REPÚBLICA DEL ECUADOR

Resolución Nro. SIS-SIS-2026-0012-R

Quito, 04 de abril de 2026

SERVICIO INTEGRADO DE SEGURIDAD ECU 911

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

Mgs. Juan Carlos Paladines Salcedo
DIRECTOR GENERAL

C O N S I D E R A N D OS:

Que, el artículo 66 en los numerales 19 y 21 de la Constitución de la República del Ecuador: Reconoce y garantiza a las personas: *"(…) 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos personales requerirán la autorización del titular o el mandato de ley." 21. El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación";*

Que, el artículo 82 de la Constitución de la República del Ecuador, establece que: *"El derecho a la seguridad jurídica se fundamenta 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, establece que: *"Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los 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. Asimismo, tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. (…)"*;

Que, el artículo 226 de la Constitución de la República del Ecuador, establece que: *"Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución*";

Que, el artículo 227 de la Constitución de la República del Ecuador textualmente, reconoce que: *"La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación.";*

Que, el primer inciso del artículo 233 de la Constitución de la República del Ecuador, establece que: *"Ninguna servidora ni servidor público estará exento de responsabilidades por los actos realizados en el ejercicio de sus funciones o por omisiones, y serán responsable administrativa, civil y penalmente por el manejo y administración de fondos, bienes o recursos públicos";*

Resolución Nro. SIS-SIS-2026-0012-R

Quito, 04 de abril de 2026

Que, la Ley Orgánica de Protección de Datos Personales (LOPDP), publicada en el Registro Oficial Suplemento Nro. 459 de 26 de mayo de 2021, establece el marco jurídico aplicable al tratamiento de datos personales, definiendo los principios, derechos de los titulares, así como las obligaciones de los responsables y encargados del tratamiento;

Que, el artículo 2 de la LOPDP, menciona: *"Ámbito de aplicación material.- La presente Ley se aplicará al tratamiento de datos personales contenidos en cualquier tipo de soporte, automatizados o no, así como a toda modalidad de uso posterior. La ley no será aplicable a: a) Personas naturales que utilicen estos datos en la realización de actividades familiares o domésticas; b) Personas fallecidas, sin perjuicio de lo establecido en el artículo 28 de la presente Ley; c) Datos anonimizados, en tanto no sea posible identificar a su titular. Tan pronto los datos dejen de estar disociados o de ser anónimos, su tratamiento estará sujeto al cumplimiento de las obligaciones de esta Ley, especialmente la de contar con una base de licitud para continuar tratando los datos de manera no anonimizada o disociada; d) Actividades periodísticas y otros contenidos editoriales; e) Datos personales cuyo tratamiento se encuentre regulado en normativa especializada de igual o mayor jerarquía en materia de gestión de riesgos por desastres naturales; y, seguridad y defensa del Estado, en cualquiera de estos casos deberá darse cumplimiento a los estándares internacionales en la materia de derechos humanos y a los principios de esta Ley, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad; f) Datos o bases de datos establecidos para la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, llevado a cabo por los organismos estatales competentes en cumplimiento de sus funciones legales. En cualquiera de estos casos deberá darse cumplimiento a los estándares internacionales en la materia de derechos humanos y a los principios de esta Ley, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad; y, g) Datos que identifican o hacen identificable a personas jurídicas. Son accesibles al público y susceptibles de tratamiento los datos personales referentes al contacto de profesionales y los datos de comerciantes, representantes y socios y accionistas de personas jurídicas y servidores públicos, siempre y cuando se refieran al ejercicio de su profesión, oficio, giro de negocio, competencias, facultades, atribuciones o cargo y se trate de nombres y apellidos, funciones o puestos desempeñados, dirección postal o electrónica, y, número de teléfono profesional. En el caso de los servidores públicos, además serán de acceso público y susceptibles de tratamiento de datos, el histórico y vigente de la declaración patrimonial y de su remuneración.";*

Que, el artículo 35 de la LOPDP, establece: *"Acceso a datos personales por parte de terceros.- No se considerará transferencia o comunicación cuando el acceso a datos personales por un tercero sea necesario para la prestación de un servicio al responsable del tratamiento de datos personales. El tercero que ha accedido a datos personales en estas condiciones debió hacerlo legítimamente. El tratamiento de datos personales realizado por terceros deberá estar regulado por un contrato, en el que se establezca de manera clara y precisa que el encargado del tratamiento de datos personales tratará únicamente los mismos conforme las instrucciones del responsable y que no los utilizará para finalidades diferentes a las señaladas en el contrato, ni que los transferirá o comunicará ni siquiera para su conservación a otras personas. Una vez que se haya cumplido la prestación contractual, los datos personales deberán ser destruidos o devueltos al responsable del tratamiento de datos personales bajo la supervisión de la autoridad de protección de datos personales. El tercero será responsable de las infracciones derivadas del incumplimiento de las condiciones de tratamiento de datos personales establecidas en la presente ley";*

Que, el artículo 37 de la LOPDP, determina: *"Seguridad de datos personales.- El responsable o encargado del tratamiento de datos personales según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la*

probabilidad de riesgos. El responsable o encargado del tratamiento de datos personales, deberá implementar un proceso de verificación, evaluación y valoración continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole, implementadas con el objeto de garantizar y mejorar la seguridad del tratamiento de datos personales. El responsable o encargado del tratamiento de datos personales deberá evidenciar que las medidas adoptadas e implementadas mitiguen de forma adecuada los riesgos identificados. Entre otras medidas, se podrán incluir las siguientes; 1) Medidas de anonimización, seudonomización o cifrado de datos personales; 2) Medidas dirigidas a mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios del tratamiento de datos personales y el acceso a los datos personales, de forma rápida en caso de incidentes; y 3) Medidas dirigidas a mejorar la residencia técnica, física, administrativa, y jurídica. 4) Los responsables y encargados del tratamiento de datos personales, podrán acogerse a estándares internacionales para una adecuada gestión de riesgos enfocada a la protección de derechos y libertades, así como para la implementación y manejo de sistemas de seguridad de la información o a códigos de conducta reconocidos y autorizados por la Autoridad de Protección de Datos Personales";

