MANUAL DEL SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES (SGPDP)

ESPOLTEL S.A.

Razón Social:	**ESPOLTEL S.A.**
RUC:	0991415106001
Fecha de emisión:	30 de diciembre de 2025
Versión:	1.0

Contenido

INTRODUCCIÓN

El presente Manual del Sistema de Gestión de Protección de Datos Personales (SGPDP) de la compañía ESPOLTEL S.A. ha sido elaborado en cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP) del Ecuador y su Reglamento General de Aplicación (RGLOPDP).

Este documento constituye el instrumento rector que orienta el tratamiento responsable, seguro y transparente de los datos personales de todas las partes relacionadas con la organización, incluyendo clientes institucionales, entidades contratantes del sector público, proveedores, contratistas, subcontratistas, personal técnico y administrativo, así como terceros vinculados a la ejecución de proyectos.

Este manual define las políticas, procedimientos, roles y mecanismos de control que garantizan el respeto a los derechos fundamentales de privacidad y protección de datos personales, en concordancia con los principios de juridicidad, transparencia, finalidad, minimización, seguridad y responsabilidad proactiva.

Objeto de la política

El objetivo es informar a los titulares de datos personales, incluyendo empleados, clientes, proveedores y prestadores de servicios sobre el tratamiento que la compañía ESPOLTEL S.A. realiza de su información personal.

Esta política describe los procedimientos de recolección, uso, almacenamiento y protección de datos personales, en estricto cumplimiento de la Ley Orgánica de Protección de Datos Personales, su reglamento general de aplicación y las normas especializadas en materia de protección de datos personales.

Datos del responsable del Tratamiento de Datos Personales:

- **Nombre del responsable:** ESPOLTEL S.A.
- **RUC:** 0991415106001
- **Domicilio:** Km. 30,5 Vía Perimetral, Campus ESPOL, Guayaquil, Ecuador.
- **Correo electrónico:** dpd@espoltel.com

Alcance de la Política

Esta política aplica a todos los tratamientos de datos personales realizados por la Empresa, incluyendo:

- Clientes
- Proveedores
- Empleados
- Prestadores de servicios
- Otros

Cualquier otro dato personal tratado en el desarrollo de sus actividades.

Marco Legal

- Constitución de la República del Ecuador (CRE)
- Ley Orgánica de Protección de Datos Personales (LOPDP)
- Reglamento General de Protección de Datos Personales (RGLOPDP)
- Ley de Comercio Electrónico, Firmas y Mensajes de Datos.

- Demás normativas (incluido resoluciones) aplicables en materia de protección de datos personales

Definiciones

Dato personal: Información sobre una persona natural identificada o identificable

Dato Sensible: Datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.

Tratamiento: Cualquier operación sobre datos personales: recolección, uso, almacenamiento, conservación, eliminación.

Titular: Persona natural a quien se refieren los datos personales.

Responsable: ESPOLTEL, quien determina las finalidades y medios del tratamiento.

Encargado: Tercero que trata datos por cuenta de ESPOLTEL.

Base de Datos: Conjunto organizado de datos personales.

Persona Natural: Individuos capaces de ejercer derechos, y contraer obligaciones.

Tercero: Persona natural o jurídica, autoridad u organismo distinto del titular, del responsable del tratamiento y del encargado del tratamiento.

Responsable del Tratamiento: Persona natural o jurídica que determina las finalidades y los medios del tratamiento de datos personales (en este caso, la Empresa).

SGPDP: Sistema de Gestión de Protección de Datos Personales.
DPD: Delegado de Protección de Datos.
SPDP: Superintendencia de Protección de Datos Personales - Autoridad de control en Ecuador.
RAT: Registro de Actividades de Tratamiento, conforme al Art. 38 del RGLOPDP.
DPIA/PIA: Evaluación de Impacto sobre la Protección de Datos / Privacy Impact Assessment.

Fases de Implementación del SGPDP

La implementación del Sistema de Gestión de Protección de Datos Personales (SGPDP) en la compañía ESPOLTEL S.A. se estructura en siete fases progresivas, con una duración total aproximada de 4 meses para las fases operativas y una auditoría anual de continuidad. Cada fase genera entregables concretos que se desarrollan a lo largo del presente Manual.

FASE	NOMBRE	DURACIÓN	OBJETIVO Y ACTIVIDADES CLAVE	RESULTADO / SECCIÓN DEL MANUAL
FASE 1	**Diagnóstico**	1–3 semanas	Conocer la situación actual. Revisión LOPDP, evaluación práctica, análisis de controles, identificación de brechas y sensibilización del personal.	Informe de diagnóstico → Anexos 1 y 2 ; Manual SGPDP
FASE 2	**Inventario de Activos y RAT**	2–3 semanas	Organizar y documentar la información. Identificación de	Control total sobre qué datos se tratan

			bases de datos, mapeo ciclo de datos, elaboración RAT, clasificación de datos (identificativos, académicos, sensibles).	→Anexo 3 y Manual SGPDP
FASE 3	**Gestión de Riesgos**	2–3 semanas	Detectar y reducir riesgos. Identificación de amenazas, evaluación probabilidad/impacto, matriz de riesgos y definición de medidas de mitigación.	Plan de tratamiento de riesgos – Manual SGPDP
FASE 4	**Marco Documental**	2–3 semanas	Formalizar políticas y procedimientos. Política de protección de datos, avisos de privacidad, gestión de incidentes, derechos ARCO, acuerdos de confidencialidad.	Sistema documentado alineado a la normativa - Manual SGPDP
FASE 5	**Implementación de Controles**	3–4 semanas	Aplicar medidas reales de protección. Control de accesos, cifrado, respaldo, protección de archivos físicos, protocolos ante incidentes y continuidad operativa.	Seguridad técnica y organizativa operativa → Anexo 2 y Manual SGPDP
FASE 6	**Capacitación Final**	1 día	Explicar lo implementado. Formación LOPDP, seguridad de la información, uso correcto de políticas, procedimientos internos, responsabilidades individuales y concientización.	LOPDP comprendido y aplicado
FASE 7	**Auditoría Anual**	Cada 12 meses	Verificar cumplimiento continuo. Revisión de políticas, actualización del RAT, incidentes registrados, nuevos riesgos, no conformidades, acciones correctivas y revisión de la dirección.	Informe de auditoría y plan de mejora continua → Anexo 4 y Manual SGPDP

CONTEXTO DE LA ORGANIZACIÓN

Factores legales y regulatorios

La organización opera en el Ecuador, por lo que debe cumplir con la Ley Orgánica de Protección de Datos Personales del Ecuador, la cual establece los principios, derechos y obligaciones para el tratamiento de datos personales. Esta normativa exige que la empresa garantice la confidencialidad, integridad y disponibilidad de la información, así como el consentimiento informado de los titulares de datos.

Adicionalmente, la empresa debe considerar regulaciones sectoriales dependiendo del tipo de proyecto ejecutado:

- En proyectos de auditorías médicas se deben cumplir disposiciones del Ministerio de Salud Pública del Ecuador relacionadas con la confidencialidad de datos sensibles de salud.
- En obras civiles pueden aplicarse normativas del Servicio Nacional de Contratación Pública (SERCOP), como la Ley Orgánica del Sistema Nacional de Contratación Pública (LOSNCP) y su reglamento general, así como normas INEN,

especialmente en contratos públicos que implican manejo de información personal.
- En proyectos energéticos, la Ley Orgánica del Servicio Público de Energía Eléctrica (LOSPEE) y su reglamento y la LOSNCP, así como regulaciones de entidades como el Ministerio de Ambiente y Energía del Ecuador.

Asimismo, la organización debe respetar derechos constitucionales establecidos en la Constitución de la República del Ecuador, como el derecho a la privacidad y protección de datos personales.

Factores políticos y económicos

El entorno político ecuatoriano ha mostrado un creciente enfoque en la regulación y supervisión del uso de datos personales, impulsando a las organizaciones a adoptar políticas claras y mecanismos de cumplimiento.

Desde el punto de vista económico:

- La empresa participa en sectores estratégicos (construcción, salud, energía), donde la confianza y reputación son clave.
- El incumplimiento en protección de datos puede derivar en sanciones económicas, pérdida de contratos (especialmente con el Estado) y afectación reputacional.
- La digitalización de procesos (licitaciones, auditorías, gestión de proyectos) implica mayor volumen de datos tratados, incrementando los riesgos asociados.

Además, la interacción con clientes públicos y privados exige estándares cada vez más altos en seguridad de la información como condición para la contratación.

Factores sociales y culturales

En el Ecuador existe una creciente conciencia ciudadana sobre la privacidad y el uso de datos personales, lo que obliga a las organizaciones a ser más transparentes en sus prácticas.

Factores relevantes incluyen:

- Mayor sensibilidad frente al tratamiento de datos sensibles, especialmente en auditorías médicas (información de salud).
- Expectativa social de que las empresas protejan adecuadamente la información de Trabajadores, contratistas y clientes.
- Cultura organizacional en transición hacia la protección de datos, donde aún es necesario fortalecer la capacitación y concienciación del personal.

Asimismo, la diversidad cultural del país implica considerar distintos niveles de comprensión sobre el uso de datos, lo que requiere políticas claras, accesibles y comunicadas adecuadamente.

Factores tecnológicos

La compañía, en el desarrollo de sus actividades, depende de manera significativa de infraestructuras y herramientas tecnológicas para la gestión, almacenamiento y tratamiento de datos personales.

En este contexto, se identifican los siguientes factores tecnológicos relevantes para la adecuada implementación del Sistema de Gestión de Protección de Datos Personales (SGPDP):

- La organización utiliza servicios de almacenamiento en la nube, lo que implica que los datos personales pueden ser gestionados en infraestructuras de terceros. En consecuencia, se deben considerar aspectos como la ubicación de los servidores, posibles transferencias internacionales de datos, niveles de seguridad ofrecidos por el proveedor, esquemas de respaldo y recuperación, así como el cumplimiento de estándares internacionales de seguridad de la información. La compañía deberá asegurarse de que dichos proveedores cumplan con la normativa ecuatoriana vigente en materia de protección de datos personales y garanticen medidas técnicas y organizativas adecuadas.
- Adicionalmente, la empresa emplea un sistema contable informatizado que procesa información personal de empleados, proveedores, contratistas y, en ciertos casos, de representantes de entidades contratantes. Este sistema constituye un punto crítico de tratamiento de datos, por lo que requiere controles de acceso robustos, trazabilidad de operaciones, mecanismos de autenticación segura y políticas de actualización.

Factores que generan riesgos como:

- Incumplimiento de la Ley Orgánica de Protección de Datos Personales del Ecuador y demás normativas aplicables.
- Sanciones legales, multas y responsabilidades civiles por vulneración de datos personales.
- Pérdida de contratos y afectación a la reputación institucional, especialmente en procesos regulados por el Servicio Nacional de Contratación Pública.
- Manejo inadecuado de datos personales y sensibles (particularmente en auditorías médicas).
- Pérdida de confianza de clientes, Trabajadores y terceros.
- Falta de cultura organizacional y capacitación en protección de datos.
- Accesos no autorizados, filtraciones o pérdida de información.
- Ciberataques y vulnerabilidades en sistemas tecnológicos.
- Dependencia de terceros sin controles adecuados de seguridad de la información.
- Exposición de datos en operaciones de campo, uso de dispositivos móviles y ejecución de proyectos.

En el contexto de la LOPD, la empresa debe:

- Cumplir con normativas legales y mantener documentación actualizada.
- Implementar políticas de protección de datos personales.
- Obtener consentimiento previo, libre e informado del titular.
- Establecer controles internos para la gestión de información.
- Restringir el acceso a datos personales según funciones.

- Garantizar transparencia en el tratamiento de datos.
- Utilizar los datos únicamente para fines autorizados.
- Capacitar al personal en protección de datos y confidencialidad.
- Implementar medidas de seguridad (contraseñas seguras, antivirus,).
- Realizar copias de seguridad periódicas.
- Mantener actualizados los sistemas tecnológicos.
- Establecer mecanismos para atender derechos de los titulares.
- Definir tiempos de conservación y eliminación de datos.
- Establecer protocolos de respuesta ante incidentes de seguridad.

Evaluación de controles de seguridad basada en ISO/IEC 27001:2022:

Área evaluada	**Nivel de cumplimiento**
Controles técnicos	85 %
Controles organizativos	65 %
Gestión de riesgos	10 %
Protección de datos	10 %
Promedio general de cumplimiento:	**43 %**

Factores Internacionales

La compañía puede realizar transferencias internacionales de datos personales debido al uso de proveedores tecnológicos y servicios de procesamiento de información que operan en infraestructuras ubicadas fuera del Ecuador.

En este sentido, se debe garantizar el cumplimiento de la LOPDP mediante la implementación de medidas contractuales, técnicas y organizativas que aseguren un nivel adecuado de protección de los datos personales durante su tratamiento en el exterior.

Como referencia de buenas prácticas internacionales, se consideran marcos como el GDPR europeo y el uso de cláusulas contractuales estándar, que permiten asegurar la confidencialidad, integridad y disponibilidad de la información en entornos internacionales.

Herramienta útil - Análisis PESTEL

Factor	**Análisis**
Político	Alta regulación y control estatal en contratación pública; cambios en políticas gubernamentales pueden afectar la gestión de datos y exigencias de cumplimiento.
Económico	Riesgo de sanciones económicas, multas o pérdida de contratos; necesidad de inversión en seguridad de la información y cumplimiento normativo.
Social	Mayor conciencia sobre privacidad; exigencia de confidencialidad, especialmente en datos sensibles como los de salud; impacto en la reputación.
Tecnológico	Uso intensivo de sistemas digitales y almacenamiento en la nube; riesgos de ciberataques, accesos no autorizados y pérdida de información.
Ecológico	Manejo de información relacionada con proyectos ambientales y comunidades; necesidad de gestión responsable de datos en contextos territoriales.
Legal	Cumplimiento obligatorio de la Ley Orgánica de Protección de Datos Personales del Ecuador y normativas sectoriales; riesgo de sanciones legales por incumplimiento.

El análisis del contexto organizacional permitió identificar que la compañía ESPOLTEL S.A. se encuentra en un proceso de transición hacia una gestión más estructurada de la protección de datos personales y de la seguridad de la información.

Si bien la empresa presenta un nivel intermedio de digitalización de documentos, así como la implementación de controles tecnológicos básicos, se identifican oportunidades de mejora relacionadas con la formalización de políticas de seguridad de la información, la gestión estructurada de riesgos y el establecimiento de procedimientos para la atención de incidentes de seguridad.

