Política de Tratamiento de Datos Personales

Asociación de Scouts del Ecuador

1. INTRODUCCIÓN

La ASOCIACIÓN DE SCOUTS DEL ECUADOR, con RUC N.º 1791230698001, con domicilio en Av. América N35-101 y Mañosca, Quito – Ecuador, correo electrónico: datospersonales@scoutsecuador.org, Casilla 17 - 08 - 8291 Tel: (5932) 2266629 / 2252617 mediante mensajería instantánea (WhatsApp) al 0958635419, y, en adelante el Responsable del Tratamiento, determina los fines y medios del tratamiento de datos personales conforme a la Ley Orgánica de Protección de Datos Personales (LOPDP).

Para efectos de la presente política, se entenderá por Responsable del tratamiento a la Asociación de Scouts del Ecuador, incluyendo a sus órganos de gobierno, niveles territoriales, estructuras operativas, dirigentes y voluntarios, quienes actúan bajo su dirección, en el marco de sus competencias y bajo su responsabilidad.

2. MARCO OPERATIVO

La presente política se fundamenta en la Ley Orgánica de Protección de Datos Personales (LOPDP), en particular en sus disposiciones relativas al deber de información (Art. 12), bases de legitimación del tratamiento, consentimiento del titular y ejercicio de derechos, así como en su Reglamento General, especialmente en lo referente a procedimientos, responsabilidades y medidas de seguridad. Asimismo, se sustenta en las resoluciones emitidas por la Superintendencia de Protección de Datos Personales (SPDP), incluyendo la normativa vigente aplicable al Delegado de Protección de Datos Personales y lineamientos de responsabilidad proactiva.

De forma complementaria, esta política incorpora los principios de privacidad desde el diseño y por defecto, gestión basada en riesgos y demostrabilidad, los cuales orientan la implementación de controles técnicos, organizativos y jurídicos adecuados, alineados con estándares internacionales de seguridad de la información.

3. DELEGADO DE PROTECCIÓN DE DATOS PERSONALES (DPD)

El Responsable ha designado un Delegado de Protección de Datos Personales, quien actúa con independencia funcional, asesorando, supervisando y verificando el cumplimiento de la normativa aplicable, así como atendiendo los requerimientos de los titulares y actuando como punto de contacto con la autoridad de control. El Delegado podrá ser contactado en el domicilio ubicado en Av. América N35-101 y Mañosca, Quito – Ecuador, así como a través del correo electrónico: datospersonales@scoutsecuador.org.

4. ÁMBITO DE APLICACIÓN

Esta política es aplicable a todos los tratamientos de datos personales realizados por la organización, incluyendo aquellos correspondientes a miembros, aspirantes, representante legal de menores de edad, personal administrativo, proveedores y cualquier tercero vinculado. Su aplicación comprende tanto medios digitales, incluido el sistema SISCOUT, como archivos físicos.

Las disposiciones de la presente política son de cumplimiento obligatorio para todos los niveles organizacionales, incluyendo órganos nacionales, distritos, grupos scouts, dirigentes, y cualquier persona que actúe por cuenta del Responsable del tratamiento.

5. PRINCIPIOS DEL TRATAMIENTO

El tratamiento de datos personales se realizará bajo los principios de licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; integridad y confidencialidad; y responsabilidad proactiva, debiendo el Responsable ser capaz de demostrar el cumplimiento de estos principios en todo momento.

6. FINALIDADES DEL TRATAMIENTO

El tratamiento de datos personales se realiza para finalidades específicas, explícitas y legítimas, debidamente determinadas por el Responsable, las cuales se detallan a continuación junto con su correspondiente base de legitimación, en concordancia con el Registro de Actividades de Tratamiento (RAT):

En relación con la **gestión de registro y administración de miembros,** los datos serán tratados para la creación, actualización y mantenimiento de perfiles en el sistema SISCOUT, así como para el seguimiento del historial institucional. Este tratamiento se fundamenta en la ejecución de la relación asociativa.

En cuanto a la **gestión formativa y participación en actividades**, los datos serán utilizados para la planificación, organización y control de actividades educativas, eventos y programas scouts. La base legal corresponde a la ejecución de la relación asociativa.

Respecto a la **gestión de comunicaciones institucionales**, los datos serán tratados para el envío de información relevante sobre actividades, avisos, convocatorias y comunicaciones operativas. Este tratamiento se basa en la ejecución de la relación asociativa y, cuando corresponda, en el consentimiento del titular para comunicaciones no esenciales.

