

MANUAL CORPORATIVO

Manual de seguridad de la información y protección de datos

Aplicable a diseño web y gráfico, correo corporativo y desarrollo de sistemas a medida.

Código del documento	GMS-MSI-001
Versión	1.0 · Edición para clientes
Fecha de emisión	15 de octubre de 2026
Titular	GEOMASTERSOLUTIONS S.A.S. · RUC 2293523072001
Responsable del documento	Lázaro Rafael Batule Águila · Representante Legal y Responsable Técnico
Contacto	info@geomastersolutions.com

Este documento describe las políticas y procedimientos de seguridad de GEOMASTERSOLUTIONS S.A.S. No contiene contraseñas, registros de clientes ni detalles que permitan acceder a sistemas. Las evidencias técnicas de configuración, pruebas y acuerdos se conservan en un expediente separado con acceso restringido y se comparten con cada cliente en lo que le concierne.

Control del documento

Versión	Fecha	Descripción del cambio	Estado
0.9	1 oct 2026	Borrador interno de trabajo: levantamiento de prácticas y procedimientos.	Sustituida
1.0	15 oct 2026	Edición para clientes: políticas y procedimientos vigentes de seguridad de la información y protección de datos personales.	Vigente

Función	Nombre	Cargo	Fecha
Elaboró	Lázaro Rafael Batule Águila	Responsable Técnico	1 oct 2026
Revisó	Lázaro Rafael Batule Águila	Representante Legal	10 oct 2026
Aprobó	Lázaro Rafael Batule Águila	Representante Legal	15 oct 2026

Este manual se revisa al menos una vez al año y tras cambios relevantes en los servicios, la normativa o la infraestructura. Cada nueva versión indica quién la aprobó, cuándo entra en vigor y qué documentos sustituye; las versiones anteriores y el historial de cambios se conservan.

Sobre este documento

El manual recoge las políticas que GEOMASTERSOLUTIONS S.A.S. aplica para proteger la información propia y la de sus clientes, quién responde por su manejo y cómo se actúa ante solicitudes e incidentes. Está concebido para todos los clientes de la empresa; las condiciones particulares de cada servicio (alcance, accesos, instrucciones de tratamiento, plazos) se precisan por escrito en el acuerdo correspondiente.

Alcance y valor del documento

La información operativa de este manual procede de la organización interna de GEOMASTERSOLUTIONS S.A.S. y de la normativa ecuatoriana de protección de datos personales. El manual no constituye por sí mismo una certificación de seguridad ni un dictamen de cumplimiento legal; los compromisos contractuales con cada cliente prevalecen sobre las reglas generales aquí descritas cuando sean más exigentes.

Contenido

1	Introducción.....	4
2	Organización y responsabilidades.....	7
3	Proveedores y servicios tecnológicos.....	8
4	Medidas de seguridad.....	9
5	Gestión de accesos y desarrollo seguro.....	10
6	Respaldos, conservación y continuidad.....	11
7	Atención de incidentes de seguridad.....	12
8	Privacidad y relación con terceros.....	13
9	Registros, revisión y mejora continua.....	14
10	Aprobación y referencias.....	15

1 Introducción

1.1 Propósito

Definir cómo GEOMASTERSOLUTIONS S.A.S. protege la información de la empresa y de sus clientes, quién responde por su manejo y qué procedimientos se aplican en la prestación de los servicios de diseño web y gráfico, correo corporativo y desarrollo de sistemas a medida.

1.2 Alcance

El manual comprende los datos personales, archivos de diseño, código fuente, sitios web, bases de datos, credenciales y documentos de negocio utilizados en la prestación de los servicios. Alcanza también los equipos de trabajo, el teléfono utilizado con clientes y los proveedores tecnológicos contratados.

1.3 Marco normativo

En Ecuador la protección de datos personales es un derecho constitucional (artículo 66, numeral 19, de la Constitución), tutelado además por la acción de hábeas data (artículo 92). La Ley Orgánica de Protección de Datos Personales (LOPDP), vigente desde mayo de 2021, desarrolla ese derecho; su régimen sancionador está en plena vigencia desde el 26 de mayo de 2023 y su Reglamento General se expidió mediante Decreto Ejecutivo 904, en noviembre de 2023. La Superintendencia de Protección de Datos Personales (SPDP) es la autoridad de control.