Objetivos Estratégicos del SGPDP - Sistema de Gestión de Protección de Datos Personales

1. Garantizar la protección de los datos personales de todos los miembros de ESPOLTEL S.A.
2. Cumplir con la normativa legal vigente en materia de protección de datos y demás.
3. Establecer procedimientos claros para la recolección, almacenamiento, uso y tratamiento de datos personales.
4. Implementar medidas de seguridad técnica y organizativa que protejan la información frente a accesos no autorizados, pérdida o uso indebido.
5. Promover una cultura institucional de privacidad, donde el personal conozca y respete los principios de protección de datos.
6. Mantener actualizados el RAT y los inventarios de activos de información.

Procesos Organizacionales

Dentro de la compañía se identifican diversos procesos en los cuales se recopilan, utilizan y gestionan datos personales, necesarios para la ejecución de proyectos.

Gestión de contratación y ejecución de proyectos

En este proceso se recopilan datos necesarios para la participación y ejecución de contratos con entidades públicas y privadas, incluyendo:

- Información de representantes de entidades contratantes
- Datos de proveedores, contratistas y subcontratistas
- Información técnica y contractual asociada a proyectos
- Datos necesarios para cumplimiento de obligaciones contractuales y legales

Gestión de talento humano

La compañía gestiona datos personales de su personal para fines laborales y administrativos, incluyendo:

- Información personal y de contacto
- Datos contractuales y salariales
- Historial laboral y profesional

- Registros de asistencia (incluyendo datos biométricos, cuando aplique)

Gestión financiera y contable

Este proceso implica el tratamiento de datos personales relacionados con la administración económica de la empresa:

- Datos de proveedores y clientes institucionales
- Información tributaria y de facturación
- Registros de pagos, contratos y transacciones
- Información bancaria o financiera asociada

Gestión de compras y proveedores

Se gestionan datos personales de terceros vinculados a la operación de la empresa:

- Proveedores y contratistas
- Representantes legales de empresas proveedoras
- Datos de contacto y documentación contractual
- Información necesaria para procesos de contratación pública

Gestión de servicios generales

Este proceso incluye el tratamiento de datos relacionados con el funcionamiento operativo de la empresa:

- Datos de visitantes a instalaciones
- Información de proveedores de mantenimiento y servicios
- Registros de control de acceso físico
- Datos asociados a seguridad y operación del edificio

Canales digitales y sistemas de información

La compañía obtiene y gestiona datos personales a través de diversos medios digitales, los cuales requieren controles de seguridad adecuados:

- Sistemas empresariales internos
- Plataformas en la nube y herramientas colaborativas
- Correo electrónico corporativo
- Sitios web y canales digitales utilizados para interacción con terceros

Recursos Disponibles

Nivel de madurez tecnológica:

- La compañía evidencia un nivel de madurez tecnológica básico a intermedio, considerando:
- Uso de herramientas digitales para la gestión de proyectos y procesos de contratación pública
- Manejo de información en sistemas administrativos, contables y de facturación electrónica

- Uso de plataformas tecnológicas y servicios en la nube para almacenamiento y gestión de información
- Comunicación digital con entidades contratantes, proveedores, contratistas y personal interno

Sin embargo, aún se requiere fortalecer:

- Sistemas de gestión de seguridad de la información
- Control de accesos a bases de datos y sistemas críticos (contables, facturación y gestión de proyectos)
- Protección frente a incidentes de ciberseguridad, especialmente en entornos iCloud
- Monitoreo y auditoría de accesos y operaciones sobre datos personales

Existencia de políticas previas

Esto constituye una base importante para la gobernanza de datos. La compañía cuenta con:

- Política formal de protección de datos personales
- Identificación del responsable del tratamiento
- Definición de titulares de datos (clientes institucionales, proveedores, contratistas, empleados, entre otros)
- Identificación de tipos de datos tratados, en función de la ejecución de proyectos y procesos contractuales
- Marco legal aplicable conforme a la normativa ecuatoriana vigente

No obstante, se recomienda fortalecer la formalización de procedimientos específicos para el tratamiento de datos en procesos de contratación pública, así como la gestión de encargados de tratamiento (proveedores tecnológicos, servicios en la nube, entre otros).

Personal capacitado:

El personal técnico, administrativo y de apoyo participa activamente en el manejo de información personal, especialmente en el contexto de ejecución de proyectos, gestión contractual, contable y operativa.

No obstante, es necesario fortalecer:

- Capacitación en normativa de protección de datos personales aplicable en Ecuador
- Buenas prácticas en privacidad y confidencialidad de la información
- Gestión segura de la información en entornos digitales y sistemas informáticos
- Concientización sobre riesgos asociados al tratamiento de datos personales y su responsabilidad individual dentro del SGPDP

En este sentido, el fortalecimiento de capacidades del personal constituye un elemento clave para garantizar el cumplimiento normativo y la adecuada protección de los datos personales gestionados por la compañía.

Cultura Organizacional

La elaboración del presente Manual evidencia el compromiso institucional inicial con la protección de datos, evidenciado en:

- Reconocimiento de la normativa vigente.
- Identificación de los titulares de datos personales.
- Definición del responsable del tratamiento.

Compromiso de la alta dirección: La elaboración de la política demuestra que la dirección reconoce la importancia de la privacidad y busca formalizar mecanismos de protección de la información.

Compromiso del personal: El nivel de compromiso del personal depende de:

- La capacitación que reciban sobre protección de datos.
- La existencia de procedimientos claros.
- La supervisión institucional del cumplimiento de la política.

Para fortalecer la cultura organizacional se recomienda:

- Programas de sensibilización.
- Protocolos de manejo de información.
- Responsables internos de protección de datos.

Herramienta útil - Análisis FODA

El Análisis FODA enfocado en privacidad y seguridad de la información se basa en cuatro ejes principales:

✓ FORTALEZAS	▲ OPORTUNIDADES
• Existencia de una política formal de protección de datos personales. • Identificación clara de titulares de datos. • Cumplimiento con la normativa ecuatoriana (LOPDP). • Reconocimiento de datos sensibles. • Manual SGPDP documentado. • Designación del DPD.	• Implementar sistemas de gestión de seguridad de la información - SGSI completo. • Capacitar al personal en privacidad. • Incorporar herramientas tecnológicas de seguridad digital. • Realizar auditorías periódicas.
✕ DEBILIDADES	**⚠ AMENAZAS**
• Protocolos operativos en desarrollo. • Capacitación limitada del personal en privacidad. • Dependencia de sistemas digitales que podrían no tener suficientes controles. • Sin auditorías periódicas implementadas. • Gestión de riesgos básica. • Sin criterios formales de retención de datos personales.	• Filtración de datos personales. • Ataques informáticos o pérdida de información. • Uso indebido de datos sensibles. • Sanciones por incumplimiento LOPDP.

Partes Interesadas

En la gestión de protección de datos intervienen diversas partes interesadas:
Titulares de los datos: Son las personas cuyos datos son tratados por la institución. Tienen derechos sobre su información personal.

- Empleados
- Clientes
- Proveedores
- Prestadores de servicios
- Otros derivados de la actividad comercial

Responsable del tratamiento: La compañía **ESPOLTEL S.A.** quien decide sobre:
- Finalidad del tratamiento
- Uso de los datos
- Medidas de seguridad.

SPDP (Superintendencia de Protección de Datos Personales): Es la autoridad de control encargada de:
- Supervisar el cumplimiento de la normativa.
- Investigar posibles infracciones.
- Garantizar los derechos de los titulares.

Encargados del tratamiento: Personas o entidades que procesan datos por cuenta de la institución, como:

- Sistemas informáticos
- Proveedores de servicios tecnológicos.

Proveedores y terceros Sus datos también deben ser protegidos según la política institucional incluyen:
- Proveedores de servicios
- Contratistas
- Visitantes institucionales

LIDERAZGO Y COMPROMISO

ESPOLTEL S.A. reconoce que la protección de datos personales constituye un derecho fundamental de las personas, garantizado por la Constitución de la República del Ecuador (Art. 66, numeral 19) y regulado por la Ley Orgánica de Protección de Datos Personales (LOPDP) y su Reglamento General de Aplicación. En virtud de ello, la organización asume el compromiso de implementar políticas, procedimientos y controles adecuados que garanticen el tratamiento lícito, seguro y transparente de los datos personales de entidades contratantes del sector público, proveedores, contratistas, subcontratistas, empleados, y demás terceros vinculados a la ejecución de proyectos.

La alta dirección promoverá una cultura organizacional basada en la responsabilidad, la confidencialidad y la protección de la información personal, asegurando que todas las actividades de tratamiento de datos se realicen respetando los principios de juridicidad, transparencia, finalidad, minimización de datos, seguridad y responsabilidad proactiva establecidos en la normativa vigente.

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

La compañía adopta la presente Política de Protección de Datos Personales con el propósito de garantizar que todo tratamiento de datos personales se efectúe de forma legítima, segura, responsable y conforme a la normativa ecuatoriana, especialmente en el marco de la ejecución de proyectos mediante contratación pública.

En este sentido, la organización se compromete a:

a) Tratar los datos personales únicamente para fines relacionados con la ejecución de proyectos, gestión contractual, administrativa, financiera, laboral, técnica y demás finalidades legítimas vinculadas a su giro de negocio.
b) Obtener, cuando corresponda, el consentimiento previo, libre, informado, específico e inequívoco de los titulares de los datos personales, salvo en los casos previstos por la ley, especialmente en el marco de relaciones contractuales con el sector público.
c) Implementar medidas técnicas, organizativas y administrativas que permitan proteger los datos personales frente a riesgos de pérdida, acceso no autorizado, alteración o divulgación indebida, incluyendo aquellos almacenados en la nube y en sistemas informáticos institucionales.
d) Garantizar que los datos personales sean tratados únicamente por personal autorizado y dentro del ámbito de sus funciones.
e) Informar a los titulares sobre el uso, finalidad, conservación y mecanismos para ejercer sus derechos de acceso, rectificación, actualización, eliminación u oposición.
f) Conservar los datos personales únicamente durante el tiempo necesario para cumplir con obligaciones contractuales, legales y regulatorias, especialmente en materia de contratación pública y normativa tributaria.
g) Establecer procedimientos internos para la gestión de incidentes de seguridad que puedan comprometer la confidencialidad, integridad o disponibilidad de los datos personales.

Roles y Responsabilidades

Para garantizar el cumplimiento de la normativa de protección de datos personales, la compañía establece los siguientes roles.

Responsable del Tratamiento

La compañía ESPOLTEL S.A., representada por la Gerencia, actuará como Responsable del Tratamiento de Datos Personales, siendo la entidad que decide sobre la finalidad, medios y condiciones del tratamiento.

Sus principales responsabilidades son:

- Garantizar el cumplimiento de la LOPDP y su Reglamento
- Definir y aprobar políticas internas de protección de datos
- Supervisar los procesos de tratamiento de datos personales
- Adoptar medidas técnicas y organizativas de seguridad
- Atender solicitudes de ejercicio de derechos de los titulares

Delegado de Protección de Datos (DPD)

La empresa designará un Delegado de Protección de Datos Personales, quien actuará como asesor y supervisor interno del cumplimiento de la normativa de protección de datos personales. Sus funciones principales serán:

- Asesorar a la institución respecto de sus obligaciones legales en materia de protección de datos personales.
- Supervisar el cumplimiento de la normativa y de la presente política institucional.
- Promover la capacitación y concienciación del personal sobre protección de datos.
- Evaluar riesgos asociados al tratamiento de datos personales.
- Actuar como punto de contacto ante la SPDP (LOPDP, Art. 35).

Áreas de Apoyo

Las diferentes áreas de la compañía ESPOLTEL S.A. (servicios generales, dpto. financiero, TICS, gerencia, dpto. de compras) deberán cumplir con las políticas y procedimientos establecidos para el tratamiento de datos personales. Entre sus responsabilidades se encuentran:

- Tratar los datos personales únicamente para el cumplimiento de sus funciones institucionales.
- Mantener la confidencialidad de la información personal a la que tengan acceso.
- Aplicar las medidas de seguridad establecidas por la institución.
- Reportar cualquier incidente o vulneración de seguridad de datos personales.

Comité de Seguridad y Privacidad de la Información

ESPOLTEL S.A. podrá conformar un Comité de Seguridad y Privacidad de la Información con el objetivo de fortalecer la gobernanza institucional en materia de protección de datos personales.

Este comité estará integrado por representantes de la dirección institucional, el Delegado de Protección de Datos, el área administrativa y el área tecnológica. **Sus funciones principales serán:**

- Analizar riesgos relacionados con el tratamiento de datos personales dentro de la institución.
- Proponer mejoras a las políticas y procedimientos de seguridad de la información.
- Revisar incidentes de seguridad y establecer medidas correctivas.
- Promover buenas prácticas de protección de datos dentro de la comunidad.

PLANIFICACION

La compañía ESPOLTEL S.A. implementará un proceso permanente de planificación para garantizar el cumplimiento de la normativa de protección de datos personales, así como la mejora continua de sus controles de seguridad de la información.

Este proceso permitirá identificar riesgos, evaluar el cumplimiento normativo y establecer medidas preventivas que aseguren la protección adecuada de los datos personales tratados por la institución.

Evaluación de Cumplimiento Legal

La empresa realizará evaluaciones periódicas del cumplimiento de la LOPDP y su Reglamento. El diagnóstico inicial arroja un 60% de cumplimiento (9 de 15 requisitos cumplidos), con las siguientes brechas prioritarias registradas en el Anexo 1.

Requisito	Estado	Prioridad
Evaluaciones de impacto de tratamiento (DPIA)	NO CUMPLE	Alta
Criterios documentados de retención y eliminación segura de datos	NO CUMPLE	Alta
Avisos de privacidad en videovigilancia y biometría	NO CUMPLE	Media
Revisiones y auditorías internas periódicas del SGPDP	NO CUMPLE	Media
Requisitos CUMPLIDOS (9/15) - ver Anexo 1 para el detalle completo	**60.0 %**	-

Estas evaluaciones incluirán:

- Identificación de las bases legales que justifican el tratamiento de datos personales dentro de la institución.
- Verificación del cumplimiento de los principios de tratamiento de datos personales establecidos en la normativa.
- Revisión de los mecanismos de obtención del consentimiento de los titulares o de sus representantes legales.
- Evaluación de los procedimientos para el ejercicio de derechos de los titulares de datos.
- Revisión del cumplimiento de obligaciones relacionadas con la conservación y eliminación de datos personales.

Los resultados de estas evaluaciones permitirán identificar brechas de cumplimiento y establecer planes de mejora para garantizar el respeto de los derechos de los titulares de datos.

