RESOLUCIÓN ADMINISTRATIVA N° ° RES-02-GR-GASPOCH-EP-PDP-2026

ESTACIÓN DE SERVICIOS ESPOCH GASOLINERA POLITÉCNICA E.P.

Ing. Mateo Coronel Cácerez
GERENTE GENERAL

CONSIDERANDO:

Que, el artículo 66 numeral 19 de la Constitución de la República del Ecuador reconoce y garantiza el derecho a la protección de datos de carácter personal;

Que, la Ley Orgánica de Protección de Datos Personales (LOPDP), publicada en el Registro Oficial Suplemento 459 de 26 de mayo de 2021, es de cumplimiento obligatorio para las instituciones del sector público, incluidas las empresas públicas creadas al amparo de la Ley Orgánica de Empresas Públicas (LOEP);

Que, el Reglamento General a la LOPDP fue expedido mediante Decreto Ejecutivo 904 y publicado en el Registro Oficial Suplemento 435 de 13 de noviembre de 2023;

Que, la Superintendencia de Protección de Datos Personales (SPDP) ha expedido normativa técnica de obligatorio cumplimiento que desarrolla la LOPDP, entre ella las Resoluciones SPDP-SPD-2025-0028-R (Delegado), SPDP-SPD-2026-0004-R (transferencias), SPDP-SPD-2026-0005-R (gran escala), SPDP-SPD-2025-0041-R (interés legítimo), SPDP-SPD-2026-0022-R y SPDP-SPD-2026-0038-R (denuncias), SPDP-SPD-2025-0030-R (seudonimización, anonimización, bloqueo y eliminación), SPDP-SPD-2025-0006-R (cláusulas contractuales), SPDP-SPD-2026-0039-R (datos biométricos) y SPDP-SPD-2026-0009-R y 0037-R (inteligencia artificial);

Que, el COESCCI, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y el Código Orgánico Monetario y Financiero contienen disposiciones sobre clasificación de datos, privacidad de software, portal de datos personales, documentos electrónicos, información crediticia y medios de pago que resultan aplicables a la institución;

Que, el artículo 48 numeral 1 de la LOPDP dispone la designación obligatoria de un Delegado de Protección de Datos Personales para las entidades del sector público, supuesto en el que se encuentra la institución en su calidad de empresa pública, que mediante Resolución Administrativa No. RES-056-GR-GASPOCH-EP-2026, de 4 de septiembre de 2026, se dejaron sin efecto las designaciones anteriores de Delegado de Protección de Datos Personales (Resoluciones Administrativas Nros. RES-023-GASPOCH-GG-2025 y RES-033-GR-GASPOCH-EP-2025), y que mediante Nombramiento de 9 de septiembre de 2026 la Gerencia General designó a la Ab. Andrea Estefanía Pinto Morales, MSc., designación registrada ante la SPDP;

Que, la misma Resolución Administrativa No. RES-056-GR-GASPOCH-EP-2026 derogó expresamente la Resolución Administrativa No. RES-034-GR-GASPOCH-EP-2025, de 29 de diciembre de 2025, que expidió el Protocolo de Tratamiento de Datos Personales de la institución, por lo que resulta necesario contar con un instrumento integral que lo sustituya;

Que, la institución opera un sistema de videovigilancia y un sistema biométrico de control de asistencia, cuya gestión técnica consta en sendos manuales operativos que deben desarrollar esta Normativa;

Que, el artículo 11 numeral 8 de la Ley Orgánica de Empresas Públicas faculta al Gerente General a aprobar y modificar los reglamentos internos que requiera la empresa pública;

En ejercicio de las atribuciones legales y reglamentarias,

RESUELVE:

EXPEDIR LA NORMATIVA INTEGRAL DE PROTECCIÓN DE DATOS PERSONALES DE LA ESTACIÓN DE SERVICIOS ESPOCH GASOLINERA POLITÉCNICA E.P.

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1.- Objeto. La presente Normativa establece los lineamientos, principios, roles, responsabilidades y procedimientos que regulan el tratamiento de datos personales efectuado por la Estación de Servicios ESPOCH Gasolinera Politécnica E.P. (en adelante, "la institución"), en cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP), su Reglamento General y la normativa técnica emitida por la Superintendencia de Protección de Datos Personales (SPDP).

Artículo 2.- Ámbito de aplicación. Esta Normativa es de cumplimiento obligatorio para las autoridades institucionales, el Directorio, la Gerencia General, las Subgerencias, todo el personal bajo cualquier modalidad contractual, y los terceros que tengan acceso a datos personales bajo responsabilidad de la institución.

Artículo 3.- Base legal. Esta Normativa se fundamenta en la Constitución de la República; la LOPDP; su Reglamento General (Decreto Ejecutivo 904, Registro Oficial Suplemento 435 de 13 de noviembre de 2023); la Ley Orgánica de Empresas Públicas; el Código Orgánico Administrativo; la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP) y su Reglamento; el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación (COESCCI), en particular sus artículos 141, 146 y 150 y su Disposición General Vigésima Sexta; la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ley 67) y su Reglamento (Decreto Ejecutivo 3496); el Código Orgánico Monetario y Financiero en lo relativo a información crediticia, sigilo y reserva y medios de pago; y la normativa técnica de la SPDP. En lo que alguna de estas normas se contraponga a la LOPDP, prevalece esta última (LOPDP, Disposición Derogatoria Cuarta). Cualquier referencia contenida en instrumentos internos a un cuerpo normativo distinto para el Reglamento General de la LOPDP se entenderá corregida y sustituida por la cita señalada en este artículo.

Artículo 4.- Definiciones. Se adoptan las definiciones establecidas en el artículo 4 de la LOPDP, en el artículo 4 de su Reglamento General y en la normativa técnica de la SPDP. Adicionalmente, para efectos de esta Normativa:

- Coactivado: persona natural o jurídica deudora de la institución, sujeta a un procedimiento de ejecución coactiva.
- Garante solidario: tercero que respalda con su firma el cumplimiento de una obligación de un servidor, trabajador o usuario frente a la institución.
- Comité de Transparencia: órgano colegiado responsable del cumplimiento de las obligaciones derivadas de la LOTAIP.
- Tratamiento a gran escala: aquel que alcance un puntaje igual o superior a seis (6) puntos según el Modelo Técnico de Gran Escala (MTGE) de la Resolución SPDP-SPD-2026-0005-R, o que se encuentre calificado como tal de manera directa y obligatoria conforme al artículo 14 de dicha resolución.
- Seudonimización, anonimización y bloqueo: medidas técnicas de seguridad definidas en la Resolución SPDP-SPD-2025-0030-R, desarrolladas en el Título VII de esta Normativa.
- Manuales operativos: el Manual y Política para la Gestión del Sistema de Videovigilancia y el Manual y Política para la Gestión del Sistema Biométrico.