Que, el artículo 38 de la LOPDP, prevé: *"Medidas de seguridad en el ámbito del sector público.- El mecanismo gubernamental de seguridad de la información deberá incluir las medidas que deban implementarse en el caso de tratamiento de datos personales para hacer frente a cualquier riesgo, amenaza, vulnerabilidad, accesos no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita en el tratamiento de los datos conforme al principio de seguridad de datos personales. El mecanismo gubernamental de seguridad de la información abarcará y aplicará a todas las instituciones del sector público, contenidas en el artículo 225 de la Constitución de la República del Ecuador, así como a terceros que presten servicios públicos mediante concesión, u otras figuras legalmente reconocidas. Estas, podrán incorporar medidas adicionales al mecanismo gubernamental de seguridad de la información"*;

Que, el artículo 39 de la LOPDP determina: *"Protección de datos personales desde el diseño y por defecto.- Se entiende a la protección de datos desde el diseño como el deber del responsable del tratamiento de tener en cuenta, en las primeras fases de concepción y diseño del proyecto, que determinados tipos de tratamientos de datos personales entrañan una serie de riesgos para los derechos de los titulares en atención al estado de la técnica, naturaleza y fines del tratamiento, para lo cual, implementará las medidas técnicas, organizativas y de cualquier otra Índole, con miras a garantizar el cumplimiento de las obligaciones en materia de protección de datos, en los términos del reglamento. La protección de datos por defecto hace referencia a que el responsable debe aplicar las medidas técnicas y organizativas adecuadas con miras a que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines del tratamiento, en los términos del reglamento";*

Que, el artículo 78 de la Ley referida indica lo siguiente: *"Seguridad de los Datos Personales.- Las y los prestadores de servicios de telecomunicaciones deberán adoptar las medidas técnicas, organizativas y de cualquier otra índole adecuadas para preservar la seguridad de su red con el fin de garantizar la protección de los datos personales de conformidad con lo establecido en la Ley Orgánica de Protección de Datos Personales"*;

Que, la Protección de Datos Personales constituye un derecho fundamental vinculado a la dignidad humana, la autodeterminación informativa y el libre desarrollo de la personalidad, debiendo garantizarse su respeto en todo tratamiento de datos personales;

Que, la Ley Orgánica de Protección de Datos Personales establece principios rectores como licitud, lealtad, transparencia, finalidad, minimización, proporcionalidad y responsabilidad proactiva, los cuales

deben observarse en todo tratamiento de datos personales;

Que, el Reglamento General a la LOPDP, expedido mediante Decreto Ejecutivo Nro. 904 de 13 de noviembre de 2023, y publicado en el Registro Oficial Suplemento Nro. 435 (Tercer Suplemento), desarrolla las disposiciones necesarias para la aplicación de la referida Ley, precisando los mecanismos de cumplimiento, control y ejercicio de derechos;

Que, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicada en el Registro Oficial Nro. 557 de 17 de abril de 2002, regula el tratamiento de información en entornos digitales, así como el uso de medios electrónicos, siendo aplicable a las actividades de tratamiento de datos personales realizadas mediante plataformas tecnológicas y servicios digitales;

Que, el artículo 146 del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, establece lo siguiente: *"Clasificación de datos.- Cuando las entidades del sector público contraten servicios tecnológicos a terceros, deberán hacerlo con proveedores que garanticen que los datos se encuentren en centros de cómputo que cumplan con estándares internacionales de seguridad y protección. Además, los datos deberán ser clasificados tomando en cuenta su criticidad y valor de la siguiente manera: Reservado: Datos que la divulgación no autorizada podría causar daños o lesiones graves, incluida la muerte de las personas identificadas en la información, o menoscabar significativamente la capacidad del gobierno para desempeñar sus competencias legales. Confidencial: Datos protegidos contra la divulgación y que sean altamente sensibles o estén legal, reglamentaria o contractualmente restringidas de su divulgación a otros organismos públicos. Abierto: Datos no restringidos fácilmente disponibles para el público en sitios web y conjuntos de datos públicos abiertos. La información o los datos específicamente clasificados como reservados y confidenciales por motivos de seguridad nacional y pertenecientes al estado ecuatoriano deberán estar alojados en centros de datos o plataformas informáticas ubicados en territorio ecuatoriano";*

Que, mediante Decreto Ejecutivo Nro. 214 de 28 de marzo de 2024, publicado en el Segundo Suplemento del Registro Oficial Nro. 529 de 01 de abril de 2024, se reformó el Decreto Ejecutivo Nro. 988 de 29 de diciembre de 2011, al señalar que: *"El Servicio Integrado de Seguridad ECU 911 es el organismo público encargado de regular, coordinar, controlar y prestar el servicio de emergencias, video vigilancia y otras actividades, de acuerdo con políticas, normativa y procesos establecidos. Para esto, podrá contar con la colaboración e información proporcionada por entidades públicas, personas naturales y jurídicas, con el fin de brindar respuestas eficaces y eficientes a las solicitudes de la ciudadanía. El servicio incluye la recepción de llamadas, visualización por video vigilancia, monitoreo de alarmas y alertas; así como, la coordinación de la disposición de recursos para respuesta en atención de emergencias, en materias de salud, seguridad ciudadana, orden público, gestión de tránsito y movilidad, gestión sanitaria, gestión de riesgos, gestión de servicios municipales y otros que fueran necesarios. Este organismo ejerce las facultades de administración y cuenta con personalidad jurídica propia, se encuentra dotado de autonomía administrativa, operativa y financiera (…)"*;

