Resolución Nro. EMASEO-GGE-2026-0010-R

Quito, D.M., 31 de julio de 2026

EMPRESA PÚBLICA METROPOLITANA DE ASEO

ECON. JUAN PABLO POZO CEVALLOS
GERENTE GENERAL
EMPRESA PÚBLICA METROPOLITANA DE ASEO
EMASEO EP.

CONSIDERANDO:

Que, los números 2, 8 y 9 del artículo 11 de la Constitución de la República del Ecuador establece los principios de igualdad, progresividad y deber estatal de respetar y hacer respetar los derechos garantizados en la Constitución;

Que, el número 19 del artículo 66 de la Constitución de la República del Ecuador reconoce y garantiza a las personas el derecho a la protección de datos de carácter personal, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección;

Que, el artículo 82 de la Constitución de la República del Ecuador establece el derecho a la seguridad jurídica, fundamentado en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes;

Que, el artículo 92 de la Constitución de la República del Ecuador reconoce el derecho de toda persona a conocer la existencia y acceder a documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico;

Que, el número 2 del artículo 225 de la Constitución de la República del Ecuador establece que el sector público comprende, entre otras, a las entidades que integran el régimen autónomo descentralizado;

Que, el artículo 226 de la Constitución de la República del Ecuador dispone que las instituciones del Estado, sus organismos, dependencias, servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades atribuidas en la Constitución y la ley, y tendrán el deber de coordinar acciones para el cumplimiento de sus fines;

Que, el artículo 227 de la Constitución de la República del Ecuador dispone que la administración pública constituye un servicio a la colectividad y se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización,

coordinación, participación, planificación, transparencia y evaluación;

Que, el artículo 315 de la Constitución de la República del Ecuador establece que el Estado constituirá empresas públicas para la gestión de sectores estratégicos, la prestación de servicios públicos, el aprovechamiento sustentable de recursos naturales o de bienes públicos y el desarrollo de otras actividades económicas;

Que, el artículo 14 del Código Orgánico Administrativo establece el principio de juridicidad, en virtud del cual la actuación administrativa se somete a la Constitución, a los instrumentos internacionales, a la ley, a los principios, a la jurisprudencia aplicable y al propio Código;

Que, los artículos 55 a 64 del Código Orgánico Administrativo regulan aspectos relativos a los órganos colegiados, su integración, convocatoria, quórum, sesiones, actas, votos particulares y utilización de medios electrónicos, en lo que resulte aplicable;

Que, el artículo 67 del Código Orgánico Administrativo dispone que el ejercicio de las competencias asignadas a los órganos o entidades administrativos incluye no solo lo expresamente definido en la ley, sino todo aquello que sea necesario para el cumplimiento de sus funciones;

Que, los artículos 68, 69, 70 y 71 del Código Orgánico Administrativo regulan la delegación de competencias, sus requisitos y efectos dentro de la administración pública;

Que, el artículo 1 de la Ley Orgánica de Protección de Datos Personales tiene por objeto y finalidad garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección;

Que, el artículo 4 de la Ley Orgánica de Protección de Datos Personales define, entre otros conceptos, al dato personal, dato sensible, responsable del tratamiento, encargado del tratamiento y Delegado de Protección de Datos Personales;

Que, el artículo 10 de la Ley Orgánica de Protección de Datos Personales establece los principios aplicables al tratamiento de datos personales, entre ellos juridicidad, lealtad, transparencia, finalidad, pertinencia y minimización, proporcionalidad, confidencialidad, calidad y exactitud, conservación, seguridad de datos personales, responsabilidad proactiva y demostrada, aplicación favorable al titular e independencia del control;

Que, el artículo 37 de la Ley Orgánica de Protección de Datos Personales dispone que el responsable o encargado del tratamiento deberá sujetarse al principio de seguridad de datos personales e implementar medidas técnicas, organizativas y de cualquier otra índole, con base en las categorías y volumen de datos, el estado de la técnica, mejores

prácticas, costos de aplicación, naturaleza, alcance, contexto y fines del tratamiento, así como la probabilidad de riesgos;

Que, el artículo 38 de la Ley Orgánica de Protección de Datos Personales establece que el mecanismo gubernamental de Seguridad de la Información deberá incluir las medidas que deban implementarse en el tratamiento de datos personales para hacer frente a riesgos, amenazas, vulnerabilidades, accesos no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita;

Que, el artículo 47 de la Ley Orgánica de Protección de Datos Personales establece las obligaciones del responsable y del encargado del tratamiento de datos personales, incluyendo la aplicación e implementación de requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas para garantizar y demostrar el cumplimiento normativo;

Que, el artículo 12 del Reglamento General a la Ley Orgánica de Protección de Datos Personales dispone que el responsable habilitará, preferentemente, herramientas o canales informáticos simplificados y de fácil acceso para que los titulares ejerzan sus derechos;

Que, el artículo 33 del Reglamento General a la Ley Orgánica de Protección de Datos Personales establece que el responsable del tratamiento deberá aplicar medidas apropiadas para la observancia efectiva de los principios de protección de datos y de los derechos reconocidos en la ley;

Que, el artículo 48 del Reglamento General a la Ley Orgánica de Protección de Datos Personales determina que el Delegado de Protección de Datos Personales asesora, vela y supervisa de manera independiente el cumplimiento de las obligaciones legales imputables al responsable y al encargado del tratamiento;