Las políticas de este manual responden a las siguientes normas:

Norma	Qué establece	Dónde lo aplica este manual
Constitución de la República (arts. 66.19 y 92)	Derecho a la protección de datos personales y acción de hábeas data.	Reconocimiento de los derechos del titular (8.1).
LOPDP [1]	Principios de finalidad, pertinencia, minimización, seguridad y confidencialidad; derechos de los titulares con respuesta en 15 días; roles de responsable y encargado; medidas de seguridad; notificación de vulneraciones a la autoridad, al responsable y a los titulares; sanciones de hasta el 1 % del volumen de negocio.	Principios (1.4), roles (2.3), medidas de seguridad (4), incidentes (7) y derechos (8.1).
Reglamento General a la LOPDP, Decreto Ejecutivo 904 [2]	Contenido del contrato entre responsable y encargado, asistencia al responsable y obligaciones de registro.	Contratos y encargo (8.2) y registros (9.1).
Resolución SPDP 2025-0006 [3]	Cláusulas de protección de datos que deben incluirse en los contratos.	Acuerdos de servicio (8.2).
Normativa tributaria del SRI [4]	Conservación de comprobantes electrónicos durante 7 años.	Reglas de conservación (6.2).
Código Orgánico Integral Penal (arts. 229 y 234)	Tipifica la revelación ilegal de bases de datos y el acceso no consentido a sistemas informáticos.	Clasificación de la información (1.7) y gestión de accesos (5).

Alcance del marco normativo

Este manual organiza las medidas con las que GEOMASTERSOLUTIONS atiende esas obligaciones y facilita al cliente la información que necesita para sus propios registros y evaluaciones. No sustituye la asesoría jurídica de cada parte ni certifica el cumplimiento de la LOPDP.

1.4 Principios

Las reglas de este manual se derivan de seis principios que orientan cualquier decisión no prevista expresamente:

Principio	Qué significa en la práctica
Mínimo privilegio	Cada acceso se concede con el menor permiso necesario, de forma individual y por el tiempo que dure la intervención.
Minimización	Solo se recogen, conservan y comparten los datos necesarios para la finalidad documentada.
Separación de datos	La información de cada cliente se mantiene separada; nunca se reutiliza para otro cliente ni para publicidad.
Verificación	Las solicitudes sensibles (contraseñas, pagos, dominios, bases de datos) se confirman por un canal conocido antes de actuar.
Trazabilidad	Las decisiones, entregas y pruebas se registran con fecha, sin copiar secretos ni datos personales innecesarios.
Transparencia	El cliente conoce qué datos se tratan, dónde, con qué proveedores y durante cuánto tiempo, y es informado sin demora ante cualquier incidente.

1.5 Compromisos con nuestros clientes

- Tratar la información del cliente únicamente para la finalidad y bajo las instrucciones acordadas por escrito.
- Proteger todas las cuentas y repositorios con verificación en dos pasos y custodiar las credenciales en un gestor seguro.
- Mantener respaldos automáticos con un período mínimo de conservación de 90 días y probar periódicamente su recuperación.
- Comunicar cualquier incidente de seguridad que afecte al cliente en las primeras 24 horas desde su detección y dentro de los plazos legales.
- Atender las solicitudes de derechos de los titulares en un máximo de 15 días calendario.
- Devolver o eliminar la información del cliente al cierre del servicio, con constancia escrita.
- Entregar al cliente, cuando lo solicite, las evidencias pertinentes de los controles aplicados a su servicio.

1.6 Términos y definiciones

Término	Definición en este manual
LOPD	Ley Orgánica de Protección de Datos Personales del Ecuador y su Reglamento General [1, 2].
SPDP	Superintendencia de Protección de Datos Personales, autoridad de control en Ecuador.
ARCOTEL	Agencia de Regulación y Control de las Telecomunicaciones; destinataria de determinadas notificaciones de vulneración.
Titular	Persona natural a la que se refieren los datos personales.
Responsable del tratamiento	Quien decide sobre la finalidad y el tratamiento de los datos. GEOMASTERSOLUTIONS lo es respecto de sus propios contactos, clientes y facturación.