Que, el artículo 2 del Decreto Ejecutivo Nro. 214, dispone: *"Agréguese en el Decreto Ejecutivo No. 988 de 29 de diciembre de 2011, un artículo innumerado a continuación del Artículo 2 con el siguiente texto: "Artículo (…). Competencias.- El Servicio Integrado de Seguridad ECU 911 ejercerá las siguientes competencias: (…) e) Regular la interoperabilidad de los sistemas y plataformas tecnológicas públicas nacionales y locales; así como los sistemas y plataformas privadas que requieran interoperar con el Servicio Integrado de Seguridad ECU 911"*;

Que, mediante Resolución Nro. SIS-ECU-DIR-2025-005 de 19 de febrero de 2025, emitida por el Comité Intersectorial del Servicio Integrado de Seguridad ECU 911, se designó al Mgs. Juan Carlos Paladines Salcedo, en calidad de Director General del Servicio Integrado de Seguridad ECU 911,

Resolución Nro. SIS-SIS-2026-0012-R

Quito, 04 de abril de 2026

conforme lo sustenta la Acción de Personal Nro. PC-NJS-0008 de 19 de febrero de 2025, que rigió a partir del 20 de febrero de 2025;

En cumplimiento de los Decretos Ejecutivos 214 y 397 y en uso de las facultades y atribuciones que confiere el literal e) del numeral 1 del artículo 77 de la Ley Orgánica de la Contraloría General del Estado, artículo 11 del Estatuto Orgánico de Gestión Organizacional por Procesos del Servicio Integrado de Seguridad ECU 911 y demás ordenamiento jurídico invocado.

RESUELVE:
EMITIR LA POLÍTICA DE PROTECCIÓN DE DATOS DEL SERVICIO INTEGRADO DE SEGURIDAD ECU 911

CAPÍTULO I
PRIVACIDAD Y ÁMBITO DE APLICACIÓN

Artículo 1.- Ámbito de aplicación.

La presente Política de Protección de Datos Personales es de cumplimiento obligatorio para todas las autoridades, servidores públicos, trabajadores, contratistas, pasantes, practicantes, proveedores y cualquier persona natural o jurídica que, en virtud de una relación jurídica con el Servicio Integrado de Seguridad ECU 911, intervenga en el tratamiento de datos personales a nivel nacional.

En consecuencia, sus disposiciones serán aplicables a todo tratamiento de datos personales realizado en el ejercicio de las competencias institucionales, cualquiera que sea el soporte, medio o modalidad utilizada, ya sea mediante procesos automatizados, semiautomatizados o manuales.

Artículo 2.- Marco normativo aplicable.

La presente Política de Protección de Datos Personales se rige por:

- La Constitución de la República del Ecuador;
- La Ley Orgánica de Protección de Datos Personales (LOPDP);
- El Reglamento General a la Ley Orgánica de Protección de Datos Personales (RLOPDP);
- La Ley de Comercio Electrónico, Firmas y Mensajes de Datos;
- Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación;
- Las resoluciones y lineamientos emitidos por la Superintendencia de Protección de Datos Personales, y;
- Demás normativa aplicable en la materia;

Artículo 3.- Responsable del tratamiento.

El responsable del tratamiento de datos personales es el Servicio Integrado de Seguridad ECU 911, entidad de derecho público con personalidad jurídica propia, con domicilio en la ciudad de Quito.

Las autoridades, directivos y responsables de las distintas dependencias velarán por el cumplimiento de la presente Política.

El tratamiento por terceros estará regulado mediante instrumento jurídico conforme a la ley.

El personal actuará bajo la autoridad del responsable, observando confidencialidad y seguridad de la

información.

El Servicio Integrado de Seguridad ECU 911 garantizará la adopción de medidas necesarias para asegurar el cumplimiento de la normativa de protección de datos personales en todas sus actividades.

Artículo 4.- Objeto del tratamiento de datos personales.

El Servicio Integrado de Seguridad ECU 911 realiza el tratamiento de datos personales mediante su recolección, registro, organización, almacenamiento, consulta, uso, interconexión, transmisión o cualquier otra operación necesaria para el cumplimiento de sus competencias institucionales, en el marco de la prestación del servicio de atención de emergencias, coordinación operativa y gestión institucional.

El tratamiento podrá efectuarse a través de sistemas tecnológicos, aplicaciones, plataformas digitales, canales de atención y procesos institucionales.

El intercambio o comunicación de datos personales con entidades públicas o privadas se realizará cuando exista una base de legitimación válida y sea necesario para el cumplimiento de sus competencias.

Artículo 5.- Naturaleza de los datos tratados.

En el marco de sus competencias, el Servicio Integrado de Seguridad ECU 911 podrá tratar datos personales identificativos, de contacto, sociodemográficos, de localización y, cuando sea estrictamente necesario, datos sensibles.

La información tratada será clasificada conforme a la normativa vigente en materia de protección de datos personales, acceso a la información pública y seguridad de la información.

Artículo 6.- Deber de información al titular.

El Servicio Integrado de Seguridad ECU 911 garantizará que el titular sea informado de manera clara y transparente sobre el tratamiento de sus datos personales.

Este deber se cumplirá mediante avisos de privacidad u otros mecanismos adecuados según el canal de recolección de la información.

Artículo 7.- Conservación de los datos.

Los datos personales serán conservados únicamente durante el tiempo necesario para cumplir con las finalidades del tratamiento, conforme a lo establecido en la LOPDP, su Reglamento General a la Ley Orgánica de Protección de Datos Personales (RLOPDP) y la normativa de gestión documental aplicable. Cumplida la finalidad, los datos serán eliminados, anonimizados, bloqueados o conservados cuando exista una obligación legal o interés público que justifique su conservación.

