RESOLUCIÓN Nro. SISECU911-DG-2024-011

ABG. ANA MARÍA AYALA ROBLES
DIRECTORA GENERAL

SERVICIO INTEGRADO DE SEGURIDAD ECU 911

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

Que, el artículo 66 numeral 19 de la Constitución de la República de Ecuador: Reconoce y garantiza a las personas: "*(…) 19. El derecho a la protección de datos 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.*"

Que, el artículo 66 numeral 19 de la Constitución de la República de Ecuador: Reconoce y garantiza a las personas: *"(…) 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 de 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 de Ecuador indica lo siguiente: *"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.

La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de

seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez.

La persona afectada podrá demandar por los perjuicios ocasionados."

Que, el artículo 226 de la Constitución de la República de 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 de 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 artículo 35 de la Ley Orgánica de Protección de Datos Personales, 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 Ley Orgánica de Protección de Datos Personales 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 resiliencia 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 Ley Orgánica de Protección de Datos Personales, 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 de 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 Ley Orgánica de Protección de Datos 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, el artículo 146 del Código Orgánico de la Economía Social de los Conocimientos 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:

1. 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.

2. 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.

3. 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, el artículo 1 del Decreto Ejecutivo 214, prescribe: *"Sustitúyase el artículo 2 del Decreto Ejecutivo No. 988, de 29 de diciembre de 2011, por el siguiente texto:"*

> *Artículo 2.- Del Servicio Integrado de Seguridad ECU-911.- 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. Además, contará con un Comité Intersectorial como máximo nivel gobernante, desde el cual se ejercerá la rectoría en el ámbito de sus competencias; y, establecerá centros operativos a nivel nacional.*
>
> *Su sede principal se encuentra ubicada en la ciudad de Quito.*;

Que, mediante Resolución No. SIS-ECU-DIR-2024-002 de 21 de mayo de 2024, emitida por el Comité Intersectorial del Servicio Integrado de Seguridad ECU 911, se designó a la Ab. Ana María Ayala Robles, en calidad de Directora General del Servicio Integrado de Seguridad ECU 911, conforme lo sustenta la Acción de Personal No. PC-NJS-0006 de 29 de mayo de 2024;

En uso de las facultades y atribuciones que confiere el artículo 77 número 1 letra e) de la Ley Orgánica de la Contraloría General del Estado, el artículo 11 del Estatuto Orgánico de Gestión Organizacional por Procesos del Servicio Integrado de Seguridad ECU 911, el Decreto Ejecutivo 214 de fecha 28 de marzo de 2024 y demás ordenamiento jurídico invocado;

RESUELVE EMITIR LA POLÍTICA DE PROTECCIÓN DE DATOS

CAPÍTULO I: PRIVACIDAD Y ÁMBITO DE APLICACIÓN

Artículo 1. Ámbito de aplicación y datos recolectados. -

El ámbito de aplicación de la presente resolución es para todo el personal del Servicio Integrado de Seguridad ECU911, a nivel nacional.

Los datos recolectados por el SIS ECU 911, son:

Plataforma	Datos manejados	Tipo de usuario
Mobile Locator	Cedula de Ciudadanía Nombres y Apellidos Teléfono Geolocalización	Ciudadano
Sistema Automatizado de Entrega de Información - Función Judicial (SAEI - FJ)	Nombres y Apellidos Correo Electrónico Videos de atención de emergencias Audios de atención de emergencias	Juez - Fiscales
Sistema de atención de emergencias	Nombres y Apellidos Teléfono	Ciudadano
Plataforma virtual de aprendizaje EVA	Cedula de ciudadanía Nombre y Apellido ciudadanía Correo Electrónico Genero Identificación étnica Discapacidad	Ciudadano