Que, el artículo 138 de la Codificación del Código Municipal para el Distrito Metropolitano de Quito, expedida mediante Ordenanza Metropolitana Nro. 095-2025, determina que el Gerente General ejerce la representación legal, judicial y extrajudicial de su respectiva empresa y es responsable ante el Directorio por su gestión administrativa, técnica y financiera;

Que, las letras a), b) y m) del artículo 142 de la Codificación del Código Municipal para el Distrito Metropolitano de Quito establecen como deberes y atribuciones del Gerente General cumplir y hacer cumplir las normas que rigen las actividades de la empresa pública metropolitana, dirigir y supervisar sus actividades, coordinar y controlar el funcionamiento de sus dependencias y adoptar las medidas adecuadas para garantizar una administración eficiente, transparente y de calidad;

Que, los números 1, 2, 4 y 8 del artículo 11 de la Ley Orgánica de Empresas Públicas

establecen como deberes y atribuciones de la o el Gerente General ejercer la representación legal, judicial y extrajudicial de la empresa pública; cumplir y hacer cumplir la ley, los reglamentos y demás normativa aplicable, incluidas las resoluciones emitidas por el Directorio; administrar la empresa pública, velando por su eficiencia empresarial; y aprobar y modificar los reglamentos internos que requiera la empresa, excepto el señalado en el numeral 8 del artículo 9 de la referida Ley;

Que, la letra d) del artículo 19, de la Ley Orgánica para la Transformación Digital y Audiovisual dispone que las entidades de la Administración Pública deberán establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información;

Que, el artículo 20 de la Ley Orgánica para la Transformación Digital y Audiovisual establece que el Marco de Seguridad Digital se articula y sustenta en las normas, procesos, roles, responsabilidades y mecanismos regulados e implementados a nivel nacional en materia de Seguridad de la Información;

Que, la Resolución Nro. SPDP-SPD-2025-0028-R, que contiene el Reglamento del Delegado de Protección de Datos Personales, regula las actividades de los delegados de protección de datos personales en el ejercicio de sus funciones, para el cumplimiento de la Ley Orgánica de Protección de Datos Personales y su Reglamento General;

Que, el artículo 12 del Reglamento del Delegado de Protección de Datos Personales dispone que incluso si prestare sus servicios bajo relación de dependencia, el delegado deberá mantener total independencia e imparcialidad en el ejercicio de sus funciones, correspondiendo al responsable garantizar mecanismos institucionales que eviten conflictos de interés y presiones indebidas;

Que, mediante Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003 de 08 de febrero de 2024, publicado en el Registro Oficial - Tercer Suplemento Nro. 509 de 1 de marzo de 2024, el Ministerio de Telecomunicaciones y de la Sociedad de la Información expidió el Esquema Gubernamental de Seguridad de la Información – EGSI que se encuentra como Anexo denominado ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACION (EGSI) Versión 3.0;

Que, el artículo 5 del Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003 dispone que es responsabilidad de la máxima autoridad de cada institución, en la implementación del EGSI, conformar la estructura de Seguridad de la información institucional, con personal formado y experiencia en gestión de Seguridad de la Información, así como asignar los recursos necesarios;

Que, el artículo 6 del Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003 dispone que la máxima autoridad designará, al interior de la institución, un Comité de Seguridad de la Información (CSI), integrado por los responsables de las áreas de Planificación,

Resolución Nro. EMASEO-GGE-2026-0010-R

Quito, D.M., 31 de julio de 2026

Talento Humano, Administrativa, Comunicación Social, Tecnologías de la Información, Jurídica y el Delegado de Protección de Datos, o quienes hagan sus veces, correspondiendo a Planificación presidirlo;

Que, la Disposición Transitoria Segunda del Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003 dispone que las máximas autoridades de las instituciones del sector público actualizarán o implementarán el EGSI en el plazo previsto en dicho instrumento;

Que, el artículo Décimo Séptimo del Estatuto de la Empresa Pública Metropolitana de Aseo EMASEO E.P., emitido mediante Resolución del Directorio No. 012-DIR-EMASEO-EP/2024/05/29, determina: *"(…) La o el Gerente General ejerce la representación legal, judicial, y extrajudicial, de la Empresa Pública Metropolitana de Aseo y es responsable ante el Directorio por su gestión administrativa, técnica y financiera. La o el Gerente General está facultado para realizar todos los actos y contratos necesarios para el cumplimiento de los fines de la empresa a su cargo (…)"*;

Que, mediante Resolución Nro. EMASEO-GGE-2026-0001-R de 05 de febrero de 2026, se designó formalmente al Ing. Javier Alejandro Salinas Sánchez como Oficial de Seguridad de la Información de EMASEO EP, disponiéndose su articulación con los procesos de adecuación del Esquema Gubernamental de Seguridad de la Información - EGSI v3.0;

Que, mediante Resolución Nro. EMASEO-GGE-2026-0004-R de 06 de marzo de 2026, se designó formalmente al Abg. Pablo Alexander Sánchez Mancero como Delegado de Protección de Datos Personales de EMASEO EP;

Que, conforme al documento Nro. EMASEO-SGT-2026-0310-M de 24 de julio de 2026 de solicitud de conformación e instalación formal del Comité de Seguridad de la Información de EMASEO EP bajo el marco del EGSI v3.0, una vez culminadas las fases iniciales de inventario de activos críticos y definición de la Declaración de Aplicabilidad (SoA), resulta indispensable formalizar la constitución de este cuerpo colegiado para validar las decisiones estratégicas de mitigación de riesgos de la empresa pública;