Término	Definición en este manual
Encargado del tratamiento	Quien trata datos por cuenta y bajo instrucciones de un responsable. GEOMASTERSOLUTIONS actúa como encargado al alojar, respaldar o mantener sistemas de un cliente.
Verificación en dos pasos (2FA)	Segundo factor de autenticación adicional a la contraseña (aplicación, código o llave) exigido para acceder a una cuenta.
Incidente de seguridad	Evento que compromete, o puede comprometer, la confidencialidad, integridad o disponibilidad de la información. Una vulneración de datos personales es un incidente con efectos sobre titulares.
RPO / RTO	Pérdida de datos tolerable (RPO) y tiempo objetivo de recuperación (RTO) acordados con el cliente para cada servicio.
Evidencia	Configuración, registro, acuerdo o prueba fechada que demuestra que un control existe y funciona.

1.7 Clasificación de la información

Toda la información se clasifica en uno de cuatro niveles, que determinan cómo se maneja:

Nivel	Ejemplos	Regla de manejo
Pública	Contenido autorizado para publicación	Se publica solo con autorización y revisión del contenido.
Interna	Planificación y documentación operativa	Su distribución se limita a la necesidad del servicio.
Confidencial	Datos personales, contratos, código fuente y respaldos	Acceso autorizado, finalidad definida y envío solo al destinatario verificado.
Restringida	Contraseñas, claves API y códigos de recuperación	Gestor o almacén seguro; nunca se incluyen en informes, código, capturas ni mensajes compartidos.

2 Organización y responsabilidades

2.1 Organización

La administración de la seguridad de la información está centralizada en Lázaro Rafael Batule Águila, representante legal de GEOMASTERSOLUTIONS S.A.S., quien actúa además como responsable técnico. En su calidad de representante legal aprueba las políticas y los recursos; como responsable técnico administra los servicios, los respaldos, las actualizaciones y la atención de incidentes y solicitudes.

La necesidad de designar un delegado de protección de datos y las obligaciones de registro se evalúan periódicamente según los tratamientos realizados, su escala y la normativa vigente.

2.2 Matriz de responsabilidades

Rol	Responsabilidades
Representante legal	Aprueba el manual, las políticas y los recursos. Firma los acuerdos de servicio, confidencialidad y encargo de tratamiento. Decide las notificaciones a autoridades y titulares.
Responsable técnico	Administra accesos, respaldos, actualizaciones y publicación. Ejecuta el procedimiento de incidentes y atiende solicitudes de titulares. Mantiene el expediente de evidencias y los registros.
Cliente	Designa a las personas autorizadas para solicitar cambios y recibir accesos. Da instrucciones de tratamiento por escrito, aprueba lo que se publica y decide la devolución o eliminación de su información al cierre.
Proveedor tecnológico	Presta infraestructura o servicios bajo condiciones contractuales documentadas. Sus condiciones, región de datos y garantías se registran antes de confiarle datos de clientes.

2.3 Datos propios y datos de clientes

Para consultas, contratación y facturación propias, GEOMASTERSOLUTIONS determina cómo usa los datos de sus contactos y actúa como responsable del tratamiento. Al alojar, respaldar o mantener sistemas por instrucciones de un cliente, actúa como encargado del tratamiento. El rol concreto, la finalidad y las instrucciones se documentan por escrito para cada servicio [1, 2].

Los datos tratados comprenden nombres, teléfonos, correos y datos de facturación de contactos propios, además de datos de usuarios, empleados o compradores dentro de los sistemas de clientes. Antes de incorporar un nuevo proyecto se verifica qué categorías de datos contiene; el tratamiento de categorías especiales (salud, biometría, menores) requiere evaluación previa y acuerdo expreso con el cliente.

Uso exclusivo de la información del cliente

La información recibida de un cliente para soporte, alojamiento o desarrollo se utiliza exclusivamente para ese servicio. No se reutiliza para publicidad, análisis propios ni para otros clientes.

3 Proveedores y servicios tecnológicos

GEOMASTERSOLUTIONS se apoya en los siguientes proveedores y recursos para prestar sus servicios. Para cada servicio contratado se documenta la entidad proveedora, la región de los datos, las condiciones de tratamiento y los subproveedores, información que se facilita al cliente cuando la solicita.