Ficha de inscripción taller Primer Respondiente	Cedula de ciudadanía Nombre y Apellido Fecha de nacimiento Correo Electrónico Cedula de ciudadanía Dirección Teléfono Dirección laboral teléfono Laboral Cargo Escolaridad Nivel de escolaridad Actividad docente Experiencia en primera respuesta Firma	Ciudadano
Líneas suspendidas	Nombres y apellidos Teléfono reportado Cedula de Ciudadanía Código dactilar de la Cedula de Ciudadanía Dirección de correo electrónico Teléfono de contacto Ciudad de residencia Discapacidad Tercera edad	Ciudadano
Redes sociales/ Requerimientos ciudadanos/ redes sociales	Ciudad de ocurrencia de la emergencia Sector de ocurrencia de la emergencia Fecha de la llamada Nombre de quien reporta la emergencia Número telefónico de quien reporta la emergencia Teléfono de contacto	Ciudadano
Vinculación con la comunidad / oficio	Nombre del delegado Teléfono	Ciudadano
Control de calidad SIA	Nombres Apellidos Teléfono Direccion de la emergencia	Ciudadano
Encuestas de satisfacción	Nombres Apellidos Teléfono Correo electrónico Sexo Edad	Ciudadano

Requerimiento ciudadanos/ Sistema de atención de emergencias	Nombre de quien reporta la emergencia Número telefónico de quien reporta la emergencia Teléfono de contacto Dirección de la emergencia	Ciudadano
APP ECU 911	Cédula Nombre apellido Ciudadanía Teléfono Tipo de discapacidad Tipo de sangre Alergias Correo electrónico Nombre y apellido del contacto de emergencia Teléfono del contacto de emergencia Parentesco del contacto de emergencia	Ciudadano

Artículo 2. Términos y Definiciones. -

Para los efectos de esta política, se adoptan las siguientes definiciones:

1. **Base de datos o fichero:** Conjunto estructurado de datos cualquiera que sea su modalidad de creación, almacenamiento, organización, tipo de soporte, tratamiento, procesamiento, localización o acceso, centralizado, descentralizado o repartido de forma funcional o geográfica.
2. **Consentimiento:** Manifestación de la voluntad libre, específica, informada e inequívoca, mediante la cual el titular de los datos personales autoriza al responsable del tratamiento.
3. **Dato biométrico:** Dato personal único, relativo a las características físicas o fisiológicas, o conductas de una persona natural que permita confirmar su identificación única, como imágenes faciales o huellas dactilares.
4. **Dato genético:** Dato personal relacionado con características genéticas heredadas o adquiridas de una persona natural, que proporcione información única sobre su fisiología o salud.
5. **Dato personal:** Información que identifica o hace identificable a una persona natural, de manera directa o indirecta.
6. **Datos sensibles:** Datos relativos a etnia, identidad de género, identidad cultural, religión, ideología, filiación política, salud, datos biométricos, y cualquier otro que, por su naturaleza, requiera protección especial.
7. **Datos relativos a la salud:** Datos personales relativos a la salud física o mental de una persona incluida a prestación de servicios de atención sanitaria que revelen información sobre su estado de salud
8. **Destinatario:** Persona natural o jurídica que ha recibido comunicación de datos personales.

9. **Entidad certificadora:** Institución reconocida por la Autoridad de Protección de Datos Personales que proporciona certificaciones relacionadas con protección de datos.
10. **Transferencia o comunicación de datos:** Cualquier acción que implique compartir, interconectar, ceder, transmitir o divulgar información personal a terceros.

CAPÍTULO II: FINALIDADES DEL TRATAMIENTO DE DATOS

Artículo 3. Finalidades

1. Coordinar de manera eficiente la atención de emergencias.
2. Evaluar la calidad del servicio mediante encuestas y análisis de datos.
3. Gestionar procesos de capacitación dirigidos a usuarios externos.
4. Apoyar actividades de videovigilancia y seguridad ciudadana.
5. Identificar oportunidades de mejora en la operación del servicio.

CAPÍTULO III: DERECHOS DE LOS TITULARES

Artículo 4. Derechos. -

1. Acceso a sus datos personales y solicitud de correcciones.
2. Eliminación de datos cuando ya no sean necesarios para las finalidades declaradas.
3. Información clara sobre el tratamiento de sus datos.