Evaluación de Cumplimiento Controles de Seguridad de la Información

La empresa evaluará periódicamente la eficacia de las medidas implementadas para proteger los datos personales, considerando: seguridad de sistemas informáticos y bases de datos, mecanismos de control de acceso, medidas de respaldo y recuperación, procedimientos de gestión de incidentes y capacitación del personal. (ISO, 2022). (Ver Anexo 2 para detalle de controles ISO 27001).

Inventario de Activos de Información

Conforme al control 5.9 de ISO/IEC 27001:2022 y Art. 38 del RGLOPDP, se mantiene el siguiente inventario de activos:

ID	Activo de Información	Tipo	Categoría	Clasificación	Ubicación	Responsable
ACT-01	Sistema contable ODOO	Digital	Financiero / Comercial	**Confidencial**	Nube / Servidor interno	Área Financiera
ACT-02	SharePoint - Gestión documental corporativa	Digital	Administrativo / Jurídico	**Confidencial**	Nube (Microsoft 365)	TICS / Todas las áreas
ACT-03	Expedientes laborales del personal (contratos, nómina, evaluaciones)	Digital / Físico	RRHH	**Confidencial**	Servidor interno / Archivo físico	Talento Humano
ACT-04	Sistema biométrico (huella dactilar - control de asistencia)	Digital	RRHH / Seguridad	**SENSIBLE**	Servidor interno (ESPOLTEL)	TICS / Talento Humano
ACT-05	Sistema de videovigilancia CCTV (imágenes y grabaciones)	Digital	Seguridad	**SENSIBLE**	Servidor seguridad (ESPOLTEL)	Gerencia / TICS
ACT-06	Expedientes médicos IESS (auditorías - datos de salud)	Digital	Salud	**SENSIBLE**	Servidor / Empresa aliada Colombia	Coordinación de Proyectos
ACT-07	Base de datos de prestadores de servicios (7 personas)	Digital / Físico	Jurídico / RRHH	**Confidencial**	SharePoint / Archivo	Gerencia / Administración
ACT-08	Base de datos de proveedores (~50 anuales)	Digital / Físico	Compras	**Confidencial**	ODOO / Archivo físico	Área de Compras
ACT-09	Documentación de licitaciones SERCOP (propuestas, contratos adjudicados)	Digital / Físico	Jurídico / Comercial	**Confidencial**	SharePoint	Gerencia / Asesoría Jurídica Externa
ACT-10	Registros contables y tributarios (facturas, retenciones, declaraciones SRI)	Digital / Físico	Financiero	**Confidencial**	ODOO / Archivo físico	Financiera
ACT-11	Correo electrónico institucional	Digital	Comunicación	**Interno**	Nube (proveedor de correo)	TICS / Todas las áreas
ACT-12	Contratos con proveedores y encargados del tratamiento	Físico / Digital	Jurídico	**Confidencial**	Administración / SharePoint	Gerencia / Asesoría Jurídica

ACT-13	Registros de solicitudes ARCO	Digital / Físico	Jurídico	**Confidencial**	Oficina DPD / SharePoint	DPD / Rep. Legal
ACT-14	Credenciales y contraseñas de sistemas (ODOO, SharePoint, correo)	Digital	TI	**CRÍTICO**	Gestor de contraseñas / TICS	TICS
ACT-15	Documentación de proyectos adjudicados (obra civil, fotovoltaje, call center)	Digital / Físico	Operativo	**Interno**	SharePoint / Archivo físico	Coordinación de Proyectos

Registro de Actividades de Tratamiento (RAT)

Conforme al Art. 38 del RGLOPDP, la compañía ESPOLTEL S.A. mantiene el Registro de Actividades de Tratamiento. A continuación, se presenta el resumen de las principales actividades:

Registro de Actividades de Tratamiento - ESPOLTEL S.A.

RUC: 0991415106001 | Rep. Legal: Cárdenas Muga Jorge Luis | Elaborado conforme a LOPDP y RGLOPDP

Actividad de tratamiento	Finalidad del tratamiento	Categoría de datos personales	Titulares de los datos	Base de legitimación	Encargados / Destinatarios	Transferencias internacionales	Plazo de conservación	Medidas de seguridad implementadas
Gestión de talento humano	Administración de contratos, pagos, control laboral y cumplimiento de obligaciones legales	Datos identificativos, laborales, académicos, financieros y de salud (certificados médicos/ expedientes médicos)	Empleados (119 trabajadores)	Ejecución de contrato y obligación legal	IESS, SRI, proveedor contable externo	No aplica	Durante la relación laboral y según normativa legal	Accesos restringidos, archivos físicos bajo custodia, respaldos digitales en SharePoint
Gestión de prestadores de servicios	Gestión de contratos de prestación de servicios, facturación mensual y actualización de datos del prestador	Datos identificativos y financieros (RUC, datos de facturación, información contractual)	Prestadores de servicios (7 personas)	Ejecución de contrato	No aplica	No aplica	Durante la relación contractual y según normativa tributaria	Acceso restringido, gestión documental en SharePoint, actualización periódica de datos (RUC)
Control de asistencia (biométrico)	Registro de ingreso, salida y control de jornada laboral	Datos biométricos (huella dactilar)	Empleados (119 trabajadores)	Interés legítimo y obligación legal	No aplica (gestionado internamente por ESPOLTEL)	No aplica	Durante la relación laboral	Control de acceso, cifrado, almacenamiento seguro
Videovigilancia	Seguridad de personas, instalaciones y control de riesgos	Imágenes y grabaciones de video	Empleados, prestadores y visitantes	Interés legítimo	Autoridades competentes (en caso necesario); gestionado internamente por ESPOLTEL	No aplica	30 a 90 días	Acceso restringido, almacenamiento seguro, señalización informativa
Auditorías médicas (IESS)	Revisión de expedientes médicos digitales de beneficiarios del IESS conforme a normativa 117; verificación de 10 requisitos del checklist normativo	Datos de salud (categoría especial bajo LOPDP Art. 26)	Pacientes / beneficiarios IESS	Obligación legal / ejecución de contrato con entidad pública (IESS)	Empresa aliada colombiana (prestador externo del IESS)	Sí — transferencia de datos a Colombia (empresa aliada)	Según normativa sanitaria y términos del contrato con el IESS	Contrato de encargado del tratamiento, cláusulas de transferencia internacional, cifrado de expedientes, acceso restringido
Gestión de licitaciones (SERCOP)	Preparación, gestión y presentación de propuestas en procesos de contratación pública	Datos identificativos, laborales y financieros de empleados y prestadores de servicios	Empleados y prestadores de servicios	Ejecución de contrato / obligación legal	SERCOP, entidades contratantes públicas	No aplica	Según normativa de contratación pública (LOSNCP)	Control documental, acceso restringido, gestión en SharePoint
Gestión de clientes / entidades contratantes	Facturación, gestión comercial y cumplimiento contractual con entidades del sector público	Datos identificativos, de contacto y financieros	Entidades públicas contratantes	Ejecución de contrato y obligación legal	SRI, SERCOP, sistemas administrativos (ODOO)	No aplica o eventual (ODOO puede operar en nube)	Según normativa tributaria	Usuarios y contraseñas, control de accesos en ODOO
Gestión de proveedores	Registro y coordinación de proveedores de bienes y servicios; compras con factura	Datos identificativos y financieros (RUC, datos de facturación)	Proveedores (~50 anuales)	Ejecución de relación comercial / obligación legal tributaria	Proveedor contable externo (compañía	No aplica	Durante la relación comercial y según normativa tributaria	Acceso restringido, gestión documental segura en SharePoint
Gestión contable	Registro contable, cumplimiento tributario y financiero	Datos identificativos y financieros de empleados, clientes y	Empleados, entidades contratantes y	Obligación legal	Sistema contable ODOO, proveedor	Posible (ODOO puede operar en nube)	Según normativa tributaria	Control de accesos, autenticación en ODOO, respaldos
Gestión de proyectos	Planificación, ejecución y control de proyectos adjudicados (obra civil, construcción, call center, fotovoltaje)	Datos identificativos básicos del personal asignado al proyecto	Empleados y prestadores de servicios	Ejecución de contrato / interés legítimo	Entidades contratantes públicas	No aplica	Durante la relación contractual y según normativa de contratación pública	Accesos controlados, supervisión interna, documentación en SharePoint
Seguridad de la información	Protección de la información y datos personales tratados contra accesos no autorizados	Todos los datos personales tratados por ESPOLTEL	Todos los titulares	Obligación legal	Proveedores tecnológicos (si aplica); TICS — Ing. Oswaldo Solano	No aplica	Según finalidad del tratamiento	Antivirus, firewall, copias de seguridad, políticas de seguridad, control de acceso a SharePoint y ODOO

⚠ Las filas en amarillo corresponden a tratamiento de datos de categoría especial (datos de salud) conforme al Art. 26 de la LOPDP. Requieren medidas reforzadas.

Gestión de Riesgos y Evaluaciones de Impacto (PIA/DPIA)

ESPOLTEL S.A. implementará una metodología de gestión de riesgos orientada a la protección de datos personales, conforme a la LOPDP y buenas prácticas de ISO/IEC 27001:2022.

Mapa de Riesgos Identificados

Riesgo	Activo afectado	Probabilidad	Impacto	Nivel de riesgo	Tratamiento
Acceso no autorizado a datos personales en la nube (SharePoint / ODOO)	Bases de datos de empleados, proveedores y clientes	Media	Alto	Alto	Implementar control de accesos por roles, autenticación multifactor y monitoreo de accesos
Fuga de información financiera o contractual	Sistema contable y facturación electrónica	Media	Alto	Alto	Cifrado de datos, políticas de contraseñas robustas y auditorías periódicas
Pérdida de información por fallos técnicos o ausencia de respaldos	Información almacenada en la nube y sistemas internos	Baja	Alto	Medio	Implementar copias de seguridad automáticas y planes de recuperación
Uso indebido de datos biométricos (huellas)	Sistema de control de asistencia	Media	Alto	Alto	Cifrado de datos biométricos y restricción estricta de accesos
Acceso indebido a datos de salud (auditorías médicas)	Expedientes médicos digitales	Media	Muy alto	Crítico	Aplicar medidas reforzadas: cifrado fuerte, control estricto de accesos, acuerdos de confidencialidad
Transferencia internacional de datos sin garantías adecuadas	Datos de pacientes (transferencias a Colombia)	Baja	Muy alto	Alto	Verificar cláusulas contractuales y cumplimiento de estándares internacionales
Intercepción o manipulación de datos en facturación electrónica	Sistema de facturación	Baja	Alto	Medio	Uso de canales seguros (HTTPS), firmas electrónicas y validaciones
Acceso no autorizado a sistemas internos Por falta de control de usuarios	Sistemas tics (ODDO, sharepoint)	Media	Alto	Alto	Gestión de identidades, autenticación Multifactor y revisión periódica de usuarios
Falta de capacitación del personal en protección de datos	Todos los activos de información	Alta	Medio	Alto	Programas de capacitación continua y concienciación
Eliminación o conservación inadecuada de datos	Bases de datos institucionales	Media	Medio	Medio	Políticas de retención y eliminación segura de información
Fallas en proveedores tecnológicos (nube, contable)	Infraestructura tecnológica tercerizada	Baja	Alto	Medio	Evaluación de proveedores y acuerdos de nivel de servicio (SLA)
Acceso físico no autorizado a instalaciones o equipos	Equipos y archivos físicos	Baja	Medio	Bajo	Control de accesos físicos y vigilancia

Supuestos para realizar DPIA

Se realizarán Evaluaciones de Impacto (DPIA) en los siguientes casos conforme al Art. 39 RGLOPDP:

- Tratamiento a gran escala de datos sensibles (salud, datos psicológicos de menores).
- Uso de sistemas de videovigilancia con capacidades de reconocimiento biométrico.
- Transferencias internacionales de datos personales.

Objetivos del SGPDP e Indicadores

Objetivo	Indicador	Meta	Frecuencia
Cumplimiento de la LOPDP	% requisitos cumplidos	≥ 90 %	Semestral
Capacitación del personal	% personal capacitado en LOPDP	100 %	Anual
Atención de solicitudes ARCO	Tasa de respuesta en plazo legal	100 %	Mensual
Gestión de incidentes	Incidentes notificados en plazo (3 días)	100 %	Por evento
Actualización del RAT	RAT revisado conforme a cambios	100 %	Anual
Madurez de controles ISO 27001	Promedio de madurez (escala 0-5)	≥ 3.5	Anual
Contratos con encargados vigentes	% proveedores con contrato firmado	100 %	Semestral
Consentimientos obtenidos	% titulares con consentimiento documentado	100 %	Anual

TIPOS Y CATEGORIAS DE DATOS PERSONALES

Con respecto al tratamiento de datos personales de los empleados, proveedores, clientes y prestadores de servicios (LOPDP, Art. 4): procesamos la siguiente información:

- **Datos de identificación y contacto:** Nombre completos, tipo de documento de identificación, nro. de documento de identificación, números telefónicos, correos electrónicos, dirección de domicilio o comercial, datos adicionales por emergencia.
- **Datos sensibles:** Datos relativos de salud, certificados médicos, información financiera con relación a los pagos de salarios, registros contables, datos biométricos, de videovigilancia.

- **Datos de Tracking:** Datos relacionados a ubicación por plataformas del servicio de transporte, metadatos de imagen por sistemas de videovigilancia, datos de registro digitales por redes sociales o página web, cookies.

Respecto de los datos que ESPOLTEL S.A. maneja, se identifican las siguientes categorías:

- **Datos de identificación y contacto:** Nombre completos, tipo de documento de identificación, nro. de documento de identificación, números telefónicos, correos electrónicos, dirección de domicilio o comercial, referencias, datos de contacto para emergencias.
- **Datos sensibles:** Datos biométricos, datos de videovigilancia, datos relativos de salud, certificados médicos, datos bancarios, datos de información financiera para los pagos de nómina y obligaciones laborales, datos de obligaciones relativas a las leyes como impuesto a la renta, ley violeta, ley de discapacidad, entre otras.
- **Metadatos:** Datos relacionados con el uso de plataformas (nube, ODOO, SharePoint, etc.) como: ID de usuario, fecha y hora de acceso, dirección IP de conexión, entre otros.

USO Y DISPOSICIÓN DEL TRATAMIENTO DE DATOS PERSONALES

La empresa reconoce y respeta el derecho a la privacidad de los titulares de datos personales, comprometiéndose a tratarlos de forma lícita, leal, transparente y conforme a la Ley Orgánica de Protección de Datos Personales (LOPDP) del Ecuador y su normativa aplicable. En este capítulo se detallan las bases legales que habilitan el tratamiento de datos personales dentro de la organización, en el marco de la ejecución de proyectos mediante contratación pública.