Proveedor o recurso	Uso	Salvaguardas aplicadas
MXroute y Zoho Mail	Correo corporativo	Cuentas administradoras protegidas con verificación en dos pasos; buzones individuales por usuario.
Google Workspace y Microsoft 365	Correo corporativo	Cuentas administradoras protegidas con verificación en dos pasos; alcance contratado documentado por cliente.
Hostinger	Alojamiento de webs y sistemas	Verificación en dos pasos, HTTPS, separación entre proyectos y actualizaciones de seguridad periódicas.
Backblaze	Respaldos de equipos, webs, sistemas y bases de datos	Copias automáticas, verificación en dos pasos y conservación mínima de 90 días.
ZeptoMail	Envío de correos transaccionales desde la web de la empresa	Uso limitado a notificaciones de la web; registros conservados según la finalidad.
Google reCAPTCHA	Protección de formularios de la web	Uso limitado a la prevención de abuso en formularios.
Repositorios privados	Almacenamiento de código fuente	Repositorios privados por proyecto y verificación en dos pasos en todas las cuentas.
Gestor de contraseñas	Custodia de credenciales	Bóveda cifrada protegida con verificación en dos pasos y mecanismo de recuperación protegido.
Correo y WhatsApp	Comunicación con clientes	Solo con contactos autorizados; las credenciales se entregan según el procedimiento de la sección 5.2.
Herramientas de IA	Apoyo al trabajo técnico y de redacción	Solo con ejemplos ficticios o material sin datos personales ni información confidencial.

El régimen aplicable a cualquier flujo internacional de datos y las garantías exigibles al proveedor se determinan y documentan antes de confiarle datos de clientes, conforme a la normativa vigente de la SPDP.

4 Medidas de seguridad

Medidas técnicas y organizativas aplicadas por GEOMASTERSOLUTIONS en la prestación de sus servicios.

Área	Medida aplicada
Administración	Gestión centralizada de la información y de los accesos de clientes por el responsable técnico, con registro de cada acceso concedido.
Credenciales	Custodia en un gestor de contraseñas protegido con verificación en dos pasos. Nunca se almacenan en código, documentos o mensajes.
Cuentas de proveedores	Verificación en dos pasos activa en todas las cuentas de correo, alojamiento, respaldos y repositorios.
Código fuente	Repositorios privados por proyecto; las contraseñas, claves y copias de bases de datos se excluyen del código y de su historial.
Equipos de trabajo	Uso exclusivo para el trabajo; contraseña o PIN, bloqueo automático, cifrado de disco, antivirus y actualizaciones automáticas.
Teléfono y WhatsApp	Bloqueo de pantalla y verificación en dos pasos de WhatsApp.
Respaldos	Copias automáticas diarias o continuas de archivos de trabajo, webs, sistemas y bases de datos, con conservación mínima de 90 días.
Recuperación	Pruebas periódicas de recuperación de archivos y de sistemas con base de datos, con registro fechado de resultado.
Revisión de seguridad	Antes de publicar se revisan accesos, permisos, contraseñas expuestas, HTTPS y actualizaciones, con registro de lo comprobado.
Mantenimiento	Revisión e instalación mensual de actualizaciones de seguridad; los avisos críticos se atienden en cuanto se conocen.
Cierre del servicio	Retiro de accesos y eliminación de los archivos que ya no se necesitan; los respaldos expiran al vencer su plazo de conservación.
Inteligencia artificial	Uso restringido a ejemplos ficticios o material sin información confidencial ni datos personales.
Privacidad	Política de privacidad publicada y canal de atención info@geomastersolutions.com .

5 Gestión de accesos y desarrollo seguro

Procedimientos a cargo del responsable técnico, aplicables a todo servicio contratado.

5.1 Alta y administración del servicio

1. **Registro del servicio.** Se registra el cliente, el servicio, la finalidad, los datos previstos, el responsable del cliente y las personas autorizadas para solicitar cambios. El alcance del acceso y del soporte se confirma por escrito.
2. **Accesos individuales** con el mínimo permiso necesario. Los accesos de administración se separan de los del usuario final cuando la plataforma lo permite; los permisos temporales se retiran al terminar la intervención.
3. **Custodia de credenciales** en el gestor con verificación en dos pasos, con un mecanismo de recuperación protegido que no depende de la misma cuenta bloqueada.
4. **Verificación por un canal conocido** de las solicitudes de cambio de contraseña, pagos, transferencia de dominios o entrega de bases de datos. No se actúa sobre una solicitud inesperada recibida solo por correo o mensajería.