Que, el mismo documento propone la conformación del Comité con la Coordinación General de Planificación y Gestión Estratégica, la Subdirección de Gestión de TICs, la Dirección Jurídica, la Coordinación General Administrativa Financiera, la Dirección de Desarrollo Empresarial y el Delegado de Protección de Datos Personales, de conformidad con el modelo institucional de EMASEO EP;

En ejercicio de las atribuciones previstas en la Constitución de la República del Ecuador, el Código Orgánico Administrativo, la Ley Orgánica de Empresas Públicas, la Ley

Resolución Nro. EMASEO-GGE-2026-0010-R

Quito, D.M., 31 de julio de 2026

Orgánica de Protección de Datos Personales, su Reglamento General, la Codificación del Código Municipal para el Distrito Metropolitano de Quito, el Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003, y demás normativa aplicable;

RESUELVE:

EXPEDIR EL REGLAMENTO INTERNO PARA EL FUNCIONAMIENTO DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES DE LA EMPRESA PÚBLICA METROPOLITANA DE ASEO - EMASEO EP.

SECCIÓN I

DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

Artículo 1.- Definición. El Comité de Seguridad de la Información y Protección de Datos Personales de EMASEO EP, en adelante "el Comité", es el órgano colegiado interno encargado de dirigir, coordinar, supervisar y emitir lineamientos estratégicos para la implementación, el mantenimiento, la mejora continua y el seguimiento del Esquema Gubernamental de Seguridad de la Información - EGSI y del Sistema de Protección de Datos Personales de EMASEO EP, sin ejercer funciones operativas ni sustituir las competencias propias de las unidades responsables.

Artículo 2.- Naturaleza y enfoque. El Comité tendrá naturaleza estratégica, coordinadora y de supervisión institucional. Sus actuaciones deberán integrar la gestión de la Seguridad de la Información, la continuidad, la ciberseguridad, la gestión de incidentes y la protección de datos personales, con enfoque de riesgos, responsabilidad proactiva, privacidad desde el diseño y por defecto, confidencialidad, integridad y disponibilidad de la información.

Artículo 3.- Acciones en materia de Seguridad de la Información. En materia de Seguridad de la Información, el Comité conocerá, aprobará, coordinará o supervisará, según corresponda, las acciones necesarias para la implementación, el mantenimiento y la mejora continua del EGSI en EMASEO EP, incluyendo políticas, controles, gestión de riesgos, planes de tratamiento, planes de concienciación, gestión de incidentes, continuidad operativa, seguimiento de hallazgos y reportes institucionales al ente rector.

Artículo 4.- Acciones en materia de Protección de Datos Personales. En materia de Protección de Datos Personales, el Comité facilitará la ejecución de acciones y la gestión de actividades necesarias para que EMASEO EP, como responsable del tratamiento,

Resolución Nro. EMASEO-GGE-2026-0010-R

Quito, D.M., 31 de julio de 2026

implemente y mantenga su Sistema de Protección de Datos Personales, mediante mecanismos, herramientas, políticas, metodologías y medidas técnicas, físicas, organizativas, jurídicas, administrativas y tecnológicas que resulten pertinentes, conforme a la Ley Orgánica de Protección de Datos Personales, su Reglamento General y la normativa secundaria emitida por la Autoridad de Protección de Datos Personales.

Artículo 5.- Conformación. El Comité estará integrado por los siguientes miembros institucionales:

No.	Área / cargo	Participación
1	Coordinación General de Planificación y Gestión Estratégica o su delegado	Preside el Comité. Voz y voto.
2	Coordinación General Administrativa Financiera o su delegado	Miembro. Voz y voto.
3	Dirección Jurídica o su delegado	Miembro. Voz y voto.
4	Dirección de Desarrollo Empresarial o su delegado	Miembro. Voz y voto.
5	Subdirección de Gestión de TICs o su delegado	Miembro. Voz y voto.
6	Subdirección de Comunicación Social Relaciones Públicas y Marketing o su delegado	Miembro. Voz y voto
7	Oficial de Seguridad de la Información	Miembro. Voz sin voto.
8	Delegado/a de Protección de Datos Personales	Asesor/a jurídico/a. / Voz sin voto.

El/la Secretario/a del Comité será quien desempeñe el cargo de Subdirector de Calidad y Procesos y será el encargado de custodiar los expedientes, actas y documentos, de conformidad con el régimen aplicable de archivo, confidencialidad, transparencia y protección de datos personales.

Cuando la materia a tratar involucre competencias específicas de Talento Humano, Secretaría General, Operaciones, Ambiente, Contratación Pública, Atención Ciudadana u otra dependencia institucional, el Comité podrá convocar a sus titulares o delegados con voz, pero sin voto. Si, en el Estatuto Orgánico vigente de EMASEO EP, existieren unidades que hagan las veces de las áreas expresamente previstas en el artículo 6 del Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003, deberán incorporarse o comparecer permanentemente, conforme lo determine la Gerencia General o el propio Comité, sin perjuicio de la integración establecida en este artículo.

Artículo 7.- Participación del Delegado de Protección de Datos Personales. El Delegado de Protección de Datos Personales participará en el Comité con voz, pero sin voto, en calidad de asesor independiente y órgano de supervisión especializada. Su intervención no tendrá carácter resolutorio ni operativo. No podrá ser obligado a ejecutar

actividades que comprometan su independencia, imparcialidad o rol de control, sin perjuicio de emitir recomendaciones, observaciones, informes, alertas de cumplimiento y criterios técnicos-jurídicos en materia de protección de datos personales.