CAPÍTULO II
PRINCIPIOS APLICABLES AL TRATAMIENTO DE DATOS PERSONALES

Artículo 8.- Principios aplicables al tratamiento de datos personales.

El tratamiento de datos personales se regirá por los principios establecidos en la Ley Orgánica de Protección de Datos Personales.

Resolución Nro. SIS-SIS-2026-0012-R

Quito, 04 de abril de 2026

CAPÍTULO III
DEFINICIONES

Artículo 9.- Definiciones

Para efectos de la presente Política, se adoptan las definiciones previstas en la normativa de protección de datos personales. Los términos de carácter operativo institucional se incluyen de manera referencial para la comprensión del funcionamiento del Servicio Integrado de Seguridad ECU 911, con el siguiente significado:

Alerta: Toda señal o aviso que ingrese al SIS ECU 911, por cualquiera de los mecanismos de información o advertencia sobre un incidente o emergencia que sucedió, que está ocurriendo o que va a suceder.

Alertante: Persona que alerta al SIS ECU 911 un incidente o emergencia que sucedió, que está ocurriendo o que va a suceder a través de los mecanismos de alerta.

Anonimización: Proceso mediante el cual los datos personales dejan de estar vinculados o no pueden asociarse a una persona natural identificada o identificable de manera irreversible.

Archivo o base de datos: Conjunto estructurado de datos personales accesible conforme a criterios determinados, cualquiera sea su forma o modalidad de creación, almacenamiento u organización.

Base de legitimación: Fundamento jurídico que habilita el tratamiento de datos personales, tales como el cumplimiento de una obligación legal, el ejercicio de potestades públicas, la ejecución de una misión realizada en interés público, el consentimiento del titular u otras previstas en la normativa vigente.

Confidencialidad: Deber de garantizar que los datos personales no sean divulgados ni accesibles a personas no autorizadas.

Consentimiento: Manifestación de voluntad libre, específica, informada e inequívoca mediante la cual el titular acepta el tratamiento de sus datos personales para una finalidad determinada.

Cookies: Archivos o dispositivos de almacenamiento y recuperación de datos que se descargan en el equipo terminal del usuario al acceder a plataformas digitales, utilizados para almacenar y recuperar información sobre la navegación.

Dato biométrico: Información obtenida a partir de un tratamiento técnico específico, relativa a características físicas, fisiológicas o conductuales de una persona natural que permitan o confirmen su identificación única.

Dato de salud: Información relativa al estado físico o mental de una persona natural, incluyendo antecedentes médicos, alergias, tipo de sangre, discapacidad u otra información vinculada a la atención de emergencias.

Dato personal: Toda información que identifica o hace identificable a una persona natural, directa o indirectamente.

Datos sensibles: Aquellos datos personales que afectan la esfera íntima del titular o cuyo uso indebido puede generar discriminación o riesgo grave.

Resolución Nro. SIS-SIS-2026-0012-R

Quito, 04 de abril de 2026

Delegado de Protección de Datos Personales (DPD): Figura encargada de asesorar, supervisar y verificar el cumplimiento de la normativa de protección de datos personales y actuar como punto de contacto con la autoridad y los titulares.

Disponibilidad: Garantía de que los datos personales sean accesibles y utilizables por personal autorizado cuando sea necesario para el cumplimiento de las finalidades del tratamiento.

Emergencia: Es el evento que pone en peligro la vida de las personas, los bienes o la continuidad de los servicios en una comunidad, y que requieren una respuesta de atención inmediata y eficaz.

Encargado del tratamiento: Persona natural o jurídica que trata datos personales por cuenta del responsable del tratamiento.

Entidad de respuesta: Institución pública o privada articulada al Servicio Integrado de Seguridad ECU 911 que interviene en la atención de emergencias, tales como Policía Nacional, Cuerpos de Bomberos, Ministerio de Salud Pública, entre otros.

Evaluación de impacto en protección de datos (EIPD): Instrumento preventivo que permite identificar, analizar y mitigar riesgos asociados a tratamientos de datos personales que puedan afectar derechos y libertades.

Geolocalización: Tratamiento de datos que permite determinar, identificar o estimar la ubicación geográfica de una persona natural o de un dispositivo asociado a esta, en tiempo real o de manera histórica, mediante tecnologías como GPS, redes móviles, direcciones IP u otros medios, incluyendo herramientas institucionales como el Mobile Locator. Cuando permita identificar o hacer identificable a una persona natural, se considerará dato personal y en determinados contextos, dato sensible.

Incidente: Tipo de perturbación puntual y de impacto limitado, que no altera gravemente el funcionamiento de un sistema o comunidad. Los incidentes son atendidos por entidades y servicios especializados de respuesta y socorro.

Integridad: Garantía de que los datos personales sean exactos, completos y no hayan sido alterados de manera no autorizada.

Interoperabilidad: Capacidad de los sistemas institucionales para intercambiar datos personales con otras entidades, bajo condiciones de seguridad y legalidad.

Medidas de seguridad: Conjunto de acciones técnicas, organizativas, administrativas y jurídicas destinadas a proteger los datos personales.

Minimización de datos: Principio que implica tratar únicamente los datos personales adecuados, pertinentes y limitados a lo necesario para la finalidad del tratamiento.

Evaluador de Operaciones: Servidor o funcionario encargado de la recepción, gestión y despacho de emergencias a través de las plataformas del Servicio Integrado de Seguridad ECU 911.

Evento: Suceso importante que podría derivar en un incidente o emergencia, programado o no, de índole social, académica, artística o deportiva.

Principio de proporcionalidad: Exigencia de que el tratamiento de datos personales sea idóneo, necesario y equilibrado en relación con la finalidad perseguida.