Consentimiento

En el desarrollo de las actividades de la empresa, se podrá solicitar el consentimiento del titular para el tratamiento de sus datos personales, especialmente en procesos de reclutamiento, registro de proveedores, visitas a instalaciones o uso de plataformas digitales.

Este consentimiento podrá ser recolectado mediante formularios físicos o digitales informando siempre la finalidad del tratamiento, conforme a la LOPDP (Art. 7, num. 1).

Ejecución de relaciones contractuales

El tratamiento de datos personales es necesario para la ejecución de contratos con entidades del sector público, proveedores, contratistas, subcontratistas y personal de la empresa.

Esto incluye la gestión de procesos de contratación pública, ejecución de obras civiles, auditorías médicas, proyectos energéticos, administración financiera y facturación electrónica, estableciendo derechos y obligaciones entre las partes, conforme a la LOPDP (Art. 7, num. 2).

Obligaciones legales

La compañía está obligada a recopilar, almacenar, procesar y, en ciertos casos, compartir información personal en cumplimiento de la normativa ecuatoriana, incluyendo disposiciones tributarias, laborales, de contratación pública y regulatorias emitidas por entidades de control.

Estas obligaciones pueden incluir el uso de sistemas contables, plataformas de facturación electrónica y reportes a entidades públicas, garantizando en todo momento la protección de los derechos de los titulares, conforme a la LOPDP (Art. 7, num. 3).

Interés legítimo

En determinadas actividades, la empresa podrá tratar datos personales con base en su interés legítimo, siempre que no prevalezcan los derechos y libertades fundamentales de los titulares.

Esto incluye, entre otros fines, la gestión de seguridad física y digital, control de accesos mediante sistemas biométricos, videovigilancia en instalaciones, administración de sistemas en la nube, mejora de procesos internos, control de calidad en proyectos y prevención de riesgos operativos y de seguridad de la información, conforme a la LOPDP (Art. 7, num. 8).

FINES DEL TRATAMIENTO DE DATOS PERSONALES

ESPOLTEL en el desempeño de sus actividades relacionadas con la postulación y ejecución de proyectos debe recolectar, administrar, archivar y utilizar datos de sus clientes, proveedores, Trabajadores y prestadores de servicios con las siguientes finalidades:

- **Gestión precontractual, contractual y ejecución de contratos públicos:** Recopilar y tratar datos personales de clientes, funcionarios públicos, proveedores, subcontratistas y personal técnico necesarios para participar en procesos de contratación y ejecutar obligaciones contractuales con entidades reguladas por el Servicio Nacional de Contratación Pública.
- **Cumplimiento de obligaciones legales y regulatorias:** Atender requerimientos de información, auditorías, fiscalizaciones y controles por parte de autoridades competentes, incluyendo entidades como el Ministerio de Salud Pública del Ecuador y otros organismos de control.
- **Gestión y ejecución de proyectos:** Administrar la información necesaria para la planificación, supervisión, control técnico y operativo de obras civiles, auditorías médicas e instalaciones energéticas, incluyendo datos de identificación y contacto de las partes involucradas.
- **Ejecución de auditorías médicas:** Tratar datos personales y datos sensibles de salud exclusivamente para fines de evaluación, control y verificación de servicios médicos, bajo estrictas medidas de confidencialidad y seguridad.
- **Gestión del talento humano:** Administrar datos personales de Trabajadores, técnicos y trabajadores de campo para procesos de selección, contratación, cumplimiento de obligaciones laborales, seguridad y salud ocupacional.
- **Gestión administrativa, financiera y de control:** Procesar datos para facturación, pagos, cumplimiento tributario, auditorías internas y externas, así como rendición de cuentas ante entidades públicas.

- **Gestión de seguridad de la información y control de accesos:** Proteger las instalaciones, sistemas y activos de la organización mediante mecanismos de control físico y lógico.
- **Relación con terceros y cadena de suministro:** Compartir datos personales con subcontratistas, consultores, aliados estratégicos y proveedores, cuando sea necesario para la ejecución de contratos públicos, garantizando el cumplimiento de obligaciones de confidencialidad y protección de datos.
- **Transparencia y rendición de cuentas:** Cumplir con principios de publicidad y acceso a la información en el marco de la contratación pública, asegurando el adecuado equilibrio entre transparencia y protección de datos personales.

PROCESO PARA EJERCER DERECHOS ARCO

ESPOLTEL S.A., respeta tus derechos sobre información personal conforme a la LOPDP. En ese sentido, los titulares podrán ejercer los siguientes derechos:

- **Acceso:** Conocer qué datos personales posee la Empresa y cómo los trata.
- **Rectificación y actualización:** Solicitar la corrección de datos inexactos o incompletos.
- **Eliminación:** Solicitar la supresión de datos cuando no exista base legal para su tratamiento.
- **Oposición:** Oponerse al tratamiento en determinados supuestos.
- **Portabilidad:** Solicitar la entrega de sus datos en formato estructurado cuando proceda.
- **Suspensión del tratamiento:** Solicitar la limitación temporal del uso de sus datos.

Para el personal administrativo, estos derechos se extienden a toda la información laboral que procesamos, incluyendo datos de contratación, evaluaciones de desempeño, información salarial y prestaciones sociales. Los Trabajadores pueden solicitar acceso a su expediente laboral, rectificar información profesional incorrecta, y ejercer sus derechos respecto a datos que no sean esenciales para la relación laboral o el cumplimiento de obligaciones legales.

Proceso y Diagrama de Flujo ARCO

DIAGRAMA DE FLUJO — PROCESO PARA EJERCER DERECHOS ARCO		
1	RECEPCIÓN	El titular de datos personales presenta su solicitud ARCO a través de los canales habilitados: · Correo electrónico: dpd@espoltel.com · Entrega física: Km. 30,5 Vía Perimetral, Campus ESPOL · Formulario institucional (Anexo 6)
▼		
2	REGISTRO	El responsable designado registra la solicitud en el sistema interno: · Asigna número de trámite único · Registra fecha de ingreso (inicia cómputo del plazo de 15 días hábiles) · Identifica el derecho solicitado y datos del titular
▼		

3	**VERIFICACIÓN DE IDENTIDAD**	Se valida la identidad del solicitante y la completitud de la solicitud: • Titular directo: cédula de ciudadanía o pasaporte • Tercero representante: poder notarial debidamente otorgado
	¿SOLICITUD COMPLETA?	✓ **SÍ → Continúa al Paso 4** ✗ NO → Se solicita información adicional al titular y se SUSPENDE el plazo hasta que la aclare. Una vez completada, regresa al Paso 3.
4	**ANÁLISIS JURÍDICO-ADMINISTRATIVO**	Se evalúa si el derecho solicitado procede, considerando: • Obligaciones legales de conservación de datos • Existencia de relación contractual vigente que requiera el tratamiento • Posible afectación a derechos de terceros • Existencia de interés legítimo debidamente fundamentado
◆	**DECISIÓN** **¿PROCEDE EL DERECHO?**	✓ **SÍ PROCEDE →** Emitir respuesta FAVORABLE en el Paso 5 ✗ **NO PROCEDE →** Emitir NEGATIVA MOTIVADA en el Paso 5, indicando las causales
5	**RESPUESTA FORMAL**	Se emite respuesta motivada al titular dentro del plazo máximo de 15 días hábiles. Si la respuesta es FAVORABLE: se informa la acción realizada sobre los datos. Si la respuesta es DENEGATORIA: se indica la causal específica de la negativa y los recursos disponibles ante la SPDP. Medio de respuesta: el indicado por el titular en su solicitud.
6	**REGISTRO DE RESPUESTA**	Se documenta la decisión adoptada en el Registro Interno de Solicitudes ARCO , incluyendo los siguientes campos: 1. Número de trámite 2. Nombre del solicitante 3. Derecho ejercido 4. Fecha de recepción 5. Fecha de respuesta 6. Decisión adoptada (favorable o denegatoria con motivación) Toda la información del registro se trata con estrictas medidas de seguridad y confidencialidad.

IMPORTANTE: El plazo de 15 días hábiles se suspende si la solicitud está incompleta (Paso 3) y se reanuda una vez el titular aclara la información requerida. La negativa de la solicitud siempre debe estar motivada, ser notificada en el plazo legal y el titular puede impugnarla ante la SPDP.

Canales para presentar solicitudes

Los titulares podrán presentar sus solicitudes mediante:

- Correo electrónico: dpd@espoltel.com
- Entrega física: Oficina administrativa - Km. 30,5 Vía Perimetral, Campus ESPOL, Guayaquil, Ecuador.
- Formulario establecido por la Institución (ver Anexo 6)

Requisitos de la solicitud

1. Nombres y apellidos completos del titular.
2. Número de identificación.
3. Derecho que desea ejercer.
4. Descripción clara de la petición.
5. Medio para recibir respuesta.
6. Documentación de respaldo, si aplica.

En caso de que actúe un tercero en representación del titular, deberá acreditarse la representación legal mediante poder debidamente notariado.

Procedimiento Interno

Una vez recibida la solicitud, la Institución cumplirá con el siguiente procedimiento interno:

- **Recepción y registro:** Se asignará un número de trámite y fecha de ingreso.
- **Verificación de identidad:** Se validará la identidad del solicitante para evitar suplantaciones.
- **Análisis jurídico-administrativo:** Se verificará si procede el derecho solicitado, considerando obligaciones legales, contractuales o interés legítimo.
- **Respuesta formal:** Se emitirá respuesta motivada dentro de los plazos legales.
- **Registro de respuesta:** Se tomará registro de la respuesta motivada que emita la Empresa al titular.

Plazos de respuesta
La Empresa atenderá las solicitudes dentro del plazo de 15 días desde la recepción de la solicitud de conformidad a la normativa vigente ecuatoriana. Si la solicitud es incompleta, se requerirá información adicional, suspendiéndose el plazo hasta su aclaración.

Casos en que puede negarse la solicitud

La empresa podrá negar total o parcialmente la solicitud cuando:

- Exista obligación legal de conservar los datos.
- El tratamiento sea necesario para el cumplimiento de una relación contractual vigente.
- Afecte derechos de terceros.
- Exista interés legítimo debidamente fundamentado.

La negativa deberá estar debidamente motivada y notificada al titular dentro del plazo de 15 días hábiles. El titular podrá impugnar la negativa ante la Superintendencia de Protección de Datos Personales (SPDP).

Registro de Solicitudes

La Institución mantendrá un **Registro Interno de Solicitudes ARCO**, que incluirá:

No.	Campo del Registro	Descripción
1	**Número de trámite**	Identificador único asignado a cada solicitud recibida.
2	**Nombre del solicitante**	Nombres y apellidos completos del titular o su representante legal.
3	**Derecho ejercido**	Tipo de derecho solicitado: Acceso, Rectificación, Eliminación, Oposición, Portabilidad o Revocación.
4	**Fecha de recepción**	Fecha en que se recibió la solicitud. Marca el inicio del cómputo del plazo legal.
5	**Fecha de respuesta**	Fecha en que se emitió y notificó la respuesta formal al titular.
6	**Decisión adoptada**	Resultado del proceso: favorable (con descripción de la acción ejecutada) o denegatoria (con la causal motivada).

Toda la información relacionada con las solicitudes será tratada bajo estrictas medidas de seguridad y confidencialidad.

CONSENTIMIENTO INFORMADO DEL TITULAR DE LOS DATOS PERSONALES

La empresa garantizará que el tratamiento de datos personales se realice sobre la base de un consentimiento previo, libre, específico, informado e inequívoco. (LOPDP, Art. 7, núm.1). El consentimiento deberá ser: Libre, Específico, Informado e Inequívoco.

El titular podrá revocar su consentimiento en cualquier momento sin efectos retroactivos. (Ver Anexo 5).

Diagrama de Flujo - Consentimiento

DIAGRAMA DE FLUJO — OBTENCIÓN DE CONSENTIMIENTO INFORMADO		
1	**IDENTIFICAR NECESIDAD**	Se determina si el tratamiento requiere consentimiento o se basa en otra base legal (contrato, ley, interés legítimo)
▼		
2	**INFORMAR AL TITULAR**	Se comunica: identidad responsable, finalidades, base legal, destinatarios, plazo conservación, derechos y canales
▼		

3	**OBTENER CONSENTIMIENTO**	Se recaba el consentimiento libre, específico, informado e inequívoco — Medios: físico, electrónico o digital
4	**CONSERVAR EVIDENCIA**	Se archiva el formulario firmado o registro digital con fecha, medio y contenido del consentimiento
5	**GESTIONAR REVOCATORIA**	Si el titular revoca: cesar el tratamiento no obligatorio, documentar la revocatoria, notificar a encargados

Para tal efecto, se establecen las siguientes disposiciones:

1. **Obtención del consentimiento:**
   La Institución solicitará el consentimiento del titular de los datos personales, o de su representante legal cuando se trate de niños, niñas y adolescentes, de manera previa a la recolección y tratamiento de sus datos personales.
2. **Condiciones del consentimiento:**
   El consentimiento deberá cumplir con las siguientes características:
   - **Libre:** otorgado sin vicios de voluntad.
   - **Específico:** referido a una o varias finalidades determinadas.
   - **Informado:** basado en información clara, accesible y comprensible.
   - **Inequívoco:** expresado mediante una acción afirmativa clara.
3. **Información mínima al titular:**
   Al momento de recabar el consentimiento, la Institución informará al titular, al menos, lo siguiente:
   - La identidad y datos de contacto de la Institución como responsable del tratamiento.
   - Las finalidades específicas del tratamiento de los datos personales.
   - La base legal que legitima el tratamiento.
   - Las posibles transferencias o comunicaciones de datos.
   - El tiempo de conservación de los datos personales.
   - Los derechos que le asisten (acceso, rectificación, actualización, eliminación, oposición, entre otros) y los canales para ejercerlos.
   - Las consecuencias de no proporcionar los datos cuando estos sean necesarios.
4. **Medios para otorgar el consentimiento:**
   El consentimiento podrá recabarse por medios físicos, electrónicos o digitales, siempre que permita dejar constancia verificable de su otorgamiento.
5. **Revocatoria del consentimiento:**
   El titular podrá revocar su consentimiento en cualquier momento, sin efectos retroactivos, mediante los mecanismos establecidos por la Institución, sin que ello afecte la licitud del tratamiento realizado con anterioridad.
6. **Excepciones al consentimiento:**

No será necesario el consentimiento cuando el tratamiento se fundamente en otras bases de legitimación previstas en la ley, tales como el cumplimiento de obligaciones legales, el interés público, la ejecución de una relación contractual o la protección de intereses vitales del titular.