Artículo 8.- Ámbito de aplicación. Las disposiciones del presente Reglamento serán de aplicación obligatoria interna para los servidores y trabajadores de EMASEO EP, en el ámbito de sus funciones y responsabilidades institucionales. Su eventual exigibilidad frente a contratistas, proveedores, consultores, encargados del tratamiento o terceros requerirá del instrumento contractual, convencional o administrativo correspondiente, sin que el presente Reglamento sustituya tales instrumentos.

Artículo 9.- Obligación de cooperación. Todas las unidades administrativas, técnicas, operativas y de apoyo de EMASEO EP deberán entregar la información, documentación, evidencias, matrices, reportes y respaldos requeridos por el Comité, el Oficial de Seguridad de la Información, el Líder Implementador de Protección de Datos Personales o el Delegado de Protección de Datos Personales, dentro de los plazos establecidos en cada requerimiento, salvo imposibilidad debidamente motivada.

SECCIÓN II

RESPONSABILIDADES DEL COMITÉ Y DE SUS MIEMBROS

Artículo 10.- Responsabilidades generales del Comité. El Comité tendrá las siguientes responsabilidades:

1. Establecer los objetivos de Seguridad de la Información y protección de datos personales, alineados a los objetivos institucionales de EMASEO EP.
2. Conocer y aprobar el Plan de Tratamiento de Riesgos del EGSI para proteger los sistemas ERP, el catastro operativo, las bases de datos institucionales y demás activos de información críticos.
3. Validar, cuando corresponda, las exclusiones de control presentadas por la Oficialía de Seguridad de la Información, con base en la Declaración de Aplicabilidad (SoA), análisis de riesgos y justificación técnica documentada.
4. Viabilizar y recomendar la asignación de recursos humanos, técnicos, financieros, tecnológicos y organizativos para las actividades de Seguridad de la Información, ciberseguridad y protección de datos personales del ejercicio fiscal correspondiente.
5. Aprobar o recomendar la aprobación de políticas, lineamientos, procedimientos, metodologías, instructivos, planes, formatos y demás instrumentos internos necesarios para la Seguridad de la Información y protección de datos personales.
6. Supervisar el comportamiento de los riesgos que afecten a los activos de información, los sistemas institucionales, la continuidad operativa, los datos

personales y los derechos de los titulares.

7. Conocer y supervisar la investigación, el análisis, la documentación, el tratamiento y el cierre de incidentes de Seguridad de la Información y vulneraciones de seguridad de datos personales, en coordinación con las unidades competentes.
8. Emitir lineamientos para la implementación de controles de Seguridad de la Información y protección de datos personales, incluyendo medidas de confidencialidad, integridad, disponibilidad, trazabilidad, minimización, seudonimización, anonimización, cifrado, control de accesos, respaldo, recuperación y continuidad.
9. Promover la cultura institucional de Seguridad de la Información, ciberseguridad, confidencialidad, protección de datos personales y uso responsable de activos de información.
10. Establecer lineamientos y supervisar la gestión de continuidad operativa de servicios y sistemas de información críticos de EMASEO EP frente a incidentes, contingencias o interrupciones.
11. Garantizar que, para los titulares de datos personales, sea claro que EMASEO EP recoge y trata sus datos, evitando medios o fines ilícitos, desleales, desproporcionados o incompatibles con la finalidad informada.
12. Velar porque los datos personales no sean tratados para fines distintos de aquellos para los cuales fueron recopilados, salvo que concurra una base de legitimación aplicable.
13. Promover la integración de protección de datos personales desde el diseño y por defecto en nuevos proyectos, sistemas, trámites, contratos, formularios, aplicaciones, procesos operativos y bases de datos institucionales.
14. Conocer, aprobar o requerir ajustes sobre metodologías de análisis de riesgos a los derechos y libertades de los titulares, evaluaciones de impacto en protección de datos personales (EIPD) y evaluaciones de medidas de seguridad.
15. Supervisar que el Registro de Actividades de Tratamiento (RAT), los inventarios de activos de información, matrices de riesgos, las evaluaciones de impacto y demás instrumentos de cumplimiento se mantengan actualizados.
16. Establecer procedimientos y canales para la atención de derechos de acceso, rectificación, actualización, eliminación, oposición, portabilidad y demás derechos reconocidos por la normativa de protección de datos personales.
17. Asegurar que las vulneraciones de seguridad que involucren datos personales sean evaluadas y notificadas, cuando corresponda, a la Autoridad de Protección de Datos Personales y a los titulares, conforme a la normativa vigente.
18. Garantizar la participación oportuna del Oficial de Seguridad de la Información y del Delegado de Protección de Datos Personales en las materias relacionadas con sus competencias.
19. Emitir lineamientos para la incorporación de cláusulas de confidencialidad, no divulgación, Seguridad de la Información y protección de datos personales en contratos, convenios, acuerdos, términos de referencia y demás instrumentos institucionales y solicitar a las áreas competentes informes de cumplimiento.
20. Requerir informes periódicos al Oficial de Seguridad de la Información, al Líder

Resolución Nro. EMASEO-GGE-2026-0010-R

Quito, D.M., 31 de julio de 2026

Implementador de Protección de Datos Personales, al Equipo Implementador, a los puntos focales o a cualquier unidad administrativa sobre avances, alertas, incumplimientos, riesgos y medidas correctivas.

Artículo 11.- Responsabilidades del Oficial de Seguridad de la Información. El Oficial de Seguridad de la Información será responsable de la implementación, coordinación, seguimiento y mejora continua del EGSI en EMASEO EP, así como de coordinar las acciones del Comité relacionadas con la seguridad de la información.