Responsabilidad proactiva: Principio que obliga al responsable del tratamiento a implementar medidas y mecanismos que permitan demostrar el cumplimiento de la normativa de protección de datos personales.

Riesgo: Probabilidad de que una amenaza se materialice y afecte la seguridad, confidencialidad, integridad o disponibilidad de los datos personales.

Seudonimización: Tratamiento de datos personales de manera que no puedan atribuirse a un titular sin información adicional, la cual debe mantenerse separada y protegida.

Sistema de confianza cero (Zero Trust): Modelo de seguridad que establece que ningún usuario o sistema es confiable por defecto, requiriendo verificación continua para el acceso a recursos.

Titular de los datos: Persona natural a quien corresponden los datos personales objeto de tratamiento.

Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales.

Transferencia o comunicación de datos: Revelación de datos personales a un tercero distinto del titular, responsable o encargado.

Trazabilidad: Capacidad de registrar y seguir las operaciones realizadas sobre los datos personales, permitiendo su control y auditoría.

Sistema de Videovigilancia: Conjunto de cámaras de videovigilancia que monitorean distintas zonas y que están conectadas a un sistema tecnológico, mismo que es capaz de almacenar imágenes y/o generar alertas en caso de detección de incidentes o emergencias.

Violación de seguridad de datos personales: Incidente que ocasiona la destrucción, pérdida, alteración, divulgación no autorizada o acceso indebido a datos personales.

CAPÍTULO IV
BASES DE LEGITIMACIÓN DEL TRATAMIENTO DE DATOS PERSONALES Y FINALIDADES

Artículo 10.- Bases de legitimación del tratamiento.

El tratamiento de datos personales en el Servicio Integrado de Seguridad ECU 911 se realizará sobre la base de las condiciones de licitud previstas en la Ley Orgánica de Protección de Datos Personales, tales como el cumplimiento de obligaciones legales, el ejercicio de potestades públicas, la protección de intereses vitales, el consentimiento del titular cuando corresponda y el interés legítimo debidamente justificado.

Artículo 11.- Tratamiento basado en interés legítimo.

El Servicio Integrado de Seguridad ECU 911 podrá tratar datos personales con fundamento en el interés legítimo, siempre que dicho tratamiento sea necesario para el cumplimiento de sus competencias institucionales y no prevalezcan los derechos y libertades fundamentales de los titulares de los datos.

La aplicación de esta base de legitimación deberá responder a una finalidad legítima, ser necesaria y

proporcional para el cumplimiento de dicha finalidad, y considerar medidas adecuadas para la protección de los datos personales.

Cuando corresponda, la institución podrá realizar y documentar un análisis de ponderación que permita verificar la legitimidad del tratamiento, considerando la finalidad perseguida, la necesidad del tratamiento y el equilibrio entre el interés institucional y los derechos y libertades fundamentales de los titulares de los datos, de acuerdo con las disposiciones aplicables en materia de protección de datos personales.

Artículo 12.- Finalidades del tratamiento de datos personales.

Los datos personales tratados por el Servicio Integrado de Seguridad ECU 911 tendrán finalidades determinadas, explícitas y legítimas, en el marco de sus competencias constitucionales, legales y reglamentarias.

De manera enunciativa y no limitativa, las finalidades del tratamiento son:

Finalidades operativas (atención de emergencias)

- Recepción, gestión y despacho de emergencias, así como la coordinación con entidades de respuesta.
- Registro y conservación de comunicaciones, incidentes y eventos para fines operativos, trazabilidad y continuidad del servicio.
- Interoperabilidad e intercambio de información con entidades autorizadas para la atención de emergencias o cumplimiento de obligaciones legales.
- Uso de herramientas tecnológicas, incluida la geolocalización, cuando sea estrictamente necesario para la atención de emergencias y la protección de las personas.
- Colaboración con autoridades competentes mediante la entrega de información conforme a la normativa vigente.

Finalidades tecnológicas y digitales

- Gestión, administración y seguridad de plataformas, sistemas y aplicaciones tecnológicas institucionales.
- Administración de servicios digitales vinculados al funcionamiento institucional.

Finalidades administrativas y de gestión interna

- Gestión administrativa, operativa, tecnológica y de talento humano necesaria para el funcionamiento institucional.

Finalidades de evaluación y mejora institucional

- Evaluación, seguimiento y mejora continua de los servicios institucionales.

Finalidades de formación y vinculación con la ciudadanía

- Desarrollo de programas de capacitación, formación y vinculación relacionados con la gestión de emergencias.

Finalidades de control y cumplimiento

- Control del uso indebido del sistema de emergencias conforme a la normativa vigente.
- Atención de requerimientos ciudadanos, administrativos o judiciales.

Finalidades de seguridad mediante videovigilancia

- Gestión y monitoreo de sistemas de videovigilancia institucional para fines de seguridad, prevención y soporte a la gestión operativa institucional.

El tratamiento de datos personales se realizará para finalidades determinadas y compatibles con las previstas en la presente Política, conforme a la normativa vigente.

Artículo 13.- Tratamiento de datos sensibles.
El tratamiento de datos sensibles por parte del Servicio Integrado de Seguridad ECU 911 se realizará cuando resulte necesario para el cumplimiento de sus competencias institucionales, en particular en el contexto de la atención de emergencias, la gestión de sistemas de videovigilancia u otras operaciones que, por su naturaleza, impliquen el tratamiento de este tipo de datos, siempre que exista una base de legitimación prevista en la normativa vigente.

En todos los casos, la institución adoptará medidas técnicas y organizativas adecuadas y reforzadas para garantizar la seguridad, confidencialidad e integridad de los datos personales, así como la protección de los derechos de los titulares, conforme a los principios de necesidad, proporcionalidad y minimización de datos.