5.2 Entrega de credenciales

Las credenciales se entregan preferentemente mediante invitaciones para que el cliente cree su propia contraseña, o mediante enlaces de acceso limitado y con caducidad. Cuando la plataforma no lo permite, se envían por un canal verificado con el contacto autorizado, se aplica el cambio obligatorio inicial si está disponible y se registra la entrega sin copiar el secreto. Se recomienda al cliente cambiar la contraseña en su primer acceso.

5.3 Desarrollo y publicación

1. **Repositorios privados.** Las contraseñas, claves y copias de bases de datos se excluyen del código y de su historial; si un secreto se expone, se revoca o rota de inmediato y se revisa su uso.
2. **Pruebas con datos ficticios.** Se comprueban permisos con cuentas de distintos roles, HTTPS, exposición de archivos, validación de entradas y configuración de producción. Se registra qué se probó y sus límites; una revisión no se denomina prueba de penetración si no lo fue.
3. **Cambios controlados.** Se realiza copia antes de cambios relevantes, se define cómo revertirlos y se comprueban después las funciones críticas. Los defectos de seguridad se corrigen antes de liberar el cambio o se documenta su tratamiento.
4. **Actualizaciones.** Revisión mensual de actualizaciones de seguridad; los avisos críticos se atienden en cuanto se conocen, sin esperar al ciclo mensual.

5.4 Cierre del servicio

Al finalizar un servicio se confirma con el cliente la entrega o devolución de su información; se retiran accesos, sesiones y claves del proveedor; se eliminan las copias de trabajo innecesarias y se informa al cliente la fecha prevista de expiración de los respaldos. Solo se conservan los documentos necesarios para una obligación legal o una finalidad documentada.

6 Respaldos, conservación y continuidad

6.1 Política de respaldo

1. **Inventario.** Por cada servicio se registra qué carpetas, sitios y bases de datos se copian, qué queda excluido, la frecuencia, el destino y la retención exacta, distinguiendo la sincronización de archivos de las versiones recuperables.
2. **Revisión semanal** del resultado de las tareas de respaldo y atención de los fallos detectados, con registro de la última copia correcta y de la acción tomada.
3. **Prueba trimestral** de recuperación de un archivo y de una muestra de sistema con base de datos en un entorno controlado, anotando origen, fecha de la copia, resultado, tiempo empleado y correcciones.
4. **RPO y RTO acordados.** La pérdida de datos tolerable y el tiempo objetivo de recuperación se acuerdan con cada cliente antes de comprometer un nivel de continuidad; los respaldos por sí solos no garantizan una recuperación en un plazo determinado.

6.2 Reglas de conservación

Información	Plazo de conservación	Aplicación
Consultas y contactos comerciales	Hasta 2 años desde la última interacción, salvo relación contractual	Conforme a la política de privacidad publicada.
Datos contractuales propios	Durante la vigencia del contrato y hasta 5 años después de finalizar	Sin perjuicio de las obligaciones tributarias y otras causas justificadas de conservación.
Comprobantes electrónicos	7 años, según el SRI [4]	Los comprobantes tributarios no se eliminan por la regla general de 5 años.
Archivos y datos del cliente	Durante el servicio; al terminar, devolución o eliminación según las instrucciones del cliente	Con constancia escrita de cierre y de las excepciones justificadas.
Respaldos	Mínimo 90 días; el plazo exacto se informa al cliente por servicio	Los datos pendientes de eliminación no se usan de forma ordinaria.

Si se restaura una copia antigua, se vuelven a aplicar las eliminaciones o restricciones posteriores. La eliminación efectiva se registra cuando corresponde.

6.3 Continuidad del servicio

Para garantizar la continuidad ante la ausencia del administrador, se mantiene un procedimiento de recuperación de acceso de emergencia, protegido y autorizado por escrito, que no implica compartir contraseñas de forma permanente. El cliente conserva en todo momento la titularidad de sus dominios, cuentas y datos, y puede solicitar su devolución.