Artículo 5.- Principios rectores. El tratamiento de datos personales se regirá por los principios de juridicidad, lealtad, transparencia, finalidad, minimización, proporcionalidad, confidencialidad, calidad y exactitud, conservación limitada, seguridad, responsabilidad proactiva y aplicación favorable al titular, previstos en el artículo 10 de la LOPDP.

Artículo 6.- Manuales operativos y jerarquía normativa. Los manuales operativos se expedirán en desarrollo de esta Normativa, mediante resolución de la Gerencia General posterior a su aprobación, y desarrollan los aspectos técnicos y de procedimiento de los sistemas que regulan. En caso de contradicción, prevalece esta Normativa. Los anexos de los manuales que contienen información de seguridad (inventarios, matrices de acceso, verificaciones técnicas, análisis de riesgos y evaluaciones de impacto) son de acceso restringido y no se publican; su carácter reservado se declara formalmente por la autoridad competente, con anterioridad a cualquier solicitud, conforme a la LOTAIP. Los manuales se revisarán al menos una vez al año.

TÍTULO II
ROLES Y RESPONSABILIDADES

Artículo 7.- Responsable del tratamiento. La institución, representada por su Gerencia General, actúa como Responsable del Tratamiento de Datos Personales, en cuanto determina las finalidades y los medios del tratamiento efectuado en el ejercicio de sus competencias, conforme al artículo 4 de la LOPDP.

Artículo 8.- Delegado de Protección de Datos Personales. El Delegado de Protección de Datos Personales ejercerá sus funciones con independencia funcional, sin recibir instrucciones respecto del ejercicio de sus atribuciones. Sus funciones son las previstas en la LOPDP y en las resoluciones correspondientes de la Superintendencia de Protección de Datos Personales, dentro de los cuales estan: asesorar al responsable y al personal; supervisar el cumplimiento de la normativa de protección de datos; asesorar en el análisis de riesgo y la evaluación de impacto; asesorar en

la gestión de vulneraciones de seguridad y su notificación; supervisar el Registro de Actividades de Tratamiento; cooperar con la SPDP como punto de contacto institucional; y las demás que establezca la Autoridad. La institución podrá designar un delegado suplente que actúe en su ausencia temporal o definitiva (Reglamento General, art. 52). La institución mantiene un solo acto vigente de designación del Delegado; todo cambio de designación deja sin efecto el anterior y se registra ante la SPDP dentro del término previsto en la ley.

Artículo 9.- Límites de las funciones del Delegado. Conforme al artículo 15 de la Resolución SPDP-SPD-2025-0028-R, la Delegada no podrá: implementar de forma directa la LOPDP y su normativa, obligación que corresponde a la institución; ejecutar de forma directa la gestión de riesgos o las evaluaciones de impacto, respecto de las cuales únicamente podrá emitir observaciones u orientaciones no vinculantes; tomar decisiones sobre la finalidad o los medios del tratamiento; ni representar a la institución ante la SPDP en calidad de responsable del tratamiento.

Artículo 10.- Impedimentos y conflictos de interés del Delegado. No podrá ejercer o mantenerse en el cargo de Delegado quien, simultáneamente, ejerciere las funciones de oficial de seguridad de la información o de oficial de cumplimiento de la institución, ni quien ejerciere un cargo de nivel jerárquico superior en el sector público, conforme a los artículos 16 y 18 de la Resolución SPDP-SPD-2025-0028-R. La Gerencia General verificará estas condiciones antes de cada designación y de forma anual.

Artículo 11.- Garantías de independencia y protección del Delegado. La institución garantizará el contacto directo del Delegado con el más alto nivel ejecutivo, la disponibilidad de recursos técnicos, financieros y humanos, y la ausencia de represalias por el correcto ejercicio de sus funciones. Esta independencia será evaluada institucionalmente, con periodicidad anual y bajo criterios no jerárquicos. En caso de remoción, cese, separación, despido o sanción presuntamente injustificados, el Delegado podrá presentar su denuncia directamente ante la SPDP.

Artículo 12.- Autoridades institucionales. El Directorio y la Gerencia General son responsables de promover una cultura institucional de protección de datos personales, respaldar la implementación de esta Normativa y disponer las acciones correctivas frente a los incumplimientos detectados.

Artículo 13.- Coordinación entre el Delegado de Protección de Datos y el Comité de Transparencia. Previo a la publicación de cualquier resolución, informe o documento institucional que individualice o permita identificar a una persona natural; incluyendo informes de organismos de control con hallazgos de responsabilidad administrativa, civil o indicios de responsabilidad penal, el Comité de Transparencia deberá remitir el documento al Delegado de Protección de Datos Personales, quien evaluará y recomendará, cuando corresponda, la reserva, disociación o anonimización de los datos personales que no sean estrictamente necesarios para la finalidad de la publicación.

Artículo 14.- Unidades con tratamiento relevante de datos personales. Sin perjuicio de las demás unidades institucionales, se identifican como unidades con mayor incidencia en el tratamiento de datos personales: la Unidad de Talento Humano (evaluaciones de desempeño, anticipos de remuneración, expedientes laborales, control de asistencia); la Subgerencia Administrativa Financiera y la Unidad de Contabilidad (facturación, sistema FÉNIX, cobro coactivo); la Unidad de Tecnologías de la Información y Comunicación (sistemas informáticos, videovigilancia, sistema biométrico, tarjetas RFID, portal institucional); la unidad de Archivo y Gestión Documental; la Subgerencia de Asesoría Jurídica; y quien ejerza las funciones de Juez de Coactiva.