Artículo 14.- Tratamiento y protección de datos de personas pertenecientes a grupos de atención prioritaria.

El tratamiento de datos personales que involucre a personas pertenecientes a grupos de atención prioritaria se realizará con estricta observancia de la Constitución de la República del Ecuador y la normativa vigente en materia de protección de datos personales, garantizando la adopción de medidas reforzadas y adecuadas para la protección de sus derechos.

En estos casos, el tratamiento deberá regirse por criterios de especial diligencia, necesidad, proporcionalidad y minimización de datos, considerando su condición de vulnerabilidad.

Cuando corresponda y el titular no tenga capacidad legal para otorgar su consentimiento, este será otorgado por su representante legal, conforme a la normativa aplicable.

Artículo 15.-Tratamiento de datos personales en emergencias.

El tratamiento de datos personales en el contexto de la atención de emergencias se fundamentará principalmente en la protección de intereses vitales del titular o de terceros y en el ejercicio de las competencias institucionales del Servicio Integrado de Seguridad ECU 911.

Cuando resulte necesario para proteger la vida, la integridad personal o la seguridad pública, dicho tratamiento podrá realizarse sin requerir el consentimiento previo del titular, conforme a la normativa vigente.

Artículo 16.- Limitación de la finalidad.

Los datos personales tratados por el Servicio Integrado de Seguridad ECU 911 serán utilizados exclusivamente para las finalidades determinadas, explícitas y legítimas establecidas en la presente

Política, y no podrán ser tratados posteriormente de manera incompatible con dichas finalidades, salvo en los casos previstos en la normativa vigente.

CAPÍTULO V
CONSERVACIÓN DE DATOS

Artículo 17.- Conservación de los datos.

El Servicio Integrado de Seguridad ECU 911 establecerá y aplicará criterios, plazos y procedimientos internos para la conservación, revisión y supresión de los datos personales, en función de la naturaleza del tratamiento, las finalidades previstas y las obligaciones legales aplicables.

Los datos personales serán conservados únicamente durante el tiempo necesario para cumplir con dichas finalidades y deberán ser objeto de revisión periódica a fin de verificar la pertinencia de su conservación.

Cumplido el plazo de conservación, los datos personales serán eliminados, anonimizados o, cuando corresponda, bloqueados, conforme a los mecanismos definidos institucionalmente.

Cuando los datos personales formen parte de procesos administrativos, investigativos o judiciales en curso, o sean necesarios para la formulación, ejercicio o defensa de derechos, su conservación se mantendrá hasta la finalización del proceso respectivo, garantizando su integridad, disponibilidad y seguridad.

CAPÍTULO VI
DERECHOS DE LOS TITULARES

Artículo 18.- Derechos de los titulares.

El Servicio Integrado de Seguridad ECU 911 garantiza a los titulares de datos personales el ejercicio de los derechos reconocidos en la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos Personales y su Reglamento, de conformidad con la normativa vigente y sus limitaciones legales.

Artículo 19.- Ejercicio de derechos.

El titular podrá ejercer sus derechos de acceso, rectificación, eliminación, oposición, limitación del tratamiento, portabilidad y a no ser objeto de decisiones automatizadas, de forma gratuita y sin requisitos desproporcionados.

Las solicitudes deberán contener, al menos, la identificación del titular o su representante, la descripción del derecho que se desea ejercer, los datos sobre los cuales se solicita la acción y un medio para recibir notificaciones.

El Servicio Integrado de Seguridad ECU 911 dispondrá de mecanismos formales, accesibles y trazables para la recepción, gestión y respuesta de solicitudes, a través de sus canales institucionales, incluido el correo electrónico: proteccion.datos@ecu911.gob.ec.

El Delegado de Protección de Datos Personales será responsable de recibir, canalizar y dar seguimiento a las solicitudes, así como de asesorar, supervisar el cumplimiento de la normativa, coordinar con las áreas

institucionales y actuar como punto de contacto con la Autoridad de Protección de Datos Personales.

La institución mantendrá registros de solicitudes e incidentes de seguridad relacionados con datos personales y articulará las acciones necesarias con sus unidades internas y encargados del tratamiento para garantizar la protección de la información.

En caso de que la solicitud esté incompleta, se requerirá su aclaración de acuerdo con las disposiciones aplicables.

Artículo 20.- Plazos.

El Servicio Integrado de Seguridad ECU 911 atenderá las solicitudes relacionadas con el ejercicio de los derechos de los titulares de datos personales dentro de los plazos y conforme a los procedimientos establecidos en la Ley Orgánica de Protección de Datos Personales de Ecuador, su Reglamento General a la Ley Orgánica de Protección de Datos Personales y la normativa administrativa aplicable.

Artículo 21.- Limitaciones.

El ejercicio de los derechos de los titulares de datos personales podrá estar sujeto a las limitaciones previstas en la normativa vigente en materia de protección de datos personales.

Dichas limitaciones se aplicarán únicamente en los casos y condiciones establecidos en la ley y su normativa aplicable.

Artículo 22.- Vías de reclamación.

El titular podrá presentar solicitudes o reclamaciones ante el Servicio Integrado de Seguridad ECU 911 a través de los mecanismos institucionales habilitados, o acudir ante la Autoridad de Protección de Datos Personales, de acuerdo con las disposiciones aplicables, cuando considere vulnerados sus derechos.

CAPÍTULO VII
PROTECCIÓN DE DATOS DESDE EL DISEÑO

Artículo 23.- Protección de datos desde el diseño y por defecto.

El Servicio Integrado de Seguridad ECU 911 aplicará el principio de protección de datos personales desde el diseño y por defecto en los sistemas, procesos, servicios y proyectos que impliquen tratamiento de datos personales, de conformidad con la normativa vigente en materia de protección de datos personales.