7 Atención de incidentes de seguridad

Todo incidente que afecte a un cliente se gestiona con el siguiente flujo, con registro fechado de cada fase.

7.1 Flujo de atención

Fase	Acciones
1. Registrar y evaluar	Anotar fecha y hora de detección, servicio, señales observadas y datos posiblemente afectados. Diferenciar hechos confirmados de sospechas; cubrir también afectaciones de disponibilidad e integridad.
2. Contener	Restringir el acceso comprometido, revocar sesiones o credenciales y aislar el componente afectado cuando resulte necesario. Coordinar con el proveedor; evitar borrar registros útiles para entender lo sucedido.
3. Preservar evidencias	Guardar alertas, registros y acciones con fecha y acceso restringido. No copiar datos personales innecesarios ni enviar bases de datos por mensajería.
4. Avisar y escalar	Contactar al cliente por el canal conocido y dejar constancia por correo. Informar qué se sabe, qué falta por confirmar, medidas adoptadas y próxima actualización. No se espera a resolver el problema para avisar.
5. Corregir y recuperar	Eliminar la causa identificada, aplicar correcciones y recuperar desde una copia evaluada. Comprobar accesos, integridad y funcionamiento antes de restablecer plenamente el servicio.
6. Cerrar y aprender	Documentar alcance final, comunicaciones, causa, recuperación y medidas pendientes. Mantener seguimiento hasta completar las acciones y conservar el registro según su finalidad.

7.2 Plazos de comunicación

Rol de la empresa	Destinatario	Plazo máximo	Condición
Encargado	Responsable del tratamiento (cliente)	2 días desde conocer la vulneración	Se comunica cuanto antes, sin esperar a confirmar todos los detalles.
Responsable	SPDP y ARCOTEL	5 días desde conocer la vulneración	Se valora la notificación, salvo el supuesto legal de riesgo improbable.
Responsable	Titulares afectados	3 días desde conocer el riesgo para sus derechos	Sin dilación; se aplican las condiciones y excepciones de los artículos 43 y 46 [1].

Objetivo de servicio: iniciar la comunicación al cliente en las primeras 24 horas desde la detección, sin ampliar un plazo contractual o legal más corto. Los plazos legales no son tiempos de espera: la llamada al cliente no sustituye las notificaciones formales que correspondan.

7.3 Contenido mínimo de la comunicación

Servicio afectado y momento de detección; hechos conocidos, diferenciados de lo que falta por confirmar; categorías de información y personas potencialmente afectadas; efectos posibles y medidas adoptadas; recomendaciones inmediatas para el cliente; responsable de contacto y fecha de la siguiente actualización. La información incompleta se amplía en actualizaciones posteriores, sin ocultar la incertidumbre.

8 Privacidad y relación con terceros

8.1 Atención de solicitudes de titulares

El canal de atención es info@geomastersolutions.com. El responsable técnico registra la solicitud, verifica la identidad de forma proporcionada (sin exigir automáticamente una copia íntegra de cédula si basta una verificación menos intrusiva) y determina si se refiere a datos propios o a datos tratados por cuenta de un cliente. En este último caso la remite al cliente y colabora siguiendo sus instrucciones [2].

Las solicitudes sobre datos propios se atienden en un máximo de 15 días calendario, plazo que la ley fija para los derechos de acceso, rectificación y eliminación [1]. Se registra la respuesta y su fundamento, la entrega segura y, cuando procede, la actualización o eliminación en los sistemas. Si existe una obligación de conservación, se explica qué información se mantiene, para qué y durante cuánto tiempo.

8.2 Contratos y confidencialidad

Cada servicio se formaliza por escrito con el alcance, las instrucciones de tratamiento, los accesos autorizados y el compromiso de confidencialidad. Cuando GEOMASTERSOLUTIONS actúa como encargado, el acuerdo identifica objeto, duración, finalidad, datos, titulares y obligaciones de las partes [2, 3], e incluye los proveedores autorizados, la respuesta a incidentes, la asistencia para atender derechos, la devolución o eliminación al cierre y el tratamiento de los respaldos.

Si se incorporan colaboradores a un servicio, sus permisos y compromisos de confidencialidad se definen antes de darles acceso, y el cliente es informado.

