiento contractual + DPA**
Países sin normativa adecuada	**Binding Contractual Clauses + Evaluación de Impacto TI**

F.4 Data Processing Agreement (DPA)

Todo intercambio de datos con clientes corporativos, proveedores tecnológicos o subencargados está sujeto a la firma de un **DPA – Data Processing Agreement**, el cual incluye:

- Obligación de confidencialidad
- Limitación de finalidad
- Prohibición de reutilización no autorizada
- Medidas de seguridad (ISO/IEC 27001 – NIST)
- Eliminación o devolución de datos al finalizar relación
- Prohibición de subtransferencia sin autorización de Quantum Terra

F.5 Cláusulas Contractuales Estándar (SCC)

En transferencias hacia jurisdicciones sin "decisión de adecuación", Quantum Terra utiliza:

- **SCC Módulo 1**: Responsable → Responsable
- **SCC Módulo 2**: Responsable → Encargado
- **SCC Módulo 3**: Encargado → Encargado (*usual en casos cloud/GIS*)

Estas cláusulas aseguran continuidad de protección y responsabilidad contractual frente a terceros.

F.6 Auditoría y documentación de transferencias

Quantum Terra mantiene evidencia documental de:

- Contratos con cláusulas SCC
- Listado de subencargados autorizados
- Evaluaciones de impacto de transferencia (cuando aplica)
- Registros de transferencia (logs)
- Notificaciones exigidas por autoridad cuando corresponda

F.7 Transferencias con proveedores autorizados (AWS / Esri y otros)

Las transferencias derivadas del uso de **servicios cloud o GIS** se limitan a funciones estrictamente técnicas. Todo proveedor actúa como **subencargado** y queda jurídicamente obligado mediante DPA.

Consultas de cumplimiento y privacidad:

Proveedor	Política de transferencia/privacidad
Amazon Web Services (AWS)	https://aws.amazon.com/privacy
Esri ArcGIS	https://www.esri.com/en-us/privacy/overview
Microsoft Azure (si aplica)	https://privacy.microsoft.com
Oracle Cloud (si aplica)	https://www.oracle.com/legal/privacy

F.8 Transparencia y derecho del titular

Los titulares podrán solicitar información sobre transferencias realizadas respecto a sus datos personales mediante solicitud al canal oficial:

privacy@quantumterra.ai | **quantum.terra@outlook.com**

ANEXO G

LISTA DE SUBENCARGADOS AUTORIZADOS Y NOTIFICACIÓN DE ACTUALIZACIONES

En cumplimiento de la obligación de transparencia establecida en el **artículo 28 del GDPR**, Sección 1798.140(h) de la **CPRA**, y la normativa mexicana aplicable, Quantum Terra mantiene una **lista formal de subencargados autorizados** para el tratamiento de datos personales en funciones técnicas necesarias para la operación de servicios.

Queda estrictamente prohibido a cualquier tercero acceder o tratar datos personales sin haber sido previamente autorizado mediante contrato y registro en esta lista.

G.1 Lista modelo de subencargados autorizados

La siguiente es la **lista operativa base de subencargados tecnológicos** utilizados por Quantum Terra, la cual puede actualizarse según requerimientos de operación o infraestructura:

Nº	Subencargado	País o Región de Procesamiento	Finalidad Operativa	Garantías de Protección
1	Amazon Web Services (AWS)	EE. UU. / Región Global	Infraestructura cloud, almacenamiento cifrado	DPA + SCC + ISO/IEC 27001
2	Esri Inc.	EE. UU. / EU	Plataforma GIS y análisis geoespacial	DPA + Política Trust Center

3	Microsoft Azure (cuando aplica)	EE. UU. / EU	Identidad y continuidad operativa	DPA + SCC + cifrado
4	Oracle Cloud (si aplica)	EE. UU. / EU	Bases de datos corporativas	DPA + SOC 2
5	Cloudflare (si aplica)	Global	Protección de red / firewall / CDN	Modelo Zero Trust

Nota: Esta lista es indicativa y puede ajustarse dependiendo de los requerimientos específicos del proyecto contratado. Para conocer la lista vigente, el cliente o titular deberá solicitarla formalmente mediante correo institucional.