Sin perjuicio de lo previsto en su acto de designación y en el EGSI, tendrá las siguientes responsabilidades:

1. Identificar y mantener actualizadas la estructura organizacional, los procesos, los activos de información, los sistemas críticos y las partes interesadas que impacten la implementación del EGSI.
2. Elaborar, actualizar y coordinar la documentación esencial del EGSI, incluyendo políticas, procedimientos, matrices, inventarios, controles, planes de tratamiento de riesgos, Declaración de Aplicabilidad (SoA), planes de concienciación, continuidad, respuesta a incidentes y mejora continua.
3. Coordinar la gestión de riesgos de Seguridad de la Información con las unidades administrativas y operativas de EMASEO EP.
4. Coordinar la gestión de incidentes de Seguridad de la Información, incluyendo su clasificación, análisis, tratamiento, escalamiento, documentación y cierre.
5. Informar al Comité sobre avances, alertas, necesidades, brechas, incumplimientos y recomendaciones vinculadas con el EGSI.
6. Actuar como punto de contacto institucional ante el ente rector en materia de Seguridad de la Información, en los términos previstos en la normativa aplicable.
7. Mantener organizada, consolidada y custodiada la documentación técnica generada durante la implementación, el seguimiento y la mejora continua del EGSI, sin perjuicio de las competencias de la Secretaría General o Gestión Documental.
8. Coordinar la entrega-recepción de la documentación y conocimiento institucional en caso de cambio, ausencia definitiva o terminación de funciones.
9. Informar a la Gerencia General, con la periodicidad que se defina en el plan de trabajo, sobre los avances, riesgos, brechas, incidentes, necesidades presupuestarias, hallazgos y recomendaciones en materia de Seguridad de la Información

Artículo 12.- Designación y rol del Delegado de Protección de Datos Personales. EMASEO EP designará y registrará ante la Autoridad de Protección de Datos Personales al Delegado de Protección de Datos Personales, conforme a la Ley Orgánica de Protección de Datos Personales, su Reglamento General y la normativa secundaria aplicable. El Delegado asesorará, velará y supervisará, de manera independiente, el cumplimiento de las obligaciones legales imputables a EMASEO EP como responsable del tratamiento y, cuando corresponda, a sus encargados del tratamiento.

Resolución Nro. EMASEO-GGE-2026-0010-R

Quito, D.M., 31 de julio de 2026

Artículo 13.- Funciones del Delegado de Protección de Datos Personales ante el Comité. Sin perjuicio de las funciones previstas en la normativa aplicable, el Delegado de Protección de Datos Personales podrá:

1. Asesorar al Comité sobre la Ley Orgánica de Protección de Datos Personales, su Reglamento General, así como las directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales.
2. Advertir riesgos, brechas, incumplimientos o conflictos de interés vinculados con el tratamiento de datos personales.
3. Emitir observaciones y recomendaciones sobre análisis de riesgos, evaluaciones de impacto, medidas de seguridad, canales para el ejercicio de derechos, cláusulas contractuales y notificaciones de vulneraciones de seguridad.
4. Informar periódicamente al Comité sobre el nivel de cumplimiento institucional en materia de protección de datos personales.
5. Cooperar con la Autoridad de Protección de Datos Personales y actuar como punto de contacto institucional, en los términos establecidos por la normativa aplicable.
6. Abstenerse de votar, ejecutar, aprobar operativamente o asumir la responsabilidad de la implementación respecto de decisiones que le corresponde supervisar.

Artículo 14.- Gestión operativa de Protección de Datos Personales. La gestión operativa de protección de datos personales estará a cargo del Líder Implementador, o del Líder de las unidades designadas, según corresponda. El Comité podrá aprobar lineamientos, requerir informes y coordinar acciones; el Delegado de Protección de Datos Personales mantendrá su rol de asesoría y supervisión independiente.

Artículo 15.- Presidencia del Comité. La Coordinación General de Planificación y Gestión Estratégica presidirá el Comité y será responsable de:

1. Aprobar el orden del día propuesto para cada sesión.
2. Convocar, instalar, presidir, suspender, diferir o clausurar las sesiones ordinarias y extraordinarias del Comité.
3. Solicitar a la Secretaría del Comité la constatación de quórum y la toma de votación de los miembros con derecho a voto.
4. Actuar con voto dirimente cuando exista empate entre los miembros con derecho a voto, siempre que el empate sea jurídicamente posible según el número de votantes presentes.
5. Cumplir y hacer cumplir los acuerdos, decisiones y resoluciones aprobadas por el Comité.
6. Requerir a los Líderes de las unidades responsables el avance de cumplimiento de los compromisos adoptados por el Comité.
7. Autorizar la participación de servidores, trabajadores o invitados institucionales que deban intervenir sobre puntos específicos del orden del día.

Resolución Nro. EMASEO-GGE-2026-0010-R

Quito, D.M., 31 de julio de 2026

8. Suscribir las actas del Comité juntamente con el/la Secretario/a del Comité y los miembros asistentes que correspondan.
9. Disponer la notificación de acuerdos, decisiones, recomendaciones y resoluciones a las unidades competentes.