En materia de **seguridad y bienestar de los miembros**, incluyendo la atención de emergencias, los datos personales, incluso aquellos de carácter sensible como información de salud o grupo sanguíneo, serán tratados con la finalidad de proteger la

integridad física de los miembros. Este tratamiento se fundamenta en el interés legítimo del Responsable y en el consentimiento explícito del titular cuando corresponda.

En relación con el **cumplimiento de obligaciones legales y regulatorias**, los datos serán tratados para atender requerimientos de autoridades, cumplimiento de normativa aplicable y gestión administrativa obligatoria. Este tratamiento se sustenta en el cumplimiento de obligaciones legales.

El Responsable garantiza que no se realizarán tratamientos para finalidades incompatibles con las aquí descritas y que cualquier nueva finalidad será previamente evaluada, documentada y comunicada al titular conforme a la normativa vigente.

7. BASES DE LEGITIMIZACIÓN

El tratamiento de datos personales se fundamenta en bases jurídicas específicas, las cuales se encuentran directamente vinculadas con cada finalidad del tratamiento, conforme al principio de licitud y en concordancia con el Registro de Actividades de Tratamiento (RAT), garantizando una correspondencia explícita y verificable:

Finalidad del tratamiento	Base de legitimación
Gestión de registro y administración de miembros	Ejecución de la relación asociativa
Gestión formativa y participación en actividades	Ejecución de la relación asociativa
Comunicaciones institucionales esenciales	Ejecución de la relación asociativa
Comunicaciones no esenciales	Consentimiento del titular
Seguridad y bienestar de los miembros (incluye datos sensibles)	Interés legítimo + Consentimiento explícito
Cumplimiento de obligaciones legales y regulatorias	Cumplimiento de obligaciones legales

El Responsable garantiza que cada tratamiento de datos personales cuenta con una base jurídica válida, previamente identificada, documentada y alineada con su finalidad específica. En caso de requerirse nuevas finalidades o cambios en las bases de legitimación, estos serán evaluados previamente, documentados en el RAT y comunicados al titular conforme a la normativa vigente.

8. CATEGORÍA DE DATOS PERSONALES

El Responsable trata distintas categorías de datos personales en función de las finalidades descritas, las cuales se detallan a continuación con ejemplos concretos:

Se tratarán **datos identificativos**, tales como nombres, apellidos, número de cédula de identidad, fecha de nacimiento y fotografía; **datos de contacto**, como dirección domiciliaria, correo electrónico y números telefónicos; así como **datos académicos y laborales**, incluyendo nivel de instrucción, ocupación y experiencia relevante para la participación en actividades.

Asimismo, se tratarán **datos de participación institucional**, tales como historial de actividades, pertenencia a grupos scouts, registros de asistencia, reconocimientos y evaluaciones dentro de la organización.

Adicionalmente, el Responsable podrá tratar **categorías especiales de datos personales**, en particular información de salud, grupo sanguíneo, religión e imagen. En este contexto, se deja expresa constancia de que los datos de salud no son tratados de manera sistemática, sino de forma **episódica y contextual**, exclusivamente en situaciones relacionadas con la gestión de emergencias, seguridad y bienestar de los miembros durante actividades scouts.

El tratamiento de estos datos sensibles se realiza bajo medidas de seguridad reforzadas, con acceso restringido y únicamente por personal autorizado, y se encuentra sujeto al consentimiento explícito del titular o de su representante legal, conforme a la normativa vigente.

El Responsable garantiza que el tratamiento de datos personales se limita a aquellos estrictamente necesarios para el cumplimiento de las finalidades definidas, en aplicación del principio de minimización.

9. ORIGEN DE LOS DATOS

Los datos personales serán obtenidos directamente del titular o de su representante legal, en el caso de menores de edad. El responsable garantiza que no se realizará recolección de datos sin una base legal válida.

10. DATOS DE MENORES DE EDAD

El tratamiento de datos personales de niños, niñas y adolescentes se realizará bajo un estándar reforzado de protección, considerando su condición de categoría especial de datos personales conforme a la Ley Orgánica de Protección de Datos Personales, y en estricto apego al principio del interés superior del niño, niña o adolescente.

En este sentido, el tratamiento de dichos datos se efectuará prioritariamente sobre la base del consentimiento expreso, libre, informado e inequívoco del representante legal del o la

persona menor de edad, garantizando en todo momento el conocimiento informado sobre las finalidades, alcance, riesgos y condiciones del tratamiento de los datos personales.

El Responsable implementará medidas técnicas, organizativas y jurídicas reforzadas para garantizar la confidencialidad, integridad y seguridad de los datos personales de menores de edad, limitando su acceso exclusivamente a personal autorizado y únicamente para las finalidades estrictamente necesarias relacionadas con la gestión educativa, operativa, de seguridad y bienestar dentro de las actividades scouts.