Artículo 15.- Servidores, trabajadores y colaboradores. Todo el personal que, en el ejercicio de sus funciones, tenga acceso a datos personales, deberá: tratarlos únicamente para las finalidades autorizadas; guardar reserva y confidencialidad durante y después de finalizada la relación laboral o contractual; cumplir esta Normativa; e informar de inmediato a la Delegada de Protección de Datos sobre cualquier incidente o riesgo de vulneración.

Artículo 16.- Encargados externos del tratamiento. Cuando la institución contrate servicios que impliquen el tratamiento de datos personales por cuenta de esta; incluyendo, de ser el caso, el proveedor del sistema FÉNIX, los proveedores de soporte del sistema de videovigilancia y del sistema biométrico u otras plataformas tecnológicas de terceros, deberá suscribirse un contrato escrito que detalle el objeto, la duración, la naturaleza y finalidad del tratamiento, las categorías de datos y las obligaciones del encargado, conforme a la LOPDP y a los Títulos VI y VII de esta Normativa.

TÍTULO III

CATEGORÍAS DE DATOS TRATADOS Y FINALIDADES

Artículo 17.- Datos de clientes y facturación. La institución trata datos de identificación (cédula o RUC) de los clientes que soliciten factura por la venta de combustibles y servicios conexos, conforme a la normativa tributaria del Servicio de Rentas Internas (SRI).

Artículo 18.- Datos de servidores y trabajadores. Se tratan datos de identificación, contacto e información contractual del personal, con la finalidad de gestionar la relación laboral, conforme al Reglamento Interno y la normativa laboral aplicable.

Artículo 19.- Datos de evaluación de desempeño. Conforme al Reglamento del Subsistema de Evaluación del Desempeño, se tratan datos relativos al cumplimiento de compromisos individuales, sanciones disciplinarias que inciden en la calificación, y evaluaciones de percepción sobre el nivel jerárquico superior, estas últimas de carácter confidencial. Los resultados se reportan al Ministerio del Trabajo conforme a la normativa del servicio público.

Artículo 20.- Datos de despacho de combustible institucional. Se tratan los datos contenidos en las solicitudes de despacho de combustible para vehículos

particulares del personal utilizados en diligencias institucionales, incluyendo la identificación del solicitante y la autorización de la Gerencia General.

Artículo 21.- Datos de usuarios de los servicios de parqueadero y lavadora. Se tratan datos de identificación del usuario, placa vehicular, y, en el caso de planes mensuales, los datos contenidos en el contrato y en el pagaré suscrito con garante solidario. El uso de tarjetas RFID para el control de acceso genera un registro de entradas y salidas del usuario, que constituye un dato de actividad sujeto a las mismas garantías de esta Normativa. El plan especial para servidores y trabajadores implica la verificación de su registro en la nómina institucional. Los datos de medios de pago se tratan conforme al artículo 29.

Artículo 22.- Datos financieros de anticipos de remuneración. Se tratan datos financieros del servidor o trabajador solicitante y del garante solidario que suscribe el pagaré, incluyendo la verificación de capacidad de endeudamiento, conforme al Reglamento Interno de Anticipos de Remuneraciones y su clasificación en el sistema FÉNIX. Este tratamiento se sujeta a los artículos 29 y 61 de esta Normativa.

Artículo 23.- Datos de solicitantes de información pública. En cumplimiento de la LOTAIP, se registran los datos de las personas que presenten solicitudes de acceso a la información pública, los cuales son reportados al Portal Nacional de Transparencia administrado por la Defensoría del Pueblo.

Artículo 24.- Datos en procesos de cobro coactivo. En el ejercicio de la jurisdicción coactiva, se tratan datos de identificación, domicilio, lugar de trabajo y patrimoniales del coactivado y, de ser el caso, de su garante, incluyendo la información que se requiera a terceros conforme al artículo 47. Este tratamiento se sujeta a los artículos 29 y 61 de esta Normativa.

Artículo 25.- Datos contenidos en informes e instrumentos de control institucional. Los informes de auditoría u otros instrumentos emitidos por organismos de control que individualicen a servidores con hallazgos de responsabilidad administrativa, civil o indicios de responsabilidad penal, serán tratados con estricta reserva y sujetos al procedimiento de coordinación previsto en el artículo 13 antes de su difusión o publicación.

Artículo 26.- Datos de videovigilancia. La institución cuenta con un sistema de videovigilancia de quince (15) cámaras instaladas, de las cuales doce (12) se encuentran operativas y tres (3) deshabilitadas, conectadas a un grabador digital de video. Se tratan imágenes de personas y vehículos, sin audio, con la finalidad de seguridad de personas, bienes e instalaciones. El tratamiento se funda en el cumplimiento de una misión realizada en interés público (LOPDP, art. 7 num. 4). Las grabaciones ordinarias se conservan hasta quince (15) días y las vinculadas a un incidente o requerimiento se bloquean hasta el cierre del expediente. Las imágenes no se utilizan para evaluar el desempeño ni para controlar la asistencia del personal. Su operación se rige por el artículo 64 y por el manual operativo respectivo.

Artículo 27.- Datos biométricos del personal. La institución utiliza un terminal biométrico de huella dactilar para registrar la asistencia del personal. La huella dactilar es un dato sensible y su tratamiento es de alto riesgo y de gran escala. Se funda, sujeto a su validación en la evaluación de impacto, en la causal del artículo 26 literal b) de la LOPDP (derecho laboral) y no en el consentimiento, dada la asimetría propia de la relación laboral. Su operación se rige por el artículo 65 y por el manual operativo respectivo.

Artículo 28.- Categorías especiales de datos personales. La institución tratará categorías especiales de datos personales (entre ellas, datos biométricos y datos de salud contenidos en justificativos médicos del personal) únicamente cuando concurra alguna de las causales previstas en el artículo 26 de la LOPDP, bajo estricta confidencialidad y con acceso restringido al personal autorizado.

Artículo 29.- Datos crediticios, de pago y sujetos a sigilo. Se observan las siguientes reglas: a) los reportes del Registro de Datos Crediticios solo se consultan con autorización del titular, se usan exclusivamente para el análisis crediticio y no pueden comercializarse ni emplearse para otro fin; b) los datos crediticios no se comunican con una antigüedad mayor al límite más estricto aplicable entre el artículo 358 del COMF (cuatro años) y el artículo 28 de la LOPDP (cinco años); c) si la institución reportare información de riesgo crediticio, responde por su exactitud y rectifica de inmediato la inexacta; d) la información obtenida de entidades financieras mantiene su sigilo y reserva, se usa solo para el fin requerido y su acceso se restringe; y, e) los medios de pago electrónicos se procesan únicamente a través de entidades autorizadas para operarlos, y los datos de tarjetas no se almacenan en los sistemas institucionales salvo necesidad y base de legitimación.