8.3 Proveedores y ubicación de los datos

Para cada proveedor se documenta la entidad contratada, el país o región de los datos, las condiciones de tratamiento, los subproveedores, los procedimientos de devolución y eliminación y los medios de contacto. El régimen aplicable al flujo internacional de datos y las garantías exigibles se determinan antes de confiar datos de clientes, conforme a la normativa vigente de la SPDP.

8.4 Uso de inteligencia artificial

Las herramientas de inteligencia artificial se utilizan únicamente con ejemplos ficticios o material sin datos personales ni información confidencial. Antes de enviar cualquier contenido se revisan también archivos adjuntos, comentarios, metadatos y código. Cualquier ampliación de este uso requiere evaluar proveedor, finalidad, autorización del cliente y riesgos antes de compartir material real.

9 Registros, revisión y mejora continua

9.1 Registros que se mantienen

Registro	Contenido	Acceso
Inventario de tratamiento y servicio	Cliente, servicio, finalidad, rol, datos tratados, proveedores, región, accesos autorizados, plazos de conservación y acuerdos.	Restringido; se comparte con el cliente la ficha de su servicio.
Revisión técnica y pruebas de recuperación	Fecha, alcance, resultado, hallazgos, correcciones y fecha de cierre de cada revisión o prueba.	Restringido; evidencias depuradas disponibles para el cliente.
Incidentes y solicitudes de derechos	Apertura, evaluación, plazos aplicables, acciones, comunicaciones y cierre de cada caso.	Restringido; el cliente recibe el informe de los casos que le afectan.

En los registros nunca se anotan contraseñas, códigos de un solo uso ni claves privadas; las evidencias se identifican por una referencia a su ubicación protegida.

9.2 Rutina de revisión

Frecuencia	Actividad	Registro
Semanal	Revisar el resultado de las tareas de respaldo y atender fallos.	Última copia correcta y acción tomada.
Mensual	Revisar e instalar actualizaciones de seguridad; registrar cambios y permisos.	Fecha, sistemas revisados y cambios aplicados.
Trimestral	Probar una restauración y revisar el estado de los controles.	Prueba de recuperación y estado de cada control.
Anual y tras cambios relevantes o incidentes	Revisar el manual, inventarios, riesgos y compromisos contractuales.	Nueva versión del manual con control de cambios.

9.3 Información disponible para el cliente

El cliente puede solicitar en cualquier momento la versión vigente de este manual, la ficha de su servicio y las evidencias pertinentes de los controles aplicados, depuradas de información de otros clientes. Los anexos técnicos con detalles de infraestructura se comparten bajo acceso restringido y, cuando corresponde, con acuerdo de confidencialidad.

10 Aprobación y referencias

10.1 Aprobación

El Representante Legal de GEOMASTERSOLUTIONS S.A.S. aprueba este manual y las políticas que contiene, que entran en vigor en la fecha indicada y son de aplicación a todos los servicios de la empresa. El documento se suscribe con firma electrónica.

Dato	Detalle
Titular del documento	GEOMASTERSOLUTIONS S.A.S.
Responsable de aprobación	Lázaro Rafael Batule Águila
Cargo	Representante Legal y Responsable Técnico
Contacto	info@geomastersolutions.com
Fecha de aprobación	15 de octubre de 2026
Fecha de entrada en vigor	15 de octubre de 2026



Lázaro Rafael Batule Águila

REPRESENTANTE LEGAL · GEOMASTERSOLUTIONS S.A.S.

Firmado electrónicamente

10.2 Referencias normativas

Fuentes consultadas el 15 de octubre de 2026.

- [1] [Ley Orgánica de Protección de Datos Personales — copia publicada por la SPDP](#)
Roles, derechos, encargo, seguridad y notificación de vulneraciones; artículos 13 a 15, 34, 43 y 46.
- [2] [Reglamento General de la LOPDP — copia publicada por la SPDP](#)
Relación responsable y encargado, asistencia y obligaciones de registro; artículos 38 a 45.
- [3] [SPDP — Resolución 2025-0006 sobre cláusulas de protección de datos en contratos](#)
- [4] [SRI — Aviso sobre conservación de comprobantes electrónicos](#)
- [5] [Política de privacidad publicada por GEOMASTERSOLUTIONS](#)