7. **Conservación de la prueba del consentimiento:**

La Institución deberá conservar evidencia del consentimiento otorgado por el titular, durante el tiempo que dure el tratamiento de los datos personales y conforme a los plazos legales aplicables.

GESTIÓN DE CONTRATOS POR TRATAMIENTO DE DATOS PERSONALES CON ENCARGADOS (PROVEEDORES EXTERNOS)

ESPOLTEL S.A., en calidad de responsable del tratamiento de datos personales, podrá recurrir a terceros para que actúen como encargados del tratamiento, cuando resulte necesario para la administración y manejo adecuado de la empresa o para la ejecución de los proyectos y obras para los que se les haya contratado, garantizando en todo momento el cumplimiento de la normativa vigente en materia de protección de datos personales en el Ecuador. (LOPDP, Art. 26).

Diagrama de Flujo - Gestión de Encargados

DIAGRAMA DE FLUJO - GESTIÓN DE CONTRATOS POR TRATAMIENTO DE DATOS PERSONALES CON ENCARGADOS (PROVEEDORES EXTERNOS)		
1	IDENTIFICAR ENCARGADO	Se detecta que un proveedor o tercero tratará datos personales de la institución
▼		
2	EVALUACIÓN DEL PROVEEDOR	Se verifica capacidad técnica, medidas de seguridad y antecedentes del potencial encargado
▼		
3	NEGOCIACIÓN Y CONTRATO	Se elabora y firma el Contrato de Encargo de Tratamiento con todas las cláusulas obligatorias (Anexo 7)
▼		
4	SUPERVISIÓN ACTIVA	Se realiza seguimiento periódico del cumplimiento: auditorías, reportes, verificación de incidentes
▼		
5	FIN DEL CONTRATO	El encargado devuelve o elimina los datos; se documenta el cierre y se archiva la evidencia

El tratamiento deberá estar regulado mediante contrato de encargo (ver Anexo 7). Las obligaciones del encargado incluyen: tratar datos solo conforme a instrucciones de la empresa, garantizar confidencialidad, implementar medidas de seguridad apropiadas, no utilizar datos para fines propios y notificar sin dilación cualquier vulneración de seguridad.

- **Subencargados:** no podrán subcontratar sin autorización previa y escrita.

- **Transferencias internacionales:** el encargado deberá garantizar niveles adecuados de protección.
- **Fin del contrato:** el encargado deberá devolver o eliminar todos los datos personales tratados.

TIEMPO DE CONSERVACIÓN

- **Datos de trabajadores:** mientras dure la relación laboral + 15 años tras finalización
- **Datos de clientes:** mientras dure la relación comercial + 7 anos
- **Datos de proveedores y prestadores de servicios:** mientras dure la relación comercial + 7 anos
- **Datos financieros:** 7-10 años según normativa SRI.
- **Imágenes de videovigilancia:** hasta 30 días, salvo que constituyan evidencia en procesos.
- **Registros de solicitudes ARCO:** 7 años.

La eliminación de datos se realizará mediante procesos seguros que garanticen que los datos sean irrecuperables. (RGLOPDP, Art. 41).

MEDIDAS DE SEGURIDAD

Medidas de Seguridad Implementadas

ESPOLTEL S.A. implementa las siguientes medidas de seguridad:

- Control de acceso físico a instalaciones y archivos
- Contraseñas seguras y acceso restringido a sistemas
- Confidencialidad del personal con acceso a datos
- Copias de seguridad periódicas
- Procedimiento de respuesta ante incidentes de seguridad
- Eliminación segura de datos al término de su ciclo de vida

Las medidas incluyen videovigilancia en áreas sensibles, alarmas de seguridad, archivos bajo llave para documentos físicos, protocolos de limpieza de escritorios y eliminación segura de documentos confidenciales.
Gestión de Incidentes y Transferencias: Mantenemos protocolos de respuesta inmediata ante incidentes de seguridad, incluyendo evaluación de impacto, medidas correctivas y notificación a autoridades cuando sea requerido. Las transferencias de datos a terceros se realizan únicamente a través de canales seguros y con contratos que garantizan estándares de seguridad equivalentes.

Realizamos evaluaciones semestrales de nuestras medidas de seguridad, auditorías internas y actualizaciones tecnológicas para mantener la protección efectiva de toda la información personal confiada a nuestra empresa.

Respecto a los incidentes y brechas de seguridad que se puedan generar dentro de la empresa se ha establecido el siguiente procedimiento:

Diagrama de Flujo - Procedimiento de Gestión de Incidentes - 7 Pasos

DIAGRAMA DE FLUJO - PROCEDIMIENTO DE GESTIÓN DE INCIDENTES (7 PASOS)		
1	**DETECTAR Y REPORTAR** (INMEDIATO)	Reportar INMEDIATAMENTE al Coordinador de Seguridad: • Por teléfono, WhatsApp, email o en persona • No esperes "a estar seguro" - reporta la sospecha Indicando: • ¿Qué pasó? • ¿Cuándo ocurrió? • ¿Qué datos están afectados? • ¿Cuántas personas afectadas? • ¿Dónde está la información (archivo, documento físico)? Ejemplos de situaciones a reportar: • "Envié por error un email con datos de un trabajador a otra persona" • "No encuentro la carpeta con certificados médicos" • "Se perdió un USB con información de empleados" • "Alguien accedió a archivos sin autorización" • "Se eliminó por error un archivo Excel con datos personales" • Por teléfono, WhatsApp, email o en persona • No esperes "a estar seguro" - reporta la sospecha
▼		
2	**REGISTRO INICIAL** (MISMO DÍA)	El Coordinador registra el incidente en el Formato de Registro (Anexo 8): • Fecha/hora de detección. • Quién reporta. • Descripción del incidente. • Datos afectados. Personas afectadas.
▼		
3	**CONTENER LA BRECHA** (PRIMERAS 24 H)	Acciones inmediatas según el tipo de brecha: **Si fue ENVÍO ERRÓNEO de información:** 1. Contactar al receptor y solicitar eliminación inmediata. 2. Confirmar que eliminó la información. 3. Verificar si compartió con alguien más. **Si fue PÉRDIDA/ROBO de documentos o dispositivos:** 1. Verificar última ubicación conocida. 2. Buscar en lugares probables. 3. Alertar a personal para que estén atentos. 4. Si no aparece en 24h, asumir como pérdida definitiva. **Si fue ACCESO NO AUTORIZADO:** 1. Identificar quién accedió.

		2. Cambiar contraseñas o restringir accesos. 3. Verificar qué hizo con la información. **Si fue ELIMINACIÓN ACCIDENTAL:** 1. Verificar si existe respaldo. 2. Intentar recuperación del archivo. Identificar qué información se perdió definitivamente
4	**EVALUAR EL RIESGO** (PRIMERAS 48 H)	El Coordinador clasifica el nivel de riesgo: **RIESGO ALTO (Notificar a autoridades Y a afectados)** · Afecta datos de salud (certificados médicos/reposos). · Más de 5 personas afectadas. · Los datos se divulgaron públicamente o a terceros. · Se perdió totalmente el control de los datos. · Hay riesgo de discriminación o perjuicio grave **RIESGO MEDIO (Notificar solo a autoridades)** · Afecta datos personales generales. · Entre 2-5 personas afectadas. · Acceso fue interno, pero no autorizado. · Hay respaldo de la información **RIESGO BAJO (Solo documentar internamente)** · Afecta a 1 persona con datos mínimos. · El acceso fue controlado rápidamente. · No hay riesgo real de perjuicio. Se recuperó toda la información
5	**NOTIFICAR** **(SEGÚN NIVEL)**	**A. Si es RIESGO ALTO o MEDIO - Notificar a AUTORIDADES:** Enviar notificación a: • Superintendencia de Protección de Datos Personales (SPDP) • Agencia de Regulación y Control de Telecomunicaciones (ARCOTEL) **Plazo:** Máximo 3 días desde detección **Medio:** Email institucional o plataforma oficial (verificar en web de SPDP/ARCOTEL) **Contenido mínimo:** · Datos de la Empresa y contacto · Qué pasó y cuándo · Cuántas personas afectadas y qué datos · Causa del incidente · Qué medidas se tomaron · Nivel de riesgo y por qué **B. Si es RIESGO ALTO - Notificar a PERSONAS AFECTADAS:** **Plazo:** Máximo 5 días desde detección **Medio:** Llamada + email/WhatsApp, o carta en mano **Contenido:**

		• Qué pasó (en lenguaje simple) • Qué datos suyos se afectaron • Qué riesgos existen para ellos • Qué hemos hecho • Qué pueden hacer ellos • Cómo contactarnos **NO notificar a personas si:** • Los datos estaban cifrados/protegidos y son ilegibles • Se recuperó toda la información antes de que alguien la viera • El esfuerzo es desproporcionado (justificar muy bien)
▼		
6	**REMEDIAR Y PREVENIR (PRIMEROS 15 DÍAS)**	**Implementar mejoras:** • Corregir la causa raíz • Reforzar medidas de seguridad • Capacitar al personal si es necesario **Documentar lecciones aprendidas:** • ¿Por qué pasó? • ¿Qué falló? • ¿Cómo evitarlo en el futuro? **Actualizar procedimientos si es necesario**
▼		
7	**CERRAR EL CASO**	1. Verificar que se completaron todas las acciones. 2. Cerrar el registro del incidente. 3. Archivar toda la documentación (mínimo 5 años).

ACTUALIZACIÓN DE LA POLÍTICA

Nos reservamos el derecho de actualizar esta Política cuando sea necesario para cumplir con nuevas leyes o mejorar en la seguridad. Te informaremos sobre las modificaciones mediante nuestros canales de comunicación habituales y publicaremos la versión actualizada en nuestro sitio web con la fecha de revisión correspondiente.

Te recomendamos consultar esta Política para mantenerte informado sobre posibles cambios y contactarnos si tienes dudas sobre alguna modificación. Actualizamos nuestra Política con el objetivo de fortalecer continuamente la seguridad y privacidad de tu información, adaptándonos a los cambios normativos y asegurando que tus datos estén siempre protegidos.

Nro. Documento:	PO_PDP_001	**Aprobación**	Gerencia General
Fecha de Vigencia	dic-25	**Versión**	SG-PDP-01.00

ESPOLTEL S.A. informa que la información contenida en la presente Política de Protección de Datos Personales es de uso exclusivo de la empresa y sus colaboradores autorizados. Los datos personales registrados y tratados conforme a este documento se encuentran protegidos bajo la normativa ecuatoriana vigente, en particular la Ley Orgánica de Protección de Datos Personales (LOPDP), su Reglamento, y demás disposiciones aplicables emitidas por la Superintendencia de Protección de Datos Personales (SPDP).

Queda prohibida la reproducción, distribución o divulgación no autorizada de este documento o de cualquier información personal contenida en las bases de datos de la Empresa.

Firmado electrónicamente por:
JORGE LUIS CARDENAS MUGA
Validar únicamente con FirmaEC

ANEXO 1: TABLA DE CUMPLIMIENTO LEGAL

Diagnóstico de cumplimiento LOPDP y RGLOPDP - ESPOLTEL S.A. - Diciembre 2025

No.	Requisito Evaluado	Cumplimiento	Observación
1	¿Se ha designado al Delegado de Protección de Datos Personales?	**SI CUMPLE**	DPD designado formalmente. Pendiente formalización mediante resolución interna.
2	¿Han firmado los empleados acuerdos de confidencialidad (NDA)?	**SI CUMPLE**	Acuerdos suscritos con los 119 trabajadores y los 7 prestadores de servicios.
3	¿Han firmado los empleados consentimiento informado para el tratamiento de sus datos personales?	**SI CUMPLE**	Consentimientos informados implementados para datos laborales.
4	¿Se dispone de consentimientos informados para la recolección de datos de terceros (clientes, proveedores, prestadores)?	**SI CUMPLE**	Cubre entidades contratantes, proveedores (~50) y prestadores de servicios (7).
5	¿Se ha implementado un procedimiento para la atención de titulares que quieran ejercer sus derechos ARCO?	**SI CUMPLE**	Procedimiento ARCO documentado. Canal habilitado: dpd@espoltel.com.
6	¿Se ha implementado un procedimiento de respuesta a incidentes de seguridad de datos personales?	**SI CUMPLE**	Protocolo de gestión de brechas de seguridad documentado e implementado.
7	¿Se organizan programas de capacitación para formar y concienciar al personal en protección de datos?	**SI CUMPLE**	Programa de capacitación implementado. Requiere periodicidad anual documentada.
8	¿Se dispone de aviso de política de privacidad en la página web institucional?	**NO CUMPLE**	Pendiente de publicación en sitio web. Prioridad Media.
9	¿Se han realizado Evaluaciones de Impacto de Tratamiento de Datos Personales (EIPD/DPIA)?	**NO CUMPLE**	*Pendiente de implementación. OBLIGATORIO para datos biométricos (biometría) y datos de salud (auditorías médicas IESS). Prioridad Alta.*
10	¿Se han suscrito contratos de encargo de tratamiento con proveedores que manejen datos personales?	**SI CUMPLE**	Suscritos con empresa aliada colombiana (auditorías IESS) y proveedor contable externo. Pendiente: ODOO (si opera en nube).
11	¿Se dispone del Registro de Actividades de Tratamiento (RAT)?	**SI CUMPLE**	RAT documentado con 11 actividades de tratamiento. Actualización semestral programada.
12	¿Se establecen criterios documentados de retención y eliminación segura de datos?	**NO CUMPLE**	*Se requiere definir política formal de retención por tipo de dato. Prioridad Alta.*
13	¿Se han implementado avisos de privacidad en videovigilancia, biometría u otros sistemas de captación?	**NO CUMPLE**	Señalética de videovigilancia en instalaciones pendiente de colocación. Biometría en proceso. Prioridad Media.
14	¿Se realizan revisiones y auditorías internas periódicas del SGPDP?	**NO CUMPLE**	*Programar primera auditoría interna para el segundo semestre 2026. Prioridad Media.*
15	¿Se cuenta con procedimientos de Protección de Datos por Diseño y por Defecto?	**NO APLICA**	No aplica en la etapa actual de implementación del SGPDP.