Artículo 30.- Prohibición de uso para fines distintos. Los datos personales tratados por la institución no podrán utilizarse para fines distintos de los informados a su titular, salvo habilitación legal expresa o consentimiento del titular.

TÍTULO IV
BASES DE LICITUD Y CONSENTIMIENTO

Artículo 31.- Bases de legitimación. El tratamiento se sustentará en alguna de las siguientes bases de licitud conforme a la LOPDP: consentimiento del titular; cumplimiento de una obligación legal; ejecución de relaciones contractuales o precontractuales; o cumplimiento de una misión realizada en interés público; y, tratándose de datos sensibles, una de las causales del artículo 26 de la LOPDP. La institución no podrá invocar el interés legítimo como base de legitimación, en razón de que la normativa de la SPDP restringe expresamente su aplicación al sector privado, condición que no ostenta la institución en su calidad de empresa pública. La regla del COESCCI que hace del consentimiento previo la base general se aplica en lo que no contradiga la LOPDP.

Artículo 32.- Consentimiento y su revocatoria. Cuando el tratamiento se sustente en el consentimiento del titular, este será libre, específico, informado e inequívoco, y podrá revocarse en cualquier momento sin efecto retroactivo, mediante los canales

que la institución habilite para el efecto. En las relaciones con el personal, el consentimiento no se utiliza como base cuando exista asimetría significativa y, si se usare, será explícito y se ofrecerá una alternativa equivalente.

TÍTULO V
DERECHOS DE LOS TITULARES

Artículo 33.- Derechos reconocidos. Los titulares podrán ejercer, de forma gratuita, los derechos de información, acceso, rectificación y actualización, eliminación, oposición, portabilidad, suspensión del tratamiento y a no ser objeto de decisiones basadas únicamente en valoraciones automatizadas, conforme a la LOPDP.

Artículo 34.- Procedimiento y plazos. Las solicitudes se presentan ante la Delegada de Protección de Datos Personales, por escrito, a través del correo epinto@gasolineraespochep.ec, del servicio en línea del portal institucional o de forma física en las instalaciones de la institución. La Delegada verifica la identidad del solicitante, registra la solicitud con acuse de recepción que consigna fecha y hora, y comunica la respuesta dentro del plazo de quince (15) días, conforme lo dispone la LOPDP. Si la solicitud requiere aclaración, se solicita por una sola vez dentro de los cinco (5) días siguientes, y el titular dispone de diez (10) días para completarla.

Artículo 35.- Medios electrónicos para información y consentimiento. Cuando la institución informe o recabe el consentimiento por medios electrónicos, informará previamente al titular sobre los equipos y programas necesarios, obtendrá su confirmación de que puede acceder a la información, le ofrecerá la opción de recibirla en papel sin costo y le permitirá revocar su consentimiento sin costo. La información podrá incorporarse por remisión mediante enlace o código QR de acceso directo cuando el titular la conozca y la acepte expresamente. Las comunicaciones periódicas incluirán un mecanismo para dejar de recibirlas y se suspenderán de inmediato al ejercerse.

Artículo 36.- Ejercicio del derecho de suspensión. Recibida la solicitud de suspensión, la institución deberá suspender el tratamiento correspondiente en un término no mayor a tres (3) días; si el tratamiento hubiere sido objeto de encargo, notificará de inmediato al encargado, quien deberá suspenderlo dentro del mismo término contado desde la notificación. La institución podrá continuar el tratamiento, no obstante la suspensión, únicamente para la formulación, ejercicio o defensa de reclamaciones; para proteger los derechos de otra persona; por razones de interés público establecidas en una norma con rango de ley; o por obligaciones legales previamente establecidas.

Artículo 37.- Ejercicio del derecho de eliminación. Cuando el titular ejerciere su derecho de eliminación, la institución le entregará un documento que acredite la eliminación de sus datos personales, incluidas las medidas de seguridad implementadas, tanto en repositorios físicos como digitales. La institución notificará a todos los encargados y terceros a quienes hubiere transferido o comunicado los datos, para que estos procedan a su eliminación dentro del término de tres (3) días,

salvo que contaren con una base de legitimación para su conservación o fueren a iniciar un tratamiento distinto, en cuyo caso asumirán la calidad de responsables. La eliminación de documentos públicos se coordina conforme al artículo 52 de la presente normativa. Este derecho se extiende a los datos de personas fallecidas, a solicitud de sus titulares de derechos sucesorios.

Artículo 38.- Ejercicio del derecho de portabilidad. Cuando la transferencia de datos personales a otro responsable, a solicitud del titular, se hubiere completado exitosamente, la institución quedará obligada a eliminar los datos transferidos de sus propios sistemas, salvo que contare con una base de legitimación para su conservación distinta al interés legítimo.

Artículo 39.- Portal de protección de datos y servicio en línea. En cumplimiento de la Disposición General Vigésima Sexta del COESCCI, la institución publica en su portal institucional: a) los derechos de los titulares, incluido el derecho a conocer el uso, finalidad, origen y destino de la información y el tiempo de conservación; b) sus políticas y procedimientos de protección de datos, esto es, la versión pública de esta Normativa, los avisos de privacidad y el contacto de la Delegada; y, c) un servicio en línea para consultas y reclamos sobre datos personales. Dicho servicio utiliza sistemas seguros, informa al usuario sobre el tipo de seguridad aplicado y emite acuse de recepción con fecha y hora.

Artículo 40.- Reclamos ante la Autoridad. De no obtener respuesta oportuna o satisfactoria, el titular podrá presentar su reclamo ante la SPDP exclusivamente a través del canal digital habilitado en su página web institucional o en el SISPDP, con firma electrónica válida a través de FirmaEC o, excepcionalmente, con firma manuscrita digitalizada, conforme a la LOPDP.