Las medidas técnicas y organizativas relacionadas con este principio se adoptarán conforme a la normativa aplicable y a los lineamientos institucionales de seguridad de la información.

Artículo 24.- Evaluación de Impacto en Protección de Datos Personales (EIPD).

Cuando un tratamiento de datos personales pueda implicar un alto riesgo para los derechos y libertades de los titulares, el Servicio Integrado de Seguridad ECU 911 realizará una Evaluación de Impacto en Protección de Datos Personales, con carácter previo al tratamiento, de acuerdo con las disposiciones aplicables.

La evaluación permitirá identificar y mitigar los riesgos asociados y deberá mantenerse documentada como evidencia del cumplimiento del principio de responsabilidad proactiva.

CAPÍTULO VIII
SEGURIDAD DE LA INFORMACIÓN

Artículo 25.- Seguridad de la información.

El tratamiento de datos personales en el Servicio Integrado de Seguridad ECU 911 se realizará garantizando el cumplimiento de los principios de seguridad de la información, en particular la confidencialidad, integridad, disponibilidad y trazabilidad de los datos personales, conforme a la normativa vigente.

Artículo 26.- Medidas de seguridad de la información

El Servicio Integrado de Seguridad ECU 911 implementará medidas técnicas y organizativas adecuadas para garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales, considerando la naturaleza de los datos, el contexto del tratamiento y los riesgos asociados.

Estas medidas se adoptarán conforme a la Política de Seguridad de la Información institucional, al Esquema Gubernamental de Seguridad de la Información (EGSI) y a los lineamientos del área competente.

El acceso a los datos personales se limitará al personal autorizado, bajo criterios de necesidad de conocer y mínimo privilegio.

La institución promoverá procesos de capacitación y concienciación del personal.

La institución podrá adoptar estándares nacionales e internacionales de seguridad de la información como referencia para la protección de los datos personales.

CAPÍTULO IX
GESTIÓN DE INCIDENTES Y CONTROL DEL TRATAMIENTO

Artículo 27.- Gestión de incidentes de seguridad

La institución establecerá procedimientos para la identificación, registro, análisis, contención, mitigación y documentación de incidentes de seguridad que afecten datos personales.

Cuando un incidente represente un riesgo para los derechos y libertades de los titulares, se adoptarán las medidas necesarias para su mitigación y, cuando corresponda, se notificará a la Autoridad de Protección de Datos Personales y a los titulares afectados, de acuerdo con las disposiciones aplicables.

La institución mantendrá un registro de incidentes de seguridad como parte del principio de responsabilidad proactiva.

Artículo 28.- Registro de actividades.

El Servicio Integrado de Seguridad ECU 911 mantendrá un Registro de Actividades de Tratamiento de

datos personales, actualizado y disponible para la autoridad competente, de acuerdo con las disposiciones aplicables.

Artículo 29.- Gestión de riesgos

La institución gestionará los riesgos asociados al tratamiento de datos personales, con el fin de identificar, analizar y mitigar posibles afectaciones a los derechos y libertades de los titulares, conforme a la normativa aplicable.

Artículo 30.- Auditorías y seguimiento

El Servicio Integrado de Seguridad ECU 911 realizará acciones de seguimiento y auditorías periódicas para verificar el cumplimiento de la normativa en materia de protección de datos personales y de la presente Política.

Los resultados deberán documentarse y servirán para la implementación de acciones de mejora.

Artículo 31.- Tratamiento en entornos digitales

El tratamiento de datos personales en entornos digitales institucionales se realizará conforme a la presente Política y a la normativa vigente, en el ámbito de los sistemas y plataformas digitales institucionales, garantizando la aplicación de medidas de seguridad adecuadas, de carácter técnico y organizativo, así como la trazabilidad de las operaciones realizadas sobre los datos personales.

Artículo 32.- Transferencias internacionales de datos personales

La transferencia internacional de datos personales se realizará conforme a las condiciones y garantías establecidas en la normativa vigente, asegurando un nivel adecuado de protección de los derechos de los titulares.

Artículo 33.- Tratamiento de datos en contextos de emergencia

El tratamiento de datos personales en contextos de emergencia y operaciones críticas se realizará garantizando la aplicación de medidas adecuadas que permitan una respuesta oportuna y eficaz, sin perjuicio del respeto a los derechos de los titulares.

En estos casos, el Servicio Integrado de Seguridad ECU 911 adoptará medidas que aseguren la confidencialidad, integridad, disponibilidad y trazabilidad de la información, considerando la naturaleza urgente del tratamiento y los riesgos asociados.

Artículo 34.- Geolocalización

El tratamiento de datos de geolocalización se realizará cuando resulte necesario para la atención de emergencias, la coordinación operativa o la protección de personas, conforme a las finalidades previstas en la presente Política.

En estos casos, el Servicio Integrado de Seguridad ECU 911 garantizará que dicho tratamiento se realice de manera proporcional, limitado a lo estrictamente necesario y por el tiempo indispensable para el cumplimiento de dichas finalidades.

Cuando los datos de geolocalización permitan identificar o hacer identificable a una persona natural,

serán tratados como datos personales y estarán sujetos a medidas de seguridad reforzadas, considerando los riesgos asociados a su uso.

El tratamiento y eventual intercambio de estos datos con autoridades competentes se realizará conforme a la normativa vigente y en el marco de las competencias legalmente atribuidas.

Artículo 35.- Videovigilancia

Los sistemas de videovigilancia institucional y las llamadas a la línea de emergencias podrán ser grabados y tratados conforme a las finalidades previstas en la presente Política.

El tratamiento de estas grabaciones se realizará garantizando la aplicación de medidas de seguridad adecuadas, así como la confidencialidad, integridad, disponibilidad y trazabilidad de la información.