Artículo 16.- Secretaría del Comité. El Subdirector de Calidad y Procesos actuará como Secretario/a del Comité, quien realizará lo siguiente:

1. Recibir propuestas de puntos para el orden del día y ponerlas en consideración de la Presidencia del Comité.
2. Elaborar las convocatorias autorizadas por la Presidencia, incluyendo la fecha, hora, modalidad, lugar o enlace de conexión, orden del día y documentación de respaldo.
3. Consolidar la información remitida por las unidades administrativas, técnicas u operativas para conocimiento del Comité.
4. Constatar el quórum de instalación y mantener el registro de asistentes.
5. Dar lectura al orden del día y al acta aprobada de la sesión anterior, cuando corresponda.
6. Mantener el registro multimedia o documental de las sesiones y elaborar las actas respectivas.
7. Mantener y custodiar el expediente del Comité, que contendrá las convocatorias, los órdenes del día, las actas, las listas de asistencia, los informes, las presentaciones, las votaciones, las resoluciones, las grabaciones y demás documentos de soporte.
8. Conceder copias certificadas o simples de la documentación que repose en el expediente, previa autorización de la Presidencia y conforme a la normativa sobre gestión documental, transparencia, confidencialidad, reserva y protección de datos personales.
9. Supervisar el seguimiento administrativo de las decisiones adoptadas por el Comité y reportar alertas de incumplimiento.

SECCIÓN III

FUNCIONAMIENTO DEL COMITÉ

Artículo 17.- Convocatorias. La Secretaría del Comité, previa autorización de la Presidencia, enviará la convocatoria a sesiones ordinarias o extraordinarias mediante el sistema de gestión documental, correo institucional u otro medio que deje constancia, señalando la fecha, hora, modalidad, lugar o enlace de conexión y orden del día. La convocatoria deberá acompañar los informes, estudios, matrices, presentaciones y demás documentos de respaldo necesarios para que los miembros adopten decisiones informadas.

Artículo 18.- Documentación previa. La falta total o parcial de documentación esencial

para el tratamiento de un punto del orden del día permitirá que el Comité difiera su conocimiento hasta contar con la información suficiente. La Presidencia podrá mantener el tratamiento del punto únicamente cuando exista urgencia institucional debidamente motivada y siempre que la decisión no afecte derechos de titulares ni comprometa la Seguridad de la Información sin soporte técnico mínimo.

Artículo 19.- Sesiones. El Comité podrá sesionar de manera presencial, virtual, híbrida o por correo electrónico institucional. En todos los casos deberá garantizarse la identificación de participantes, registro de asistencia, conservación de evidencia, disponibilidad de documentos de soporte y archivo de las actuaciones en el expediente correspondiente.

Artículo 20.- Sesiones ordinarias. El Comité sesionará ordinariamente conforme al calendario aprobado en la primera sesión de cada ejercicio fiscal o en la sesión de instalación. La convocatoria a sesiones ordinarias deberá realizarse con al menos tres (3) días hábiles de anticipación.

Artículo 21.- Sesiones extraordinarias. El Comité podrá sesionar extraordinariamente por disposición de la Presidencia o a pedido de uno de sus miembros con derecho a voto, operará la autoconvocatoria en cualquier momento y lugar, siempre que se encuentren presentes la totalidad de los miembros que conforman el Comité.

Artículo 22.- Invitados. Los servidores, trabajadores, consultores, asesores, responsables de procesos o terceros autorizados que participen en calidad de invitados lo harán únicamente respecto del punto para el cual fueron convocados, con voz, pero sin voto. Su participación podrá estar sujeta a obligaciones de confidencialidad, reserva y protección de datos personales.

Artículo 23.- Quórum de instalación. El quórum se conformará con la asistencia de la mitad más uno de los miembros con derecho a voz y voto. Para la instalación será necesaria la presencia de la Presidencia o su delegado/a. El Delegado de Protección de Datos Personales, el Secretario/a del Comité y los invitados no serán considerados para el cálculo del quórum de instalación, cuando actúen con voz, pero sin voto.

Artículo 24.- Votación y adopción de decisiones. Las decisiones, acuerdos y resoluciones del Comité se adoptarán por mayoría simple de los miembros presentes con derecho a voto. El voto será afirmativo o negativo y deberá constar en el acta. En caso de empate, siempre que este sea jurídicamente posible por la composición de los miembros votantes presentes, la Presidencia o su delegado/a tendrá voto dirimente.

Artículo 25.- Desarrollo de la sesión. Las sesiones del Comité se desarrollarán, al menos, conforme al siguiente orden, dependiendo de la modalidad de la sesión:

Resolución Nro. EMASEO-GGE-2026-0010-R

Quito, D.M., 31 de julio de 2026

1. Constatación del quórum por parte de la Secretaría del Comité.
2. Instalación de la sesión por parte de la Presidencia.
3. Conocimiento y aprobación del orden del día.
4. Conocimiento y aprobación del acta anterior, cuando corresponda.
5. Exposición, deliberación y tratamiento de los puntos aprobados.
6. Presentación de recomendaciones u observaciones del Delegado de Protección de Datos Personales, cuando la materia verse sobre datos personales o derechos de titulares.
7. Formulación de mociones, acuerdos, recomendaciones o resoluciones.
8. Votación por los miembros con derecho a voto.
9. Lectura de compromisos, responsables y plazos.
10. Clausura de la sesión.

Artículo 26.- Registro de sesiones. Toda sesión será registrada mediante actas. Las actas y documentos de respaldo permanecerán bajo custodia de la Secretaría del Comité conforme al régimen de archivo, confidencialidad, transparencia y protección de datos personales aplicable.