TÍTULO VI

TRANSFERENCIA Y COMUNICACIÓN DE DATOS A TERCEROS

Artículo 41.- Reglas generales. La institución únicamente transferirá o comunicará datos personales a terceros cuando cuente con el consentimiento del titular o cuando exista una habilitación legal expresa, conforme a la LOPDP, su Reglamento General, y a las resoluciones de la SPDP.

Artículo 42.- Transferencias por obligación legal. Se reconocen como transferencias amparadas en obligación legal, entre otras: el reporte de resultados de evaluación de desempeño al Ministerio del Trabajo; el registro de solicitantes de información pública en el Portal Nacional de Transparencia de la Defensoría del Pueblo; y la remisión de información a la SPDP, al SRI y a los demás organismos de control competentes.

Artículo 43.- Encargados externos y sistemas de terceros. El uso del sistema FÉNIX y de cualquier otra plataforma tecnológica administrada por un tercero para el tratamiento de datos personales institucionales deberá contar con el respectivo instrumento contractual o interinstitucional que garantice el cumplimiento de la LOPDP por parte del proveedor o administrador del sistema.

Artículo 44.- Clasificación de datos y servicios tecnológicos de terceros. La institución clasifica sus datos como reservados, confidenciales o abiertos; y, registra la clasificación en el Registro de Actividades de Tratamiento. Los datos personales se clasifican como confidenciales, sin perjuicio de los que la ley declara de acceso público (LOPDP, art. 2). Los servicios tecnológicos de terceros que alojen o procesen datos se contratan solo con proveedores cuyos centros de cómputo cumplan estándares internacionales de seguridad y protección, y los datos reservados o confidenciales por motivos de seguridad nacional que pertenezcan al Estado se alojan en territorio ecuatoriano. En la adquisición, actualización o mantenimiento de software o firmware queda prohibida la instalación de agentes o mecanismos que extraigan información de la institución sin su autorización y conocimiento. En las adquisiciones de software se observan, cuando corresponda, la evaluación y la prelación de los artículos 145 y 148 del COESCCI.

Artículo 45.- Cláusulas de protección de datos en contratos. Todo contrato que la institución suscriba con un encargado o tercero que implique el tratamiento de datos personales incorporará una cláusula de protección de datos personales que, no podrá:

- Ser ambigua o vaga respecto del tratamiento, la finalidad o los derechos de los titulares;
- Permitir finalidades no legítimas, lícitas, específicas o explícitas;
- Carecer de una base de legitimación para el tratamiento;
- Omitir la identidad del responsable o del encargado, los derechos del titular u otra información relevante;
- Eximir a las partes de implementar medidas de seguridad;
- Permitir la recopilación de más datos de los estrictamente necesarios;
- Limitar indebidamente el ejercicio de los derechos de los titulares;
- Permitir transferencias ulteriores sin garantías adecuadas o sin informar al titular;
- Contener exenciones excesivas de responsabilidad; u,
- Omitir el plazo de conservación de los datos personales.

Artículo 46.- Obligaciones del encargado al finalizar la relación jurídica. Concluida la relación jurídica con un encargado del tratamiento, este deberá devolver o eliminar los datos personales tratados dentro del término de cinco (5) días, y entregar a la institución el documento que acredite dicha devolución o eliminación. Los contratos de encargo incorporarán una cláusula específica que garantice el cumplimiento de esta obligación.

Artículo 47.- Requerimiento de datos a terceros en procesos coactivos. La facultad de requerir información relativa a los coactivados a personas naturales o jurídicas, públicas o privadas, se ejercerá de forma proporcional y limitada a lo estrictamente necesario para la sustanciación del procedimiento coactivo, dejando constancia de dicho requerimiento en el expediente. Los requerimientos a entidades del sistema financiero se apoyan en una excepción legal al sigilo y reserva, y quien obtiene la información asume la responsabilidad inherente al sigilo y la reserva.

Artículo 48.- Filtro de datos personales previo a publicaciones. Ninguna dependencia institucional publicará, en el portal institucional o en el Portal Nacional de Transparencia, documentos que individualicen a personas naturales con hallazgos de responsabilidad administrativa, civil o indicios de responsabilidad penal, sin la evaluación previa de la Delegada de Protección de Datos Personales prevista en el artículo 13 de esta Normativa.

Artículo 49.- Documentación de respaldo y conservación de las transferencias. La institución conservará, por un período mínimo de tres (3) años, la documentación que respalde, demuestre y acredite la legalidad y legitimidad de cada transferencia o comunicación de datos personales que realice, la cual estará disponible para la SPDP cuando esta la requiera.

Artículo 50.- Acuerdos escritos con destinatarios y responsabilidad del destinatario. Toda transferencia nacional a un tercero deberá formalizarse mediante un acuerdo escrito en el que el destinatario se comprometa a utilizar los datos personales únicamente para los fines autorizados. El destinatario que reciba los datos personales asumirá, desde ese momento, la calidad de responsable del tratamiento respecto de dichos datos.

TÍTULO VII
CONSERVACIÓN, ARCHIVO, DOCUMENTOS ELECTRÓNICOS, SEUDONIMIZACIÓN, ANONIMIZACIÓN Y BLOQUEO

Artículo 51.- Plazos de conservación. Los datos personales se conservarán conforme a los siguientes plazos de referencia, transcurridos los cuales serán eliminados, bloqueados o anonimizados:

Categoría de datos	Plazo de conservación
Datos de clientes y facturación	7 años, conforme a la normativa tributaria del SRI
Datos de servidores y trabajadores activos	Mientras dure la relación laboral, más el plazo de prescripción de obligaciones laborales
Evaluaciones de desempeño	5 años, conforme a los plazos de reincidencia del Reglamento del Subsistema de Evaluación
Contratos y pagarés de planes de parqueadero	Vigencia del contrato, más 7 años por eventual proceso de cobro
Registros de acceso RFID (entradas y salidas)	1 año, salvo que formen parte de un proceso en curso