Artículo 5. Consentimiento. -

El tratamiento de datos personales requerirá el consentimiento libre, informado y específico del titular, salvo excepciones legales u órdenes de autoridad competente.

CAPÍTULO IV: MEDIDAS DE SEGURIDAD

Artículo 6. Seguridad de los datos. -

1. Implementación de sistemas de cifrado y control de acceso.
2. Realización de auditorías periódicas para garantizar la seguridad.
3. Aplicación de protocolos de gestión de riesgos tecnológicos y operativos.
4. Uso de herramientas de monitoreo para la detección y prevención de incidentes de seguridad.

Artículo 7. Transferencia de datos. -

1. Los datos podrán ser transferidos a terceros autorizados para fines específicos, como seguridad y atención de emergencias.
2. Todo tercero deberá cumplir con las normativas de protección de datos establecidas.
3. Se deberá contar con acuerdos de confidencialidad y garantizar mecanismos de auditoría para verificar el cumplimiento normativo.

Artículo 8. Excepciones de consentimiento para la transferencia o comunicación de datos personales. -

1. No será necesario el consentimiento del titular en los siguientes casos:
    - Cuando el tratamiento o la comunicación de datos personales se realice en el marco de la atención de una alerta o emergencia.
    - Cuando sea requerido por orden judicial o mandato legal.
    - En cumplimiento de una obligación legal que recaiga sobre el del Servicio Integrado de Seguridad ECU-911.
    - Para proteger los derechos humanos del titular o de otra persona natural.
2. Estos casos deberán estar documentados y contar con los respectivos controles de seguridad para garantizar la protección de los datos.

CAPÍTULO V: TRATAMIENTO DE DATOS PERSONALES ESPECIALES

Artículo 9. Datos sensibles. -

1. Se consideran sensibles los datos relacionados con salud, etnia, religión, antecedentes penales y otros definidos por la ley.
2. Su tratamiento requerirá autorización expresa del titular, salvo excepciones legales y las establecidas en la presente política.

Artículo 10. Categorización especial. -

1. Datos biométricos recolectados a través de sistemas de videovigilancia.
2. Información vinculada a la localización móvil de los usuarios.
3. Registros generados por plataformas de atención de emergencias.
4. Información registrada en sistemas de audio y video para procesos de atención o auditoría de emergencias.

CAPÍTULO VI: ACTUALIZACIÓN Y CUMPLIMIENTO DE LA POLÍTICA

Artículo 11. Evaluación y actualización. -

El Servicio Integrado de Seguridad ECU-911 será responsable de evaluar periódicamente la aplicación de esta política y realizar ajustes necesarios para garantizar su eficacia.

Artículo 12. Difusión y cumplimiento

1. Esta política será publicada en los portales oficiales del Servicio Integrado de Seguridad ECU-911 para garantizar su acceso público.
2. Se promoverá la capacitación del personal en los principios y obligaciones establecidos en esta política.
3. Se implementarán mecanismos de verificación y auditoría para asegurar el cumplimiento integral de esta política.

El Servicio Integrado de Seguridad ECU-911 será responsable de la difusión y

aplicación de esta política en todas sus operaciones, garantizando la protección de los datos personales en conformidad con el marco normativo ecuatoriano.

DISPOSICIONES GENERALES

PRIMERA. - La socialización de esta Resolución estará a cargo de la Dirección de Asesoría Jurídica del Servicio Integrado de Seguridad ECU 911.

SEGUNDA. - La Dirección de Comunicación Social del Servicio Integrado de Seguridad ECU 911, publicará la presente Resolución y su anexo, en el sitio web institucional de la entidad.

La presente Resolución entrará en vigencia a partir de su suscripción, sin perjuicio de los trámites legales pertinentes.

Dado en la ciudad de Quito, a los 31 días del mes de diciembre de 2024

Firmado electrónicamente por:
ANA MARIA AYALA ROBLES

Ab. Ana María Ayala Robles
DIRECTORA GENERAL
SERVICIO INTEGRADO DE SEGURIDAD ECU 911