Artículo 27.- Actas. El desarrollo y decisiones de cada sesión se registrarán en un acta, que contendrá:

- Número de acta, lugar, fecha, hora de inicio y cierre de la sesión.
- Tipo de sesión y modalidad de realización.
- Nombres completos, cargos y calidad de participación de los asistentes.
- Constancia de quórum.
- Orden del día aprobado.
- Resumen de los puntos tratados, intervenciones, recomendaciones y observaciones relevantes.
- Pronunciamientos del Delegado de Protección de Datos Personales, cuando correspondan.
- Votación adoptada por los miembros con derecho a voto.
- Decisiones, acuerdos, resoluciones, responsables y plazos.
- Constancia de votos particulares o motivaciones de voto, si las hubiere.
- Firmas de la Presidencia, Secretaría del Comité y miembros que correspondan.

La propuesta de acta será enviada por la Secretaría del Comité, a los miembros dentro de los cinco (5) días hábiles posteriores a la sesión. Los miembros tendrán tres (3) días hábiles para remitir observaciones. Si no se recibieren observaciones dentro de dicho plazo, el acta se entenderá aprobada para fines de suscripción, salvo disposición expresa en contrario adoptada por el Comité.

Artículo 28.- Resoluciones y seguimiento. Las resoluciones del Comité serán

obligatorias para las unidades de EMASEO EP, dentro del ámbito de sus competencias internas, y serán de aplicación desde su aprobación del Comité. La Secretaría del Comité llevará el registro en una matriz de cumplimiento de acuerdos, responsables, plazos, evidencias y estado de cumplimiento, que será conocida periódicamente por el Comité.

Artículo 29.- Confidencialidad y reserva. Los miembros del Comité, el Delegado de Protección de Datos Personales, el/la Secretario/a del Comité, los invitados y los servidores que accedan a información tratada por el Comité deberán guardar confidencialidad respecto de información reservada, confidencial, sensible, estratégica, técnica, operativa, contractual, de seguridad o que contenga datos personales. Esta obligación subsistirá aun después de cesar en sus funciones o participación.

Artículo 30.- Gestión de conflictos de interés. Los miembros del Comité deberán informar oportunamente cualquier conflicto de interés real, potencial o aparente que pudiera afectar su imparcialidad en la deliberación o votación de un asunto. El Comité dejará constancia en acta y resolverá la forma de tratar el punto correspondiente, garantizando transparencia, juridicidad y protección de los intereses institucionales y derechos de los titulares.

Artículo 31.- Canal institucional de protección de datos personales. EMASEO EP creará y mantendrá un correo electrónico institucional específico para la recepción de solicitudes, consultas, comunicaciones y requerimientos vinculados con la protección de datos personales. Para el efecto, se dispone la creación del correo datospersonales@emaseo.gob.ec, o del que técnicamente defina la Subdirección de Gestión de TICs, garantizando trazabilidad, seguridad, acceso controlado, archivo, continuidad y atención oportuna.

Artículo 32.- Relación con otros órganos, equipos o responsables. El Comité coordinará sus actuaciones con la Gerencia General, el Oficial de Seguridad de la Información, el Delegado de Protección de Datos Personales y los líderes de las unidades responsables. Las funciones del Comité no sustituyen las competencias legales, contractuales, administrativas, técnicas u operativas de cada dependencia.

DISPOSICIONES GENERALES

PRIMERA.- Normativa supletoria. En todo lo no previsto en el presente Reglamento, el Comité se sujetará al Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003, al EGSI v3.0 o el que se encuentre vigente al momento de la aplicación, al Código Orgánico Administrativo, a la Ley Orgánica de Protección de Datos Personales, a su Reglamento General, a la normativa secundaria emitida por la Superintendencia de Protección de Datos Personales y demás normativa aplicable.

Resolución Nro. EMASEO-GGE-2026-0010-R

Quito, D.M., 31 de julio de 2026

SEGUNDA.- No sustitución de responsabilidades. La creación y funcionamiento del Comité no exime ni sustituye las responsabilidades de las unidades administrativas, técnicas, operativas, financieras, jurídicas o de apoyo de EMASEO EP respecto de la Seguridad de la Información, gestión documental, protección de datos personales, administración de contratos, atención ciudadana, gestión de riesgos, continuidad operativa o cumplimiento normativo.

TERCERA.- Independencia del Delegado de Protección de Datos Personales. Ninguna disposición del presente Reglamento podrá interpretarse como subordinación técnica, jerárquica o funcional del Delegado de Protección de Datos Personales respecto del Comité, en el ejercicio de sus funciones legales de asesoría, supervisión, cooperación con la Autoridad de Protección de Datos Personales y como punto de contacto. El Comité deberá facilitar su participación oportuna y el acceso a información necesaria para el desempeño de sus funciones.

CUARTA.- Gestión documental. La Secretaría del Comité asegurará la conformación, codificación, conservación, archivo y disponibilidad del expediente físico o electrónico del Comité, observando las reglas de Seguridad de la Información, protección de datos personales, confidencialidad, reserva y gestión documental.

DISPOSICIONES TRANSITORIAS

PRIMERA.- Instalación del Comité. Dentro de los 10 días hábiles siguientes a la suscripción de la presente resolución, la Presidencia convocará a sesión de instalación del Comité, en la cual se aprobará el calendario inicial de sesiones, la matriz de seguimiento, el plan de trabajo inicial y los mecanismos de coordinación con el Oficial de Seguridad de la Información y el Delegado de Protección de Datos Personales, y demás instrumentos relacionados con la implementación del EGSI.