Anticipos de remuneración (pagaré, garante)	Hasta la extinción total de la obligación, más el plazo de prescripción civil
Expedientes de cobro coactivo	Hasta la extinción de la obligación o prescripción de la acción coactiva
Solicitudes de acceso a la información pública (LOTAIP)	2 años, conforme a los plazos del Portal Nacional de Transparencia
Informes y comunicaciones de órganos de control (Contraloría)	Conservación permanente del expediente; la versión publicada se somete al filtro del Art. 48
Grabaciones ordinarias de videovigilancia	Hasta 15 días, mediante sobrescritura cíclica
Copias y fragmentos de videovigilancia vinculados a incidentes o requerimientos	Bloqueados hasta el cierre del expediente y los plazos legales aplicables
Plantilla biométrica (huella dactilar)	Mientras dure la relación y el mecanismo; eliminación dentro de 5 días hábiles desde la baja, el cambio de mecanismo o la revocatoria
Registros de marcación de asistencia	Mientras dure la relación laboral, más el plazo de prescripción de las acciones laborales aplicable
Documentación de respaldo de transferencias de datos	3 años, conforme al Art. 4 de la Resolución SPDP-SPD-2026-0004-R
Informes de auditoría y de cumplimiento (tratamientos de gran escala)	5 años, conforme a los Arts. 17 y 18 de la Resolución SPDP-SPD-2026-0005-R

Artículo 52.- Archivo y eliminación de documentos públicos. La eliminación de datos personales contenidos en documentos públicos se coordina con la unidad de Archivo y Gestión Documental y se sujeta a la tabla de plazos de conservación documental y a la regla técnica nacional para la organización y mantenimiento de

los archivos públicos. La conservación de documentos que constituyan patrimonio del Estado, o que sean necesarios para cumplir una obligación legal, se ampara en los artículos 10 literal i) y 18 numerales 2 y 10 de la LOPDP. Toda eliminación se documenta mediante acta, y los originales físicos de contratos, pagarés u otros títulos no se destruyen por haber sido digitalizados.

Artículo 53.- Documentos electrónicos y firma electrónica. Los mensajes de datos y los documentos firmados electrónicamente tienen validez jurídica y valor probatorio. La institución adopta como estándar, en cumplimiento de la norma de control interno 410-17 y del artículo 94 del Código Orgánico Administrativo, las siguientes reglas: a) las firmas electrónicas se generan y verifican con el aplicativo FirmaEC; b) un documento firmado electrónicamente se conserva en su original electrónico y, si se imprime o se escanea después de impreso, pierde su integridad y autenticidad; c) un mismo instrumento no combina firmas electrónicas y manuscritas; d) los registros electrónicos conservan su origen, destino, fecha y hora e integridad, con códigos de verificación cuando corresponda; e) la digitalización de documentos físicos para sustituir sus originales cumple los requisitos del Reglamento a la Ley 67, arts. 4 y 5; y, f) quienes administran, archivan o conservan información pública responden personalmente por su ocultación, alteración o pérdida (LOTAIP, art. 10).

Artículo 54.- Seudonimización. La institución podrá seudonimizar datos personales como medida técnica de seguridad, previo un análisis de gestión de riesgos, en los casos de prestación de servicios cuando no sea imprescindible conocer la identidad del titular, procesos de investigación estadística, o auditorías internas y pruebas de sistemas. Los datos seudonimizados mantendrán el estatus de datos personales. Toda acción de reidentificación será registrada.

Artículo 55.- Anonimización. La anonimización que realice la institución deberá ser exhaustiva, considerando todos los atributos que, directa o indirectamente, pudieren llevar a la reidentificación del titular. Tratándose de datos de salud, se priorizará la anonimización sobre otras medidas, y todo tratamiento de datos de salud anonimizados requerirá la autorización previa de la SPDP. Los datos debidamente anonimizados no requerirán del consentimiento del titular para su transferencia o comunicación.

Artículo 56.- Bloqueo. Cumplida la finalidad del tratamiento, los datos personales podrán conservarse bajo la medida de bloqueo, que implica su mantenimiento seguro con acceso limitado y restringido, únicamente cuando existiere una base de legitimación que lo habilite.

TÍTULO VIII
MEDIDAS DE SEGURIDAD

Artículo 57.- Medidas organizativas. La institución implementará procedimientos internos de acceso, uso y custodia de la información; capacitación periódica al personal; y suscripción de compromisos de confidencialidad por parte del personal, proveedores y terceros.

Artículo 58.- Medidas técnicas. Se implementarán controles de acceso mediante usuarios y credenciales individuales, contraseñas seguras, respaldo periódico de la información, y protección de los equipos y sistemas frente a accesos no autorizados, incluyendo los sistemas de videovigilancia, el terminal biométrico y los que administran los registros de las tarjetas RFID. Los formularios y servicios electrónicos que reciban datos personales usan canales seguros e informan sobre la seguridad aplicada.

Artículo 59.- Control de acceso y confidencialidad. El acceso a los datos personales estará limitado al personal autorizado en función de sus competencias. Todo acceso, uso o divulgación indebida constituirá infracción y dará lugar a las responsabilidades administrativas, civiles o penales correspondientes.

TÍTULO IX
GESTIÓN DE RIESGOS, TRATAMIENTO A GRAN ESCALA Y EVALUACIÓN DE IMPACTO

Artículo 60.- Tratamiento a gran escala: metodología. Conforme a la Resolución SPDP-SPD-2026-0005-R, la Delegada de Protección de Datos Personales determinará, para cada tratamiento identificado en el Título III, si este alcanza la calificación de "gran escala", aplicando el Modelo Técnico de Gran Escala (MTGE), que suma el puntaje de las siguientes seis variables:

Variable	Puntaje mínimo	Puntaje máximo
Número de titulares (12 meses)	1 punto (hasta 1.000)	4 puntos (más de 100.000)
Volumen de datos por titular	0,5 puntos (hasta 10 tipos)	3 puntos (más de 100 tipos)
Categorías de datos	0,5 puntos (datos básicos)	3 puntos (más de una categoría especial, grupos vulnerables o datos penales)
Frecuencia del tratamiento	0,5 puntos (puntual)	2 puntos (continua o en tiempo real)
Permanencia del tratamiento	0,5 puntos (ocasional)	2 puntos (prolongada)
Alcance geográfico	1 punto (local)	3 puntos (global o transfronterizo)

El tratamiento será considerado de gran escala cuando el puntaje total fuere igual o superior a seis (6) puntos. El resultado del cálculo se documentará en el Registro de Actividades de Tratamiento y se actualizará al menos una vez al año.