TOTAL ✓ SI CUMPLE: 9/15 ✕ NO CUMPLE: 1/15 EN PROCESO: 4/15 - NO APLICA: 1/15	**60.0 %**	**Diagnóstico Inicial - Diciembre 2025**

ANEXO 2: EVALUACIÓN DE CUMPLIMIENTO DE CONTROLES DE SEGURIDAD ISO 27001: 2022

Aplicada a ESPOLTEL S.A. – Diciembre 2025

Escala: 0=No aplica | 1=No implementado | 2=Parcialmente implementado | 3=Implementado | 4=Implementado y verificado | 5=Optimizado

Controles Organizacionales (Sección 5) - Cumplimiento: 60 %

No.	Control	Descripción	Nivel
5.1	**Políticas de seguridad de la información**	Se definen, aprueban y comunican al personal las políticas de seguridad.	**4**
5.2	**Roles y responsabilidades**	Se definen y asignan roles de seguridad de la información. Responsable TICS	**3**
5.3	**Segregación de deberes**	Se segregan las áreas de responsabilidad en conflicto.	**3**
5.4	**Responsabilidades de gestión**	La Gerencia General exige la aplicación de las políticas de seguridad.	**3**
5.5	**Contacto con autoridades**	Se mantiene contacto con autoridades pertinentes (SPDP, ARCOTEL, ARCERNNR).	**4**
5.6	**Contacto con grupos de interés**	Se mantiene contacto con foros especializados en seguridad.	**1**
5.7	**Inteligencia de amenazas**	Se recopila y analiza información sobre amenazas de seguridad.	**3**
5.8	**Seguridad en gestión de proyectos**	La seguridad se integra en los proyectos adjudicados (obra civil, fotovoltaje, call center).	**3**
5.9	**Inventario de activos**	Se desarrolla y mantiene un inventario de activos de información.	**3**
5.10	**Uso aceptable de activos**	Se establecen reglas para el uso aceptable de la información (ODOO, SharePoint).	**3**
5.31	**Legislación, regulaciones y contratos**	Se identifican los requisitos legales y contractuales de seguridad (LOPDP, LOSNCP, LOSPEE).	**3**
5.34	**Privacidad y protección de datos personales**	Se identifican y cumplen los requisitos de privacidad conforme a la LOPDP.	**3**

Controles de Personas (Sección 6) - Cumplimiento: 57.5 %

No.	Control	Descripción	Nivel
6.1	**Investigación de antecedentes**	Verificación de antecedentes del personal y prestadores de servicios.	**3**
6.2	**Términos y condiciones del empleo**	Los contratos laborales y de prestación de servicios incluyen responsabilidades de seguridad.	**3**
6.3	**Concienciación, educación y capacitación**	El personal recibe formación en seguridad de la información y protección de datos.	**3**
6.4	**Proceso disciplinario**	Existe un proceso formal para gestionar infracciones de seguridad.	**2**
6.5	**Responsabilidades tras la terminación**	Se gestionan las responsabilidades al finalizar la relación laboral o contractual.	**3**
6.6	**Acuerdos de confidencialidad**	Empleados (119) y prestadores (7) firmaron acuerdos de confidencialidad (NDA).	**4**

Controles Físicos (Sección 7) - Cumplimiento: 60 %

No.	Control	Descripción	Nivel
7.1	**Perímetros de seguridad física**	Se definen y usan perímetros para proteger áreas sensibles en las instalaciones de ESPOLTEL.	**3**
7.2	**Entrada física**	Se controla y registra el acceso físico a las instalaciones (sistema biométrico propio).	**4**

7.3	**Seguridad de oficinas y salas**	Las oficinas y áreas sensibles están aseguradas adecuadamente.	**3**
7.4	**Monitoreo físico**	Se realiza monitoreo continuo de instalaciones mediante CCTV (gestionado internamente).	**4**
7.7	**Escritorio y pantalla limpios**	Se aplica política de escritorio y pantalla limpios.	**2**
7.10	**Medios de almacenamiento**	Los medios de almacenamiento se gestionan durante su ciclo de vida.	**3**
7.14	**Eliminación segura de equipos**	Los equipos se eliminan o reutilizan de forma segura.	**3**

Controles Tecnológicos (Sección 8) - Cumplimiento: 60 %

No.	Control	Descripción	Nivel
8.1	**Dispositivos de usuario final**	Los dispositivos de usuario están protegidos (ODOO, SharePoint, correo institucional).	**3**
8.2	**Derechos de acceso privilegiado**	El acceso privilegiado está restringido y gestionado por TICS	**3**
8.3	**Restricción de acceso a información**	El acceso a la información está restringido por roles (SharePoint, ODOO).	**3**
8.5	**Autenticación segura**	Se implementan procedimientos de autenticación segura en sistemas.	**3**
8.7	**Protección contra malware**	Se implementa protección contra malware actualizada.	**3**
8.12	**Prevención de fuga de datos**	Se aplican medidas de prevención de fuga de datos. Refuerzo pendiente para datos de salud.	**2**
8.13	**Copia de seguridad**	Las copias de seguridad se mantienen y prueban regularmente (SharePoint y ODOO).	**3**
8.15	**Registro de eventos (logging)**	Se producen, almacenan y analizan registros de actividades en sistemas.	**3**
8.20	**Seguridad en redes**	Las redes están protegidas y administradas por el área TICS.	**3**
8.24	**Uso de criptografía**	Se definen reglas para el uso de criptografía. Pendiente refuerzo en datos biométricos y de salud.	**2**

Resumen por Área de Control

Área de Control	% Cumplimiento	Nivel promedio	Tendencia
Controles Organizacionales	60 %	3.0 / 5	Estable →
Controles de Personas	57.5 %	2.9 / 5	En mejora ↑
Controles Físicos	60 %	3.0 / 5	Estable →
Controles Tecnológicos	60 %	2.8 / 5	Estable →
PROMEDIO GENERAL	**59.4 %**	**2.9 / 5**	**Nivel Intermedio**

ANEXO 3: INVENTARIO DE ACTIVOS DE LA INFORMACIÓN

ESPOLTEL S.A. - Conforme al Control 5.9 ISO/IEC 27001:2022 y Art. 38 RGLOPDP - Diciembre 2025

ID	Activo de Información	Tipo	Categoría	Clasificación	Ubicación	Responsable
ACT-01	Sistema contable ODOO	Digital	Financiero / Comercial	**Confidencial**	Nube / Servidor interno	Área Financiera
ACT-02	SharePoint - Gestión documental corporativa	Digital	Administrativo / Jurídico	**Confidencial**	Nube (Microsoft 365)	TICS / Todas las áreas
ACT-03	Expedientes laborales del personal (contratos, nómina, evaluaciones)	Digital / Físico	RRHH	**Confidencial**	Servidor interno / Archivo físico	Talento Humano
ACT-04	Sistema biométrico (huella dactilar - control de asistencia)	Digital	RRHH / Seguridad	**SENSIBLE**	Servidor interno (ESPOLTEL)	TICS / Talento Humano
ACT-05	Sistema de videovigilancia CCTV (imágenes y grabaciones)	Digital	Seguridad	**SENSIBLE**	Servidor seguridad (ESPOLTEL)	Gerencia / TICS
ACT-06	Expedientes médicos IESS (auditorías - datos de salud)	Digital	Salud	**SENSIBLE**	Servidor / Empresa aliada Colombia	Coordinación de Proyectos
ACT-07	Base de datos de prestadores de servicios (7 personas)	Digital / Físico	Jurídico / RRHH	**Confidencial**	SharePoint / Archivo	Gerencia / Administración
ACT-08	Base de datos de proveedores (~50 anuales)	Digital / Físico	Compras	**Confidencial**	ODOO / Archivo físico	Área de Compras
ACT-09	Documentación de licitaciones SERCOP (propuestas, contratos adjudicados)	Digital / Físico	Jurídico / Comercial	**Confidencial**	SharePoint	Gerencia / Asesoría Jurídica Externa
ACT-10	Registros contables y tributarios (facturas, retenciones, declaraciones SRI)	Digital / Físico	Financiero	**Confidencial**	ODOO / Archivo físico	Financiera
ACT-11	Correo electrónico institucional	Digital	Comunicación	**Interno**	Nube (proveedor de correo)	TICS / Todas las áreas
ACT-12	Contratos con proveedores y encargados del tratamiento	Físico / Digital	Jurídico	**Confidencial**	Administración / SharePoint	Gerencia / Asesoría Jurídica
ACT-13	Registros de solicitudes ARCO	Digital / Físico	Jurídico	**Confidencial**	Oficina DPD / SharePoint	DPD / Rep. Legal

ACT-14	Credenciales y contraseñas de sistemas (ODOO, SharePoint, correo)	Digital	TI	**CRÍTICO**	Gestor de contraseñas / TICS	TICS
ACT-15	Documentación de proyectos adjudicados (obra civil, fotovoltaje, call center)	Digital / Físico	Operativo	**Interno**	SharePoint / Archivo físico	Coordinación de Proyectos

Clasificación de Datos Personales por Categoría

Clasificación	Descripción	Ejemplos en ESPOLTEL S.A.
SENSIBLE / CRÍTICO	Datos cuyo tratamiento inadecuado puede generar discriminación grave, perjuicio a derechos fundamentales o comprometer la seguridad operativa.	Datos biométricos (huella dactilar), datos de salud (expedientes IESS), credenciales y contraseñas de sistemas.
CONFIDENCIAL	Datos cuya divulgación no autorizada puede causar perjuicio a la empresa o a los titulares.	Expedientes laborales, contratos, nómina, propuestas de licitación SERCOP, datos financieros, datos de proveedores y prestadores.
INTERNO	Datos de uso interno, no destinados al público general.	Correos institucionales, documentación de proyectos, comunicaciones internas, registros operativos.
PÚBLICO	Datos que pueden ser divulgados sin restricción.	Nombre de ESPOLTEL S.A., RUC, dirección, teléfonos públicos, información publicada en SERCOP.

ANEXO 4: EVALUACIÓN DE LA POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

Aplicada a ESPOLTEL S.A. - Diciembre 2025

Esta evaluación verifica el grado de implementación de los componentes esenciales de la Política de Protección de Datos Personales conforme a la LOPDP y buenas prácticas internacionales.

No.	Componente evaluado	Estado	Puntaje	Acciones recomendadas
1	Política formal de protección de datos aprobada y publicada	**Implementado**	**4 / 5**	Revisar y actualizar anualmente.
2	Designación del Delegado de Protección de Datos (DPD)	**Implementado**	**4 / 5**	Formalizar mediante resolución institucional interna.
3	Registro de Actividades de Tratamiento (RAT) actualizado	**Implementado**	**4 / 5**	Actualizar semestralmente y ante nuevos tratamientos. RAT con 11 actividades documentadas.
4	Inventario de activos de información documentado	**Implementado**	**3 / 5**	Completar con valoración de riesgos por activo.
5	Procedimientos para ejercicio de derechos ARCO	**Implementado**	**4 / 5**	Difundir canales entre todo el personal y prestadores de servicios de ESPOLTEL.
6	Consentimientos informados para todos los tratamientos	**Implementado**	**4 / 5**	Actualizar formularios para prestadores de servicios y tratamientos de datos de salud (auditorías IESS).
7	Contratos de encargo con proveedores externos que manejan datos	**Implementado**	**3 / 5**	Completar con proveedor de ODOO (si opera en nube) y verificar vigencia del contrato con empresa aliada colombiana.
8	Evaluaciones de Impacto (EIPD/DPIA) realizadas	**No implementado**	**1 / 5**	*Realizar EIPD para: (1) datos biométricos y (2) datos de salud con transferencia internacional (auditorías IESS). Prioridad Alta.*
9	Medidas técnicas de seguridad (cifrado, control de accesos)	**Parcialmente implementado**	**3 / 5**	Reforzar cifrado en datos biométricos y expedientes médicos IESS. Mejorar control de accesos en SharePoint y ODOO.
10	Medidas físicas de seguridad (control de acceso, CCTV)	**Implementado**	**4 / 5**	Colocar señalética de videovigilancia en todas las instalaciones. Sistema CCTV operado internamente por ESPOLTEL.
11	Capacitación periódica del personal en protección de datos	**Parcialmente implementado**	**2 / 5**	*Implementar programa anual de capacitación. Incluir a los 7 prestadores de servicios y al personal del área TICS.*
12	Procedimiento de gestión de incidentes y brechas de seguridad documentado	**Implementado**	**4 / 5**	Realizar simulacros periódicos. Incluir protocolo específico para brechas en datos de salud e IESS.
13	Política de retención y eliminación segura de datos	**No implementado**	**1 / 5**	*Definir calendario de retención por tipo de dato, especialmente para*

				videovigilancia (30-90 días) y expedientes IESS.
14	Auditorías internas periódicas del SGPDP	**No implementado**	**1 / 5**	*Programar primera auditoría interna para segundo semestre 2026. Prioridad Media.*
15	Avisos de privacidad visibles en puntos de recolección de datos	**Parcialmente implementado**	**2 / 5**	*Instalar señalética en videovigilancia. Colocar avisos en formularios de ingreso, biométrico y en la página web.*
PUNTAJE TOTAL OBTENIDO		**44 / 75 - 58.7 % - Nivel de madurez: INTERMEDIO**		

Conclusiones de la Evaluación

ESPOLTEL S.A. muestra un nivel de madurez INTERMEDIO (58.7%) en la implementación de su Política de Protección de Datos Personales. Los componentes más sólidos son: la política formal aprobada, la designación del DPD, el RAT (con 11 actividades documentadas), los procedimientos ARCO y los consentimientos informados. Las principales brechas se encuentran en: la realización de Evaluaciones de Impacto (EIPD) -especialmente urgente para el tratamiento de datos biométricos y datos de salud con transferencia internacional a Colombia-, la definición de criterios de retención y eliminación de datos, la capacitación sistemática del personal, y la realización de auditorías internas periódicas.

Se recomienda enfocar los esfuerzos del próximo período en cerrar estas brechas prioritarias, lo que permitiría alcanzar un nivel de madurez superior al 80%.

ANEXO 5: Modelo de consentimiento para uso de datos personales

AUTORIZACIÓN DE USO Y PROTECCIÓN DE DATOS PERSONALES
ESPOLTEL S.A. - Consentimiento Informado del Trabajador

El TRABAJADOR declara que ha sido informado de manera clara y suficiente sobre el tratamiento de sus datos personales y, en virtud de lo dispuesto en la Ley Orgánica de Protección de Datos Personales (LOPDP), su Reglamento General (RGLOPDP) y normativa complementaria, otorga su consentimiento libre, expreso, específico, informado e inequívoco a favor de la compañía ESPOLTEL S.A., en adelante *ESPOLTEL*, para el tratamiento de sus datos personales con las siguientes finalidades:

1. **Gestión laboral y administrativa:** Para la administración de la relación laboral, registro y control de asistencia, gestión de nómina, pago de haberes, beneficios sociales, aportes al IESS, obligaciones fiscales, cumplimiento de reglamento interno y demás trámites derivados de la normativa laboral ecuatoriana. Incluye el tratamiento de documentos personales tales como actas de matrimonio, certificados médicos y datos académicos, en la medida en que sean requeridos para el cumplimiento de obligaciones laborales.