SEGUNDA.- Adecuación de instrumentos internos. El Comité conocerá y priorizará, en su plan inicial de trabajo, la revisión o emisión de políticas, procedimientos, matrices, instructivos y formatos necesarios para el cumplimiento del EGSI y de la normativa de protección de datos personales, incluyendo el procedimiento de incidentes, el procedimiento de atención de derechos de titulares, lineamientos de contratos y cláusulas de protección de datos personales, análisis de riesgos, evaluaciones de impacto y gestión de activos de información.

TERCERA.- Equipos focales. Para la revisión institucional de los productos correspondientes a las fases 4 y 5 del contrato civil de servicios profesionales para la implementación de la normativa de protección de datos personales en EMASEO EP, se

Resolución Nro. EMASEO-GGE-2026-0010-R

Quito, D.M., 31 de julio de 2026

conformará un equipo focal temporal integrado por los titulares o sus delegados de las siguientes dependencias:

- Coordinación General Administrativa Financiera;
- Coordinación General de Planificación y Gestión Estratégica;
- Coordinación General Técnica;
- Dirección Jurídica;
- Subdirección de Comunicación Social, Relaciones Públicas y Marketing;
- Delegado de Protección de Datos Personales, quien actuará como asesor en materia de protección de datos personales con los demás miembros.

En el término de dos (2) días, los titulares ratificarán su intervención o en su defecto delegarán por escrito a la persona que actuará en representación de cada área. Dicha delegación deberá ser informada de manera oportuna al Delegado de Protección de Datos Personales.

Cada dirección estará representada por su director o por un servidor formalmente delegado. En el caso de la Subdirección de Comunicación Social, Relaciones Públicas y Marketing, la Unidad de Control de Servicios Operacionales y la Unidad de Secretaría General, participará su respectivo titular, responsable o delegado.

La intervención del equipo focal se limitará exclusivamente a revisar, dentro del ámbito de competencia de cada dependencia, los siguientes entregables contractuales:

- **Fase 4 – Implementación operativa institucional:**

a) Propuestas de ratificación o rectificación de instrumentos jurídicos;
b) Registro actualizado de actividades de tratamiento; y,
c) Reporte institucional de cumplimiento.

- **Fase 5 – Comunicación institucional, publicación y resolución de implementación:**

a) Propuesta de canales de comunicación para la difusión;
b) Actualización de la intranet y de la página web institucional;
c) Proyecto de resolución administrativa de implementación; y,
d) Informe final de implementación.

Los integrantes revisarán los productos que guarden relación con las atribuciones, procesos y actividades de tratamiento de datos personales de su dependencia y remitirán al administrador del contrato sus observaciones, recomendaciones o conformidad dentro del término que este determine. Las observaciones deberán estar debidamente motivadas y circunscribirse al contenido del entregable sometido a revisión.

Resolución Nro. EMASEO-GGE-2026-0010-R

Quito, D.M., 31 de julio de 2026

La participación del equipo focal no comprenderá la elaboración de los productos contractuales, la ejecución de obligaciones propias del contratista ni la administración del contrato. Tampoco implicará, por sí sola, la recepción o aceptación contractual de los entregables, atribuciones que corresponderán al administrador del contrato conforme al instrumento contractual y a la normativa aplicable.

El equipo focal concluirá sus funciones una vez finalizadas las revisiones de los entregables correspondientes a las fases 4 y 5 y formalizada la recepción del informe final de implementación.

DISPOSICIONES FINALES

PRIMERA.- Ejecución. Encárguese la ejecución de la presente resolución a los miembros del Comité representados por el Presidente y el Oficial de Seguridad de la Información.

SEGUNDA.- Notificación y socialización. Encárguese a Secretaría General o a la unidad competente de gestión documental la notificación de la presente resolución a todas las unidades de EMASEO EP. Encárguese a la unidad de Comunicación Social o quien haga sus veces su socialización interna y publicación en los medios institucionales que correspondan.

TERCERA.- Vigencia. La presente resolución entrará en vigencia a partir de su suscripción, sin perjuicio de su socialización, publicación interna o registro administrativo correspondiente.

Dada en la ciudad de Quito, Distrito Metropolitano,

Firmado electrónicamente por:
JUAN PABLO POZO CEVALLOS

Econ. Juan Pablo Pozo Cevallos
Gerente General
EMPRESA PÚBLICA METROPOLITANA DE ASEO

Referencias:
- EMASEO-SGT-2026-0310-M

Copia:
Señor Doctor
Rodrigo Javier Jimenez Roman
Lider de Secretaria General

Resolución Nro. EMASEO-GGE-2026-0010-R

Quito, D.M., 31 de julio de 2026

EMPRESA PÚBLICA METROPOLITANA DE ASEO - UNIDAD DE SECRETARIA GENERAL
EMPRESA PÚBLICA METROPOLITANA DE ASEO

Señor Doctor
Werner Wenceslao Altamirano Salazar
Líder de Normativa y Asesoría Jurídica
EMPRESA PÚBLICA METROPOLITANA DE ASEO - UNIDAD DE NORMATIVA Y ASESORÍA JURÍDICA
EMPRESA PÚBLICA METROPOLITANA DE ASEO

NUT: GADDMQ-2026-9017

Acción	Siglas Unidad	Fecha
Elaborado por: Werner Wenceslao Altamirano Salazar	EMASEO-UNA	2026-07-27
Revisado por: Ariel Jerusalen Mediavilla Valenzuela	EMASEO-UNA	2026-07-31
Revisado por: Romel Miguel Rosales Orellana	EMASEO-DJA	2026-07-31