Artículo 61.- Casos de calificación directa de tratamiento a gran escala. Conforme al artículo 14 de la Resolución SPDP-SPD-2026-0005-R, constituyen tratamiento a gran escala de manera directa y obligatoria, sin necesidad de aplicar el MTGE, entre otros: los tratamientos de datos sensibles y de datos biométricos; la observación, vigilancia o monitoreo sistemático de personas en zonas de acceso público mediante videovigilancia; y el tratamiento estructural de datos personales en sistemas de información crediticia, financiera o de evaluación de riesgo económico. En consecuencia, se califican como de gran escala el sistema biométrico del artículo 27, las cámaras de videovigilancia que cubren zonas de acceso público (artículo 26) y, previa evaluación de la Delegada, los tratamientos de anticipos de remuneración (artículo 22) y de cobro coactivo (artículo 24).

Artículo 62.- Evaluación de impacto (EIPD). Conforme al artículo 42 de la LOPDP, al artículo 12 de la Resolución SPDP-SPD-2026-0005-R y al artículo 15 de la Resolución SPDP-SPD-2026-0039-R, la evaluación de impacto es obligatoria, de forma previa a su implementación o continuidad, para todo tratamiento calificado como de gran escala. Para los sistemas de videovigilancia y biométrico actualmente en operación, se ejecutará dentro de los sesenta (60) días siguientes a la aprobación de esta Normativa. Su ejecución corresponde a la institución, a través de las unidades responsables; la Delegada emite observaciones y orientaciones no vinculantes. La evaluación del sistema biométrico se revisa cada doce (12) meses y cuando cambie el nivel de riesgo.

Artículo 63.- Contenido mínimo de la evaluación de impacto. La evaluación de impacto contendrá, al menos: la descripción sistemática de las operaciones de tratamiento y sus finalidades; la justificación de su necesidad y proporcionalidad; los niveles de riesgo obtenidos conforme a los criterios de evaluación aplicados; y las medidas previstas para hacer frente a los riesgos identificados, incluidas las garantías y medidas de seguridad adoptadas. La información contenida en la evaluación se limitará a la necesaria para respaldarla, sin incluir detalles confidenciales relacionados con las implementaciones de seguridad.

Artículo 64.- Reglas de videovigilancia. El sistema de videovigilancia se sujeta a las siguientes reglas: a) su finalidad se limita a la seguridad de personas, bienes o instalaciones; b) queda prohibida la grabación de audio, incluso con fines de supervisión del desempeño laboral, y las funciones de detección o búsqueda de rostros permanecen deshabilitadas salvo evaluación de impacto y autorización previas; c) queda prohibido videovigilar baños, vestidores, lactarios, comedores u otras zonas que vulneren la intimidad; d) cada cámara cuenta con justificación documentada de su necesidad, y las que cubren oficinas se reproducen únicamente ante un incidente de seguridad documentado; e) las imágenes no se emplean para evaluar el desempeño ni controlar la asistencia del personal, y solo excepcionalmente pueden aportarse como evidencia de un incidente de

seguridad concreto, con autorización escrita de la Gerencia General, aviso a la Delegada y garantía del derecho de defensa del servidor; f) las zonas videovigiladas se señalizan con información por capas, y el aviso de privacidad se publica en el portal institucional; g) las copias a autoridades competentes se entregan bajo requerimiento escrito y con registro de cadena de custodia, y conservan fecha, hora, cámara de origen e integridad; y, h) el acceso remoto o en la nube del fabricante requiere autorización de la Gerencia General, criterio de la Delegada y evaluación previa de transferencias. Los criterios del artículo 15 de la Resolución SPDP-SPD-2025-0041-R se aplican como referencia de buenas prácticas.

Artículo 65.- Reglas del sistema biométrico. El sistema biométrico se sujeta a las siguientes reglas: a) solo se mantiene si la evaluación de impacto acredita su necesidad estricta y la insuficiencia de alternativas no biométricas, y la Gerencia General decide, con base en ella, mantener la huella dactilar o migrar a un mecanismo no biométrico; b) se ofrece siempre a cada servidor un mecanismo alternativo equivalente que no requiera biometría, sin consecuencia desfavorable, y quien opta por él es dado de baja del enrolamiento; c) se privilegia la plantilla biométrica y no se conservan imágenes ni rostros; d) la plantilla se elimina dentro de cinco (5) días hábiles desde la desvinculación, el cambio de mecanismo o la revocatoria, con acta; e) los datos biométricos no se reutilizan para finalidad distinta, como el control de acceso físico o la vigilancia; f) ninguna sanción, descuento o decisión que afecte derechos se adopta exclusivamente con base en el registro biométrico, y el servidor puede pedir una explicación motivada; g) no se enrolan niñas, niños ni adolescentes; y, h) las funciones de reconocimiento facial, captura de imágenes y conexión a plataformas externas del terminal permanecen deshabilitadas salvo evaluación de impacto y autorización previas.

Artículo 66.- Sistemas de inteligencia artificial. Si la institución desarrolla, implementa o utiliza sistemas de inteligencia artificial que traten datos personales; incluyendo las funciones de analítica de los equipos de videovigilancia o biométricos y los sistemas provistos por un encargado externo, tales como el sistema FÉNIX, dicho tratamiento se sujetará a la Resolución SPDP-SPD-2026-0009-R y su reforma contenida en la Resolución SPDP-SPD-2026-0037-R, debiendo realizarse la gestión de riesgos y, cuando corresponda, la evaluación de impacto, de manera previa al desarrollo o implementación del sistema.

Artículo 67.- Auditorías y conservación de informes. Los tratamientos calificados como de gran escala se someterán a auditorías internas o externas con periodicidad al menos anual. Los informes de auditoría y los informes anuales de cumplimiento se conservarán por un período mínimo de cinco (5) años.

TÍTULO X
GESTIÓN DE INCIDENTES Y VULNERACIONES DE SEGURIDAD

Artículo 68.- Incidente de seguridad. Se considerará incidente de seguridad cualquier evento que afecte la confidencialidad, integridad o disponibilidad de los datos personales tratados por la institución.

Artículo 69.- Reporte y contención. Todo incidente o sospecha de incidente será reportado de inmediato a la Delegada de Protección de Datos Personales, quien coordinará las acciones de contención y análisis.