2. **Cumplimiento de obligaciones contractuales, legales y de contratación pública:** Para el cumplimiento de obligaciones derivadas de los contratos que ESPOLTEL mantiene con sus clientes y entidades contratantes, especialmente cuando se requiera la verificación del cumplimiento de obligaciones laborales o de seguridad social, o el control de ingreso a instalaciones. Incluye expresamente el uso de datos del trabajador (nombre, número de cédula, cargo, afiliación al IESS, certificado de aportes, rol de pagos u otra información pertinente) en propuestas de licitación y procesos de contratación pública ante el SERCOP y demás entidades públicas competentes.

3. **Atención de requerimientos de autoridades:** Para atender solicitudes, requerimientos, órdenes o disposiciones emitidas por autoridades administrativas, judiciales o de control (ministerios, juzgados, Superintendencias, IESS, SRI, Superintendencia de Protección de Datos Personales – SPDP- u otras entidades competentes), en el marco de procesos administrativos, judiciales o de fiscalización, así como para la defensa de los derechos e intereses legítimos de ESPOLTEL ante dichas instancias.

4. **Gestión de seguridad y salud ocupacional:** Para el cumplimiento de las disposiciones sobre prevención de riesgos laborales, control médico ocupacional, vigilancia epidemiológica y programas de seguridad industrial, conforme a la normativa vigente. El tratamiento de datos de salud se realiza únicamente en el marco de las obligaciones legales aplicables y con las medidas de seguridad reforzadas exigidas por el Art. 26 de la LOPDP.

5. **Comunicación interna, capacitación y desarrollo profesional:** Para gestionar procesos de comunicación interna, programas de capacitación, desarrollo de competencias, evaluaciones de desempeño y promoción profesional dentro de

ESPOLTEL, así como para la elaboración de organigramas, directorios corporativos y materiales institucionales que faciliten la interacción entre los trabajadores.

6. **Control de acceso, seguridad física e informática:** Para administrar el control de ingreso y salida del personal a las instalaciones físicas y a los sistemas informáticos de ESPOLTEL, incluyendo el uso de sistemas de videovigilancia (CCTV) y registro biométrico (huella dactilar). El tratamiento de datos biométricos se realiza con base en el interés legítimo y la obligación legal aplicable, y constituye tratamiento de datos de categoría especial conforme al Art. 26 de la LOPDP, por lo que el trabajador otorga consentimiento expreso y específico para dicho tratamiento en el recuadro habilitado al final de este documento.

7. **Administración de beneficios laborales y extralaborales:** Para la administración de beneficios laborales y extralaborales tales como seguros médicos, seguros de vida, programas de asistencia al empleado, actividades de bienestar o incentivos, pudiendo requerir la transferencia de datos a aseguradoras, instituciones financieras u otros proveedores de servicios vinculados.

8. **Auditoría interna o externa y controles financieros:** Para procesos de auditoría interna o externa, controles financieros, verificaciones contables y cumplimiento de normas de transparencia corporativa, en la medida en que se requiera utilizar información del trabajador para fines de verificación y control.

9. **Administración de sistemas informáticos y activos digitales:** Para la administración de cuentas de correo electrónico corporativo, sistemas informáticos (incluyendo ODOO y SharePoint), software de gestión, equipos de trabajo y monitoreo del uso adecuado de activos digitales, únicamente en el marco permitido por la legislación laboral y de protección de datos.

CONSENTIMIENTO EXPRESO PARA DATOS DE CATEGORÍA ESPECIAL (Art. 26 LOPDP)
Conforme al Art. 26 de la LOPDP, el tratamiento de datos biométricos (huella dactilar) y datos de salud (certificados médicos, información de salud ocupacional) requiere consentimiento expreso y específico. El trabajador declara a continuación su aceptación diferenciada:

☐ Autorizo expresamente el tratamiento de mis datos biométricos (huella dactilar) para control de asistencia conforme a la finalidad No. 6.
☐ Autorizo expresamente el tratamiento de mis datos de salud (certificados médicos, información de salud ocupacional) para las finalidades No. 1 y No. 4.

ESPOLTEL S.A. se compromete a:

- Tratar los datos personales del TRABAJADOR de forma lícita, leal, proporcional y transparente, garantizando la confidencialidad y la seguridad técnica, física y organizativa necesaria para su protección.
- No utilizar ni comunicar los datos personales para finalidades distintas a las aquí autorizadas, salvo mandato legal o requerimiento de autoridad competente.

- Conservar los datos personales únicamente por el tiempo necesario para cumplir con las finalidades indicadas, y posteriormente proceder a su bloqueo, anonimización o eliminación, conforme a lo dispuesto en el RGLOPDP y resoluciones de la Superintendencia de Protección de Datos Personales (SPDP).
- Facilitar al TRABAJADOR el ejercicio de sus derechos de acceso, rectificación, actualización, eliminación, oposición, portabilidad y suspensión del tratamiento, los cuales podrán ejercerse por escrito dirigiéndose al correo electrónico dpd@espoltel.com o presencialmente en las oficinas de ESPOLTEL S.A. (Vía Perimetral Km 30.5, campus ESPOL, Guayaquil). El plazo de respuesta es de 15 días hábiles.

El TRABAJADOR manifiesta haber leído y comprendido el contenido de la presente autorización, y acepta expresamente el tratamiento de sus datos personales conforme a los fines y condiciones aquí establecidos.

Nombre completo:	
Número de cédula:	
Cargo:	
Fecha:	
Firma del trabajador:	

ANEXO 6: Formulario general ejercicio de derechos ARCO

ESPOLTEL S.A. - Conforme a la Ley Orgánica de Protección de Datos Personales (LOPDP)

1. DATOS DEL TITULAR

Nombres completos:	
Apellidos completos:	
Cédula de ciudadanía / Pasaporte:	
Correo electrónico:	
Teléfono de contacto:	
Dirección:	
Ciudad:	

2. DERECHO QUE DESEA EJERCER (Marque con una X)

[ ]	ACCESO — Deseo conocer qué datos personales trata la Institución sobre mí.
[ ]	RECTIFICACIÓN — Deseo corregir datos inexactos o incompletos.
[ ]	ELIMINACIÓN — Deseo solicitar la eliminación de mis datos personales.
[ ]	OPOSICIÓN — Deseo oponerme a ciertos tratamientos de mis datos personales.
[ ]	PORTABILIDAD — Deseo recibir mis datos en formato estructurado.
[ ]	LIMITACIÓN — Deseo restringir el tratamiento de mis datos.

3. DESCRIPCIÓN DE SU SOLICITUD

4. DOCUMENTOS ADJUNTOS

- [ ] Copia de cédula de ciudadanía o pasaporte (obligatorio)
- [ ] Poder notarial (si actúa en representación de otra persona)
- [ ] Otros documentos de respaldo: _____

5. DECLARACIÓN Y FIRMA

Declaro que la información proporcionada es verdadera y completa. Autorizo a la compañía ESPOLTEL S.A. a verificar la autenticidad de los datos proporcionados.

Lugar y fecha:	**Firma del titular:**

Entregar este formulario en:
ESPOLTEL S.A. - Vía Perimetral Km 30.5, campus ESPOL, Guayaquil, Guayas
Correo electrónico: dpd@espoltel.com
Plazo de respuesta: 15 días hábiles

ANEXO 7: Modelo de contrato de encargo de tratamiento

CONTRATO DE ENCARGO DEL TRATAMIENTO DE DATOS PERSONALES

Al amparo de la Ley Orgánica de Protección de Datos Personales del Ecuador (LOPDP), su Reglamento General y demás normativa aplicable

---

Lugar: Guayaquil, Ecuador **Fecha:** _____

COMPARECIENTES

Por una parte, ESPOLTEL S.A., sociedad anónima debidamente constituida, con RUC **0991415106001**, con domicilio en la ciudad de Guayaquil, República del Ecuador, representada legalmente por el señor **JORGE LUIS CÁRDENAS MUGA**, portador de la cédula de ciudadanía No. **0908930662**, en su calidad de Representante Legal, a quien en adelante se denominará el **"RESPONSABLE DEL TRATAMIENTO"** o simplemente **"EL RESPONSABLE"**.

Por otra parte, _____ (nombre o razón social), con número de identificación tributaria / registro _____, con domicilio en la República de _____, representada legalmente por _____, portador del documento de identidad No. _____, a quien en adelante se denominará el **"ENCARGADO DEL TRATAMIENTO"** o simplemente **"EL ENCARGADO"**.

Las partes, de mutuo acuerdo y libres de toda presión, coacción o vicio del consentimiento, suscriben el presente Contrato de Encargo del Tratamiento de Datos Personales, que se regirá por las siguientes cláusulas:

ANTECEDENTES

PRIMERO.- ESPOLTEL S.A. es una empresa de economía mixta, que desarrolla actividades en telecomunicaciones, producción televisiva, construcción y obras de ingeniería civil, y que suscribe contratos con entidades privadas y públicas, a través del Sistema Nacional de Contratación Pública (SERCOP).

SEGUNDO.- En el marco de sus actividades, ESPOLTEL S.A. requiere los servicios de auditoría médica prestados por EL ENCARGADO, consistentes en la revisión, análisis y validación de expedientes médicos digitales de beneficiarios del Instituto Ecuatoriano de Seguridad Social (IESS), en cumplimiento de la normativa institucional del IESS, incluyendo los requisitos establecidos en la Resolución No. CD 117 y demás disposiciones aplicables.

TERCERO.- Para la prestación de dichos servicios, EL ENCARGADO accederá y tratará datos personales de categoría especial —concretamente, datos de salud— por cuenta y bajo instrucción de EL RESPONSABLE. Dicho tratamiento implica una transferencia

internacional de datos personales desde la República del Ecuador hacia la República de _____.

CUARTO.- Ambas partes reconocen que el tratamiento de datos personales descrito está sujeto a la Ley Orgánica de Protección de Datos Personales del Ecuador (LOPDP), su Reglamento General, y demás normativa emitida por la Superintendencia de Protección de Datos Personales (SPDP), siendo el presente contrato el instrumento jurídico habilitante para dicha transferencia internacional, conforme al artículo 54 y siguientes de la LOPDP.

CLÁUSULAS

PRIMERA.- OBJETO DEL ENCARGO

EL ENCARGADO tratará los datos personales que le sean comunicados por EL RESPONSABLE, o a los que tenga acceso con motivo de la prestación del servicio de auditoría médica al IESS, única y exclusivamente conforme a las instrucciones documentadas de EL RESPONSABLE y en los términos previstos en el presente contrato.

SEGUNDA.- DATOS OBJETO DEL TRATAMIENTO

Categorías de titulares: Beneficiarios, afiliados y/o derechohabientes del Instituto Ecuatoriano de Seguridad Social (IESS) cuyos expedientes médicos sean objeto de auditoría.

Tipos de datos: Datos de identificación (nombres, cédula/número de afiliación), datos de contacto, y datos relativos a la salud (diagnósticos, tratamientos, prestaciones médicas, historia clínica, resultados de exámenes y demás contenido de los expedientes médicos digitales).

Categorías especiales: SÍ — Datos de salud (Art. 26 LOPDP). El tratamiento de estas categorías especiales requiere la adopción de medidas reforzadas de seguridad y confidencialidad por parte de EL ENCARGADO.

Operaciones de tratamiento: Acceso, lectura, consulta, análisis, validación y generación de informes de auditoría. Queda expresamente prohibido cualquier tratamiento ulterior no autorizado por EL RESPONSABLE.

TERCERA.- FINALIDAD DEL TRATAMIENTO

EL ENCARGADO tratará los datos exclusivamente para las siguientes finalidades:

a) Revisar y auditar expedientes médicos digitales de beneficiarios del IESS conforme a los parámetros establecidos por dicha institución (Resolución CD 117 y demás normativa aplicable).

b) Validar el cumplimiento de los requisitos técnicos y de calidad exigidos para la prestación de servicios médicos.

c) Elaborar informes de auditoría para ser entregados exclusivamente a EL RESPONSABLE.

Queda prohibido el tratamiento de los datos para fines distintos a los aquí establecidos, incluyendo cualquier uso comercial, cesión a terceros, o enriquecimiento de bases de datos propias.

CUARTA.- DURACIÓN DEL ENCARGO

El presente encargo tendrá vigencia desde la fecha de suscripción del presente contrato hasta la terminación del contrato principal o convenio de auditorías médicas suscrito entre ESPOLTEL S.A. y el IESS, o hasta que EL RESPONSABLE notifique por escrito la conclusión del encargo, lo que ocurra primero.

A la terminación del encargo, serán de aplicación las obligaciones previstas en la Cláusula Décima Tercera del presente contrato.

QUINTA.- OBLIGACIONES DEL ENCARGADO

EL ENCARGADO se obliga a:

a) Tratar los datos personales única y exclusivamente conforme a las instrucciones documentadas de EL RESPONSABLE, sin que pueda utilizar los datos para fines propios ni para finalidades distintas a las acordadas.

b) Garantizar que las personas autorizadas para acceder a los datos personales —incluyendo auditores, analistas y personal de soporte— hayan suscrito un compromiso de confidencialidad de carácter indefinido, o estén sujetas a una obligación legal equivalente de secreto.

c) Implementar y mantener las medidas técnicas y organizativas de seguridad establecidas en la Cláusula Séptima del presente contrato, adecuadas al riesgo y a la naturaleza de los datos de salud tratados.

d) No subcontratar el tratamiento de datos personales, ni total ni parcialmente, sin autorización previa, expresa y por escrito de EL RESPONSABLE.

e) Asistir a EL RESPONSABLE, mediante medidas técnicas y organizativas apropiadas, en la atención de solicitudes de ejercicio de derechos por parte de los titulares (acceso, rectificación, eliminación, oposición, portabilidad y suspensión del tratamiento).

f) Asistir a EL RESPONSABLE en el cumplimiento de sus obligaciones relativas a seguridad del tratamiento, evaluaciones de impacto relativas a la protección de datos (EIPD) y notificación de vulneraciones de seguridad a la SPDP.

g) Devolver o eliminar de forma segura todos los datos personales al término del encargo, conforme a lo establecido en la Cláusula Décima Tercera.

h) Poner a disposición de EL RESPONSABLE toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en este contrato, incluyendo registros de actividades de tratamiento.

i) Permitir y facilitar la realización de auditorías e inspecciones por parte de EL RESPONSABLE, conforme a la Cláusula Décima Segunda.

j) Notificar a EL RESPONSABLE, sin dilación indebida y en un plazo máximo de DOS (2) días hábiles, cualquier vulneración de seguridad de los datos personales de la que tuviere conocimiento.

k) Cumplir la normativa de protección de datos de _____ aplicable al tratamiento realizado en su territorio, en la medida en que sea compatible y no menos protectora que la LOPDP del Ecuador.