El acceso a dichas grabaciones estará restringido al personal autorizado y se limitará a los fines que motivaron su obtención, quedando prohibido su uso para finalidades distintas, salvo habilitación legal.

La conservación de las grabaciones se realizará por el tiempo estrictamente necesario, conforme a los criterios y plazos definidos institucionalmente y a la normativa vigente.

Artículo 36.- Intercambio de información

El Servicio Integrado de Seguridad ECU 911 podrá intercambiar o comunicar datos personales con entidades públicas o privadas que intervengan en la atención de emergencias, cuando sea necesario para la protección de la vida, la integridad de las personas o el cumplimiento de obligaciones legales.

Artículo 37.- Garantías en el tratamiento

El tratamiento de datos personales en contextos de emergencia deberá ejecutarse bajo criterios de especial diligencia, considerando la naturaleza urgente de las operaciones y los riesgos asociados al tratamiento de la información.

El Servicio Integrado de Seguridad ECU 911 adoptará medidas que permitan garantizar la confidencialidad, integridad, disponibilidad y trazabilidad de los datos personales, así como mecanismos de control que aseguren la correcta utilización de la información en dichos contextos.

En ningún caso la urgencia del tratamiento justificará el uso de los datos personales para finalidades distintas a las previstas en la presente Política o en la normativa vigente.

CAPÍTULO X
RESPONSABILIDAD Y CONFIDENCIALIDAD

Artículo 38.- Responsabilidades.

El incumplimiento de las disposiciones contenidas en la presente Política por parte de servidores públicos, trabajadores o terceros vinculados al Servicio Integrado de Seguridad ECU 911 estará sujeto a las responsabilidades que correspondan conforme a la normativa vigente.

Artículo 39.- Responsabilidad proactiva.

Resolución Nro. SIS-SIS-2026-0012-R

Quito, 04 de abril de 2026

El Servicio Integrado de Seguridad ECU 911 adoptará un enfoque de responsabilidad proactiva, implementando mecanismos de control, supervisión, auditoría y documentación que permitan demostrar el cumplimiento de la normativa de protección de datos personales ante la autoridad competente.

Artículo 40.- Confidencialidad.

Toda persona que intervenga en el tratamiento de datos personales en el Servicio Integrado de Seguridad ECU 911 estará sujeta al deber de confidencialidad y al cumplimiento obligatorio de la presente Política.

Se prohíbe la divulgación, acceso no autorizado o uso indebido de datos personales, salvo en los casos previstos en la normativa vigente o por disposición de autoridad competente.

Este deber subsistirá incluso después de finalizada la relación con la institución.

El incumplimiento dará lugar a las responsabilidades administrativas, civiles y penales correspondientes, conforme a la normativa aplicable.

DISPOSICIONES GENERALES

PRIMERA.- Cumplimiento institucional: Las autoridades y responsables de las distintas dependencias del Servicio Integrado de Seguridad ECU 911 deberán garantizar la aplicación, difusión y cumplimiento de la presente Política en el ámbito de sus competencias.

SEGUNDA.- Instrumentos complementarios: El Delegado de Protección de Datos Personales podrá proponer, asesorar y emitir recomendaciones sobre lineamientos, protocolos y directrices para la adecuada implementación de la presente Política, en coordinación con las unidades competentes, sin perjuicio de las responsabilidades que correspondan a las áreas encargadas de su ejecución..

TERCERA.- Gestión documental y registro: El tratamiento de datos personales se articulará con los sistemas institucionales de gestión documental y archivo, garantizando su adecuada conservación, acceso controlado y seguridad de la información.

CUARTA.- Actualización de la Política: La presente Política podrá ser actualizada por cambios normativos, institucionales o tecnológicos, o por disposición de la autoridad competente. Las actualizaciones serán difundidas por los canales institucionales.

QUINTA.- Difusión y socialización de la Política: Dispóngase la publicación y difusión de la presente Política para conocimiento de los titulares de datos personales y del personal institucional, a través de los canales institucionales correspondientes; para el efecto, la Dirección de Gestión Documental, en coordinación con la Dirección de Comunicación, realizará las acciones necesarias de socialización y comunicación, a fin de garantizar su adecuada implementación y cumplimiento.

DISPOSICIONES TRANSITORIAS

PRIMERA.- Adecuación institucional: Las dependencias del Servicio Integrado de Seguridad ECU 911 deberán identificar, documentar y validar los tratamientos de datos personales bajo su responsabilidad, en coordinación con el Delegado de Protección de Datos Personales, a fin de mantener actualizado el Registro de Actividades de Tratamiento.

Resolución Nro. SIS-SIS-2026-0012-R

Quito, 04 de abril de 2026

SEGUNDA.- Evaluación de impacto: Las dependencias identificarán los tratamientos de alto riesgo y realizarán las Evaluaciones de Impacto en Protección de Datos Personales (EIPD), en coordinación con el Delegado, quien validará su aplicación de acuerdo con las disposiciones aplicables.

DISPOSICIÓN DEROGATORIA

PRIMERA.- Deróguese la Resolución Nro. SISECU911-DG-2024-011, así como todas las disposiciones, normas, instructivos o instrumentos internos de igual o inferior jerarquía que se opongan o resulten incompatibles con la presente Resolución.

DISPOSICIÓN FINAL

La presente Resolución entrará en vigencia a partir de su suscripción, sin perjuicio de su publicación en el Registro Oficial.

Documento firmado electrónicamente

Mgs. Juan Carlos Paladines Salcedo
DIRECTOR GENERAL

Copia:
Señorita Abogada
Maria del Cisne Ochoa Olmedo
Directora de Gestión Documental y Archivo

av/mb

Firmado electrónicamente por:
JUAN CARLOS
PALADINES SALCEDO
Validar únicamente con FirmaEC