Artículo 70.- Notificación. Cuando el incidente represente un riesgo para los derechos y libertades de los titulares, se notificará a la SPDP dentro del plazo máximo de cinco (5) días y, de ser necesario, a los titulares afectados dentro de tres (3) días, conforme a la LOPDP. Se dejará constancia de la fecha y hora de conocimiento del incidente y de cada notificación.

Artículo 71.- Registro de incidentes. La institución mantendrá un Registro Interno de Incidentes de Seguridad, bajo supervisión de la Delegada de Protección de Datos Personales.

TÍTULO XI
REGISTRO DE ACTIVIDADES Y REGISTRO NACIONAL

Artículo 72.- Registro de Actividades de Tratamiento. La institución mantendrá actualizado un Registro de Actividades de Tratamiento que consigne, para cada uno de los tratamientos descritos en el Título III, las finalidades, categorías de datos, categorías de titulares, plazos de conservación, medidas de seguridad aplicadas, la clasificación del dato conforme al artículo 44, y el resultado de la calificación de gran escala conforme al artículo 60. Este registro estará disponible para la SPDP cuando esta lo requiera.

Artículo 73.- Registro Nacional de Protección de Datos Personales. La institución reportará y mantendrá actualizada ante la SPDP la información de sus bases de datos en el Registro Nacional de Protección de Datos Personales, dentro del término de diez (10) días desde el inicio de cada tratamiento, conforme al artículo 51 de la LOPDP.

TÍTULO XII
RESPONSABILIDAD Y CUMPLIMIENTO

Artículo 74.- Incumplimiento. El incumplimiento de esta Normativa dará lugar a las responsabilidades administrativas, civiles o penales a que hubiere lugar, sin perjuicio de las sanciones previstas en la LOPDP.

Artículo 75.- Vigencia, revisión y cumplimiento. Esta Normativa será revisada y actualizada periódicamente por la Delegada de Protección de Datos Personales, o cuando se produzcan cambios normativos, tecnológicos o institucionales que así lo requieran, incluida la emisión de nueva normativa técnica por parte de la SPDP.

DISPOSICIONES GENERALES

Primera.- Esta Normativa es de cumplimiento obligatorio para todas las autoridades, servidores, trabajadores, proveedores y terceros que intervengan en el tratamiento de datos personales bajo responsabilidad de la institución.

Segunda.- Los casos no previstos en esta Normativa se resolverán aplicando la LOPDP, su Reglamento General y las resoluciones de la SPDP.

Tercera.- Se deja constancia de que la Resolución Administrativa No. RES-034-GR-GASPOCH-EP-2025, que expidió el Protocolo de Tratamiento de Datos Personales, fue derogada mediante la Resolución Administrativa No. RES-056-GR-GASPOCH-EP-2026, de 4 de septiembre de 2026, y que la presente Normativa lo sustituye.

DISPOSICIONES TRANSITORIAS

Primera.- En un plazo no mayor a sesenta (60) días desde la aprobación de esta Normativa, la Delegada de Protección de Datos Personales, en coordinación con las unidades señaladas en el artículo 14, aplicará el MTGE a los tratamientos descritos en el Título III y actualizará el Registro de Actividades de Tratamiento conforme al artículo 72, incluyendo la ficha de los tratamientos de videovigilancia y de control biométrico, y reportará los tratamientos al Registro Nacional.

Segunda.- En un plazo no mayor a treinta (30) días, la unidad de Tecnologías de la Información y Comunicación verificará y documentará la configuración técnica de los sistemas de videovigilancia y biométrico (audio, funciones faciales, conexiones remotas, agentes o telemetría y almacenamiento), y la comunicará a la Delegada y a la Gerencia General, que decidirá sobre las cámaras deshabilitadas y sobre el plan de soporte o reemplazo de los equipos discontinuados.

Tercera.- En un plazo no mayor a sesenta (60) días, la institución ejecutará las evaluaciones de impacto previstas en el artículo 62, completará el análisis de necesidad y alternativas del sistema biométrico, habilitará el mecanismo alternativo, entregará los avisos de privacidad, colocará la señalética por capas y pondrá en funcionamiento el portal y el servicio en línea del artículo 39.

Cuarta.- En un plazo no mayor a noventa (90) días: a) la Subgerencia de Asesoría Jurídica revisará los contratos vigentes con encargados y terceros para incorporar las cláusulas del artículo 45; b) la unidad de Archivo y Gestión Documental, con la Subgerencia de Asesoría Jurídica, verificará y propondrá la tabla de plazos de conservación documental conforme al artículo 52; y, c) la Subgerencia de Asesoría Jurídica y la Subgerencia Administrativa Financiera confirmarán el régimen aplicable al monedero electrónico de los usuarios recurrentes y a los medios de pago conforme al artículo 29.

Quinta.- Sin perjuicio de los plazos anteriores, los sistemas biométricos en uso se adecuarán a la Resolución SPDP-SPD-2026-0039-R dentro de los doce (12) meses contados desde su publicación en el Registro Oficial.

DISPOSICIÓN FINAL

La presente Normativa entrará en vigencia a partir de su suscripción, sin perjuicio de su publicación en los medios institucionales, con excepción de los anexos de seguridad de los manuales operativos, que no se publican.

Dado en la ciudad de Riobamba, en el despacho de Gerencia General de la Estación de Servicios ESPOCH Gasolinera Politécnica E.P., a los 15 días del mes de octubre de 2026.

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MATEO SEBASTIAN CORONEL CACEREZ

ING. MBA. MATEO CORONEL CÁCEREZ
GERENTE GENERAL
ESTACION DE SERVICIOS ESPOCH GASOLINERA POLITÉCNICA GASPOCH E. P.

ELABORADO POR: AB. ESTEFANIA PINTO DELEGADA PROTECCION DATOS GASPOCH EP 15/10 /2026	Validar únicamente en FirmaEC. Firmado electrónicamente por: ANDREA ESTEFANIA PINTO MORALES
REVISADO POR: AB. PAULINA PÉREZ CHICO SUBGERENTE JURÍDICO GASPOCH EP 15/10 /2026	Validar únicamente en FirmaEC. Firmado electrónicamente por: MYRIAM PAULINA PEREZ CHICO