G.2 Principios aplicables

Todos los subencargados tecnológicos están sujetos a los siguientes principios contractuales obligatorios:

- **No adquisición de control ni derechos sobre los datos tratados.**
- **Prohibición de uso para fines propios o comerciales.**
- **Confidencialidad permanente y protección reforzada.**
- **Medidas de seguridad técnicas alineadas a ISO/IEC 27001 y NIST.**
- **Prohibición de subencargado en cadena sin autorización de Quantum Terra.**
- **Supresión obligatoria de datos al finalizar relación contractual.**

G.3 Procedimiento de actualización de subencargados

Quantum Terra podrá incorporar nuevos subencargados cuando sea necesario para la prestación del servicio. Para ello:

1. Evaluará riesgos y cumplimiento (Evaluación de Due Diligence del Proveedor).
2. Firmará un **Data Processing Agreement (DPA)** con obligaciones equivalentes.
3. Actualizará esta lista conforme al registro oficial.
4. **Notificará a clientes afectados** cuando el cambio impacte el procesamiento de datos personales.
5. Ofrecerá al cliente la posibilidad de **formular objeción razonable** si lo permite la relación contractual.

G.4 Solicitud formal de lista vigente

Clientes y titulares podrán solicitar la **lista actualizada de subencargados** mediante escrito libre a:

privacy@quantumterra.ai | **quantum.terra@outlook.com**

G.5 Conexión normativa

Este Anexo se vincula con:

- **Sección 6 – Transferencias Internacionales de Datos**
- **Sección 7 – Subencargados**
- **Anexo F – Cláusulas SCC/DPA**
- **Anexo I – Políticas AWS/Esri**

ANEXO H

AVISO DE PRIVACIDAD CORTO Y CLÁUSULA DE ACEPTACIÓN OBLIGATORIA

El presente Anexo contiene el **modelo oficial de Aviso de Privacidad Breve** y la **cláusula de consentimiento expreso** que deberá utilizarse en plataformas digitales, formularios, contratos electrónicos y demás interfaces operadas por **Quantum Terra GeoTech AI LLC**.

H.1 Aviso de Privacidad Corto (uso web/formularios)

Este aviso se despliega en **formularios de captura**, **registros de usuarios**, **portales operativos** y **pantallas de autenticación**:

Aviso de Privacidad – Resumen Operativo

Quantum Terra GeoTech AI LLC trata datos personales para finalidades relacionadas con administración de cuentas, autenticación de acceso, operación de servicios contratados, soporte técnico, trazabilidad operativa y medidas de seguridad. Para conocer información completa sobre el tratamiento de datos personales, transferencias internacionales, ejercicio de derechos y medidas de seguridad implementadas, consulte la Política Integral de Privacidad disponible en:

https://quantumterra.ai/privacy

Para ejercer sus derechos de acceso, rectificación, oposición, portabilidad o revocación del consentimiento, comuníquese a **privacy@quantumterra.ai**.

H.2 Cláusula de Consentimiento Obligatorio (captura verificable)

Cláusula de Aceptación

[ ] He leído y acepto el contenido del Aviso de Privacidad y autorizo el tratamiento de mis datos personales conforme a las finalidades descritas.

Fecha y hora: _____

IP/Origen: _____

Versión aceptada: Política de Privacidad v____

Este modelo se aplica con registro digital para mantener evidencia de cumplimiento legal en caso de auditoría o verificación normativa.

H.3 Prueba de consentimiento – Evidencia legal

Quantum Terra conservará evidencia documental de aceptación para cumplimiento y trazabilidad, mediante:

- Sellado digital de aceptación (timestamp)
- Registro técnico (IP, agente de dispositivo)
- Identificador único de consentimiento por usuario
- Versión legal aceptada (historial versionado)
- Almacenamiento seguro para fines de evidencia jurídica

H.4 Revocación del consentimiento

Cuando el tratamiento se base en consentimiento (Ver Sección 11), el titular podrá revocarlo en cualquier momento enviando solicitud por los canales oficiales:

privacy@quantumterra.ai

quantum.terra@outlook.com

H.5 Integración obligatoria en sistemas

Este aviso debe integrarse técnicamente en:

Medio	Obligatorio
Portal web institucional	Sí
Panel de acceso a servicios	Sí
Formularios de registro	Sí
Plataformas internas y SaaS	Sí
Aplicaciones móviles o API privadas	Sí
Puntos de recopilación comercial	Sí