SEXTA.- INSTRUCCIONES DOCUMENTADAS

Las instrucciones iniciales de EL RESPONSABLE al ENCARGADO son las siguientes:

a) Los datos de salud objeto del encargo serán accedidos únicamente por el personal del ENCARGADO expresamente autorizado para cada proceso de auditoría.

b) Los datos no podrán ser descargados, copiados, ni almacenados en dispositivos o sistemas distintos a los aprobados por EL RESPONSABLE.

c) Los resultados de la auditoría se entregarán exclusivamente a EL RESPONSABLE en el formato y medio que este indique.

d) Los datos no podrán ser objeto de tratamiento fuera del ámbito geográfico de _____ sin autorización escrita previa de EL RESPONSABLE.

Cualquier instrucción adicional deberá ser comunicada por escrito. Si EL ENCARGADO considerare que una instrucción infringe la normativa de protección de datos aplicable, lo informará de forma inmediata y documentada a EL RESPONSABLE.

SÉPTIMA.- MEDIDAS DE SEGURIDAD

Dado que se tratan datos de salud (categoría especial), EL ENCARGADO implementará, como mínimo, las siguientes medidas:

Técnicas: Control de accesos por perfil de usuario; cifrado de datos en tránsito y en reposo; copias de seguridad periódicas; registros de auditoría (logs) de acceso a los datos; autenticación de doble factor para el personal con acceso a expedientes.

Organizativas: Políticas internas de protección de datos y seguridad de la información; programa de capacitación y concientización del personal; protocolo de gestión de incidentes de seguridad; designación de un responsable interno de privacidad.

Jurídicas: Contratos y/o compromisos de confidencialidad suscritos por todo el personal con acceso a los datos; cláusulas de protección de datos en eventuales contratos con subencargados autorizados.

OCTAVA.- SUBENCARGO

EL ENCARGADO NO podrá subcontratar el tratamiento de datos personales objeto del presente contrato sin contar con autorización previa, expresa y por escrito de EL RESPONSABLE.

En caso de que EL RESPONSABLE autorice la subcontratación, EL ENCARGADO deberá:

i. seleccionar subencargados que ofrezcan garantías suficientes de cumplimiento de la normativa de protección de datos;
ii. imponer al subencargado las mismas obligaciones de protección de datos establecidas en el presente contrato; y
iii. responder directamente ante EL RESPONSABLE por el cumplimiento de dichas obligaciones, con independencia de la responsabilidad del subencargado.

Subencargados autorizados actualmente: Ninguno.

NOVENA.- TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

Autorización: EL RESPONSABLE autoriza expresamente la transferencia internacional de datos personales desde la República del Ecuador hacia la República de _____, al amparo del artículo 54 y siguientes de la LOPDP y el presente contrato, que constituye el instrumento jurídico habilitante.

País de destino: República de _____.

Garantías: Las garantías adecuadas para la transferencia internacional están dadas por las obligaciones contractuales asumidas por EL ENCARGADO en virtud del presente

contrato, que imponen un nivel de protección equivalente al exigido por la LOPDP del Ecuador.

Mecanismo habilitante: Contrato de encargo del tratamiento con cláusulas de protección equivalente (Art. 54 literal c) LOPDP).

Queda expresamente prohibida cualquier transferencia ulterior de los datos a un tercer país distinto de _____ sin autorización escrita previa de EL RESPONSABLE.

DÉCIMA.- COLABORACIÓN EN EL EJERCICIO DE DERECHOS

Cuando EL ENCARGADO recibiere una solicitud de ejercicio de derechos por parte de un titular (acceso, rectificación, eliminación, oposición, portabilidad o suspensión del tratamiento), deberá:

a) Notificar a EL RESPONSABLE en un plazo máximo de TRES (3) días hábiles desde la recepción de la solicitud.

b) No dar respuesta directa al titular sin instrucción expresa de EL RESPONSABLE.

c) Proporcionar a EL RESPONSABLE toda la información y asistencia necesaria para dar respuesta en los plazos legales.

d) Ejecutar las instrucciones de EL RESPONSABLE respecto al tratamiento de la solicitud.

DÉCIMA PRIMERA.- NOTIFICACIÓN DE VULNERACIONES DE SEGURIDAD

Ante cualquier vulneración de seguridad de los datos personales (incluyendo accesos no autorizados, pérdida, destrucción, alteración o divulgación indebida), EL ENCARGADO deberá:

1. Notificar a EL RESPONSABLE en un plazo máximo de DOS (2) días hábiles desde que tuviere conocimiento del incidente.

2. Proporcionar, como mínimo, la siguiente información: naturaleza de la vulneración; categorías y número aproximado de titulares afectados; tipos y volumen estimado de datos comprometidos; causa presunta del incidente; medidas adoptadas y previstas para mitigar sus efectos; evaluación preliminar del riesgo para los titulares.

3. Documentar el incidente en un registro interno de vulneraciones.

4. Colaborar activamente con EL RESPONSABLE en la gestión del incidente, incluyendo la notificación a la Superintendencia de Protección de Datos Personales (SPDP) si fuere procedente.

DÉCIMA SEGUNDA.- AUDITORÍAS E INSPECCIONES

EL RESPONSABLE, directamente o a través de un tercero designado, podrá en cualquier momento:

a) Solicitar información detallada sobre las actividades de tratamiento realizadas por EL ENCARGADO.

b) Realizar auditorías de cumplimiento, con un preaviso razonable de al menos CINCO (5) días hábiles, salvo en casos de urgencia motivada por una vulneración de seguridad o requerimiento de la SPDP.

c) Realizar inspecciones en las instalaciones de EL ENCARGADO donde se realice el tratamiento.

EL ENCARGADO se obliga a facilitar el acceso a sus instalaciones, sistemas y documentación, y a proporcionar toda la información requerida dentro de los plazos solicitados.

Periodicidad mínima de auditorías: una (1) vez al año, o a solicitud de EL RESPONSABLE cuando existan indicios de incumplimiento.

DÉCIMA TERCERA.- DEVOLUCIÓN O ELIMINACIÓN DE DATOS

Al término del encargo, por cualquier causa, EL ENCARGADO deberá, en un plazo máximo de QUINCE (15) días calendario:

a) Devolver a EL RESPONSABLE todos los datos personales en su poder, en el formato y medio que este indique; O

b) Eliminar de forma segura e irrecuperable todos los datos personales, así como todas las copias existentes, utilizando métodos que imposibiliten su recuperación.

La opción aplicable será la que EL RESPONSABLE indique por escrito.

EL ENCARGADO emitirá un certificado de devolución o eliminación segura dentro del mismo plazo.

Excepción: Los datos que deban conservarse por obligación legal expresa quedarán bloqueados y solo podrán ser tratados para el cumplimiento de dicha obligación, debiendo EL ENCARGADO informar a EL RESPONSABLE de esta circunstancia.

DÉCIMA CUARTA.- RESPONSABILIDAD Y GARANTÍAS

EL ENCARGADO será responsable de los daños y perjuicios causados a EL RESPONSABLE y/o a los titulares de los datos como consecuencia de:

i. tratamientos realizados en contravención de las instrucciones documentadas;
ii. infracciones a la normativa de protección de datos aplicable; o
iii. vulneraciones de seguridad atribuibles a su negligencia o incumplimiento.

EL ENCARGADO se obliga a mantener vigente, durante toda la duración del encargo, una póliza de seguro de responsabilidad civil profesional por un monto mínimo de USD _____, y a acreditar su vigencia a solicitud de EL RESPONSABLE.

DÉCIMA QUINTA.- CONFIDENCIALIDAD

Las partes se comprometen a mantener la más estricta confidencialidad sobre los datos personales objeto del tratamiento y sobre la información obtenida en el contexto del presente contrato. La obligación de confidencialidad subsistirá indefinidamente, incluso después de la terminación de la relación contractual por cualquier causa.

DÉCIMA SEXTA.- LEGISLACIÓN APLICABLE Y JURISDICCIÓN

El presente contrato se rige por la Ley Orgánica de Protección de Datos Personales (LOPDP) del Ecuador, su Reglamento General, las disposiciones de la Superintendencia de Protección de Datos Personales (SPDP), y demás normativa ecuatoriana aplicable.

Sin perjuicio de ello, EL ENCARGADO se obliga asimismo a cumplir la normativa de protección de datos personales vigente en la República de _____ en lo relativo al tratamiento realizado en su territorio.

Cualquier controversia derivada de la interpretación, ejecución o terminación del presente contrato será sometida a los jueces competentes de la ciudad de Guayaquil, República del Ecuador.

En prueba de conformidad, las partes suscriben el presente contrato en la ciudad de Guayaquil, a los _____ días del mes de _____ del año _____.

_____	_____
ESPOLTEL S.A.	_____
Jorge Luis Cárdenas Muga	*(Nombre del Encargado)*
Representante Legal	_____
C.C. 0908930662	*(Cargo / Representante Legal)*
RUC: 0991415106001	*(Identificación / NIT)*
RESPONSABLE DEL TRATAMIENTO	ENCARGADO DEL TRATAMIENTO

ANEXO 8: REGISTRO SIMPLIFICADO DE BRECHAS DE SEGURIDAD

Campo	Detalle	Información a completar
INCIDENTE NO.	Número correlativo	_____
Fecha de detección	Fecha en que se identificó el incidente	____ / ____ / _____
Hora	Hora de detección	____ : ____
Reportado por	Nombre de quien reporta	_____
Cargo	Cargo de quien reporta	_____
¿Cómo se detectó?	Descripción del modo de detección	_____
Descripción del incidente	¿Qué ocurrió exactamente?	_____
Tipo de brecha	Pérdida/robo | Envío erróneo | Acceso no autorizado | Eliminación accidental | Otro	[ ] Marcar el tipo
Archivos / documentos afectados	Detalle de los archivos o sistemas comprometidos	_____
Datos comprometidos	Tipo de datos afectados (identificativos, salud, laborales, etc.)	[ ] Marcar los tipos
NO. de personas afectadas	Número estimado de titulares afectados	_____
Nivel de riesgo	ALTO | MEDIO | BAJO	[ ] Marcar nivel
Justificación del nivel	Razón por la que se asigna ese nivel de riesgo	_____
Medidas inmediatas adoptadas	Acciones tomadas para contener la brecha	_____

Notificación a SPDP	¿Se notificó? Fecha	[ ] SÍ [ ] NO — Fecha: ___
Notificación a personas afectadas	¿Se notificó? Fecha	[ ] SÍ [ ] NO — Fecha: ___
Causa raíz	Origen del incidente	_____
Lecciones aprendidas	Aprendizajes del incidente	_____
Mejoras implementadas	Acciones correctivas y preventivas	_____
Estado del caso	Abierto | En proceso | Cerrado	[ ] Marcar estado
Fecha de cierre	Fecha de cierre formal del caso	____ / ____ / _____
Firma del Responsable	Firma del Coordinador de Seguridad	_____

ANEXO 9: MODELO DE NOTIFICACIÓN A AUTORIDADES

Guayaquil, (Fecha)

Señores:
Superintendencia de Protección de Datos Personales (SPDP)
Agencia de Regulación y Control de Telecomunicaciones (ARCOTEL)

Asunto: Notificación de Brecha de Seguridad de Datos Personales

De conformidad con el Art. 24 del Reglamento de la LOPDP, la compañía ESPOLTEL S.A. notifica la siguiente vulneración de seguridad:

1. DATOS DEL RESPONSABLE

- Nombre del responsable: ESPOLTEL S.A.
- RUC: 0991415106001
- Domicilio: Km. 30,5 Vía Perimetral, Campus ESPOL, Guayaquil, Ecuador.
- Correo electrónico: dpd@espoltel.com
- Coordinador de Seguridad: _____ Tel: _____

2. EL INCIDENTE

- ¿Qué pasó?: _____
- Fecha de ocurrencia: _____
- Fecha de detección: _____
- Tipo de brecha: [ ] Confidencialidad [ ] Integridad [ ] Disponibilidad

3. DATOS Y PERSONAS AFECTADAS

- Número de personas afectadas: _____
- Datos comprometidos: [ ] Identificativos [ ] Laborales [ ] Menores de edad [ ] Salud
- Sistemas afectados: _____

4. CAUSA

(Explicar brevemente qué causó el incidente: error humano, falla técnica, robo, etc.)

5. MEDIDAS TOMADAS Y EVALUACIÓN DE RIESGO

- Acciones inmediatas: _____
- Mejoras implementadas: _____

- Nivel de riesgo: [ ] ALTO [ ] MEDIO [ ] BAJO
- Notificación a afectados: [ ] SÍ — Fecha: _____ [ ] NO — Justificación: _____

Quedamos a disposición para cualquier información adicional.

Atentamente,

_____

Gerente General

ESPOLTEL S.A.

ANEXO 10: MODELO DE NOTIFICACIÓN A PERSONA AFECTADA

Guayaquil, (Fecha)

Estimado/a (Nombre):

Le informamos que detectamos un incidente de seguridad que afectó algunos de sus datos personales.

QUÉ OCURRIÓ

(Explicación simple y directa del incidente, cuándo pasó y cómo fue detectado)

QUÉ DATOS SUYOS SE AFECTARON

- (Dato 1: ej. nombre y cédula)
- (Dato 2: ej. información de salud de fecha ___)

QUÉ RIESGOS EXISTEN PARA USTED

(Explicar honestamente qué podría suceder como consecuencia del incidente)

QUÉ HEMOS HECHO

- (Medida 1 adoptada por la institución)
- (Medida 2 adoptada por la institución)

QUÉ PUEDE HACER USTED

- (Recomendación 1 para el titular afectado)
- (Recomendación 2 para el titular afectado)

CONTACTO Y SUS DERECHOS

Para cualquier pregunta: _____ | Teléfono: _____ | Email: dpd@espoltel.com

Usted puede solicitar más información sobre sus datos o presentar un reclamo ante la SPDP si considera que sus derechos fueron vulnerados.

Lamentamos este incidente y le aseguramos nuestro compromiso de proteger su información.

Atentamente,

Firmado electrónicamente por:
JORGE LUIS CARDENAS MUGA
Validar únicamente con FirmaEC

Gerente General

ESPOLTEL S.A.