H.6 Conexión normativa y documental

Este Anexo se vincula con:

- **Sección 0.8** – Aceptación obligatoria del aviso
- **Sección 11** – Consentimiento y revocación
- **Anexo E** – Aviso de Privacidad por Capas
- **Anexo F** – Garantías de transferencia

ANEXO I

POLÍTICAS DE PRIVACIDAD Y SEGURIDAD DE PROVEEDORES TECNOLÓGICOS (AWS, ESRI Y OTROS)

Este Anexo proporciona **referencia documental oficial** a las políticas de privacidad, tratamiento de datos, cumplimiento normativo y estándares de seguridad de los **proveedores tecnológicos utilizados por Quantum Terra GeoTech AI LLC** en calidad de **subencargados de tratamiento**, conforme al artículo 28 del GDPR, la CPRA y la legislación mexicana aplicable.

La integración de estos proveedores se realiza únicamente bajo:

- Contratos de procesamiento de datos (**DPA – Data Processing Agreement**),
- Cláusulas contractuales de transferencia (**SCC** cuando aplica),
- Modelo de seguridad documentado (**MTO – Medidas Técnicas y Organizativas**),
- Supervisión de cumplimiento a cargo de Quantum Terra.

I.1 Relación jurídica con proveedores

Quantum Terra utiliza herramientas e infraestructura tecnológica de estos proveedores **en calidad de cliente corporativo bajo licenciamiento**, no como socio comercial, reseller o representante. En consecuencia:

- Dichos proveedores **no tienen autorización para usar los datos tratados con fines propios**.
- **No existe cesión ni transferencia de propiedad** de los datos personales manejados.
- Quantum Terra **mantiene el control del tratamiento** en todo momento.
- Los proveedores actúan **únicamente como subencargados tecnológicos** dentro de una relación de servicio.

I.2 Políticas oficiales de proveedores tecnológicos

Proveedor	Tipo de Servicio	Política de Privacidad Oficial	Seguridad y Cumplimiento
Amazon Web Services (AWS)	Infraestructura cloud, hosting y cómputo escalable	https://aws.amazon.com/privacy/	https://aws.amazon.com/compliance/
Esri (ArcGIS Platform)	Procesamiento GIS, mapas, análisis espacial	https://www.esri.com/en-us/privacy/overview	https://trust.arcgis.com
Microsoft Azure	Identidad, cloud híbrida,	https://privacy.microsoft.com	https://learn.microsoft.com/azure/security

(cuando aplica)	servicios AI		
Oracle Cloud *(cuando aplica)*	Bases de datos, nube empresarial	https://www.oracle.com/legal/privacy/	https://www.oracle.com/corporate/security-practices/
Cloudflare *(cuando aplica)*	Seguridad de red, firewall, mitigación DDoS	https://www.cloudflare.com/privacypolicy/	https://www.cloudflare.com/trust-hub/

I.3 Cumplimiento normativo garantizado

Todos los proveedores tecnológicos utilizados deben acreditar como mínimo:

- Certificaciones **ISO/IEC 27001, SOC 2 o equivalentes**
- Seguridad en infraestructura **cloud** con cifrado de datos
- Política de protección de datos compatible con **GDPR**
- Mecanismos de gobernanza y respuesta a incidentes
- Programas de continuidad operativa (**BCP/DRP**)
- Soporte para auditoría o solicitud de información legal

I.4 Seguimiento y actualización

El listado de proveedores tecnológicos es dinámico y puede ser actualizado en función de nuevas necesidades de arquitectura, soporte o continuidad operativa. Toda modificación:

1. Será evaluada mediante **análisis de riesgo del proveedor**.
2. Se registrará en el **Listado de Subencargados Autorizados** (Anexo G).
3. Generará **notificación** a clientes si impacta tratamiento de datos personales.

I.5 Base normativa

Este Anexo se emite en cumplimiento de:

- Art. 28, 44–49 del **GDPR**
- Sección 1798.140(h) de la **CPRA**
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares (México) y el marco regulatorio digital aplicable en 2025
- Principios **OCDE** para protección de datos

Para consulta o aclaración sobre este Anexo:

privacy@quantumterra.ai | quantum.terra@outlook.com