En ningún caso se tratarán datos personales de menores de edad para finalidades incompatibles con su desarrollo integral, ni se realizará un uso que pueda afectar sus derechos fundamentales.

11. TRANSFERENCIAS Y ENCARGADOS DEL TRATAMIENTO

Los datos personales podrán ser tratados por terceros en calidad de encargados, en virtud de contratos de encargo que establezcan de forma expresa y verificable obligaciones de confidencialidad, seguridad, tratamiento conforme a instrucciones documentadas del Responsable, limitación de finalidad, subcontratación controlada, notificación de incidentes y eliminación o devolución de los datos al finalizar la relación contractual.

Cuando el tratamiento implique transferencias internacionales de datos personales, el Responsable garantizará que dichas transferencias se realicen únicamente hacia países u organizaciones que cuenten con un nivel adecuado de protección reconocido, o en su defecto, mediante la implementación de garantías apropiadas, tales como cláusulas contractuales, acuerdos de confidencialidad reforzados y mecanismos jurídicos que aseguren el cumplimiento de los principios de la LOPDP.

El Responsable mantendrá un control continuo sobre los encargados del tratamiento, incluyendo procesos de debida diligencia previa a su contratación, verificación de sus medidas de seguridad y cumplimiento normativo, así como la definición de obligaciones específicas en materia de protección de datos personales.

Adicionalmente, el Responsable realizará auditorías periódicas a los encargados del tratamiento con una frecuencia mínima anual o conforme al nivel de riesgo identificado, pudiendo incluir revisiones documentales, evaluaciones de cumplimiento y requerimientos de evidencia de controles implementados, con el fin de garantizar la adecuada protección de los datos personales y la responsabilidad proactiva.

12. PLAZOS DE CONSERVACIÓN

El Responsable establece plazos de conservación diferenciados en función de la finalidad del tratamiento, el tipo de datos personales involucrados, el nivel de riesgo y las obligaciones legales aplicables, en cumplimiento del principio de limitación del plazo de conservación y responsabilidad proactiva.

Los plazos de conservación establecidos en la presente política se determinan en atención a obligaciones legales específicas del ordenamiento jurídico ecuatoriano, incluyendo normativa tributaria, contable, administrativa, civil y de prescripción de responsabilidades, así como a criterios de necesidad, proporcionalidad y gestión del riesgo.

En aquellos casos en los que se establecen rangos de conservación, la determinación del plazo concreto aplicable será definida mediante una evaluación interna documentada, considerando, entre otros factores, la naturaleza del tratamiento, el nivel de riesgo para los derechos y libertades de los titulares, la existencia de controversias potenciales, requerimientos de trazabilidad institucional y obligaciones legales vigentes.

Dichas evaluaciones y la decisión adoptada se documentarán en el Registro de Actividades de Tratamiento (RAT) y, cuando corresponda, en las Evaluaciones de Impacto en Protección de Datos (EIPD), como parte del principio de responsabilidad proactiva y demostrabilidad ante la autoridad de control.

En ningún caso los datos personales serán conservados por un plazo superior al estrictamente necesario sin una base legal o justificación documentada que lo respalde.

Los plazos definidos se fundamentan en criterios de necesidad, proporcionalidad, trazabilidad institucional, cumplimiento normativo y defensa ante eventuales responsabilidades legales o administrativas. Una vez cumplida la finalidad del tratamiento o expirado el plazo establecido, los datos serán eliminados o anonimizados mediante mecanismos seguros, dejando evidencia verificable del proceso.

A continuación, se detalla la tabla de conservación por finalidad:

Finalidad del tratamiento	**Tipo de datos**	**Plazo de conservación**	**Justificación**
Gestión de miembros (registro, historial, participación)	Datos identificativos, contacto, académicos	Durante la relación + 5 a 10 años posteriores	Trazabilidad institucional, responsabilidades legales y defensa ante reclamaciones
Gestión de seguridad y bienestar	Datos sensibles (salud, grupo sanguíneo)	Solo durante la necesidad operativa	Principio de minimización y alto nivel de riesgo asociado
Gestión de menores de edad	Datos identificativos y sensibles	Durante la relación + máximo 5 años	Interés superior del menor y reducción de riesgo

Obligaciones legales, contables y administrativas	Datos financieros y administrativos	7 años	Cumplimiento de normativa tributaria y obligaciones legales en Ecuador
Registros de consentimiento	Evidencia de aceptación (logs, formularios)	Mínimo 5 años	Demostrabilidad ante la autoridad de control
Registros de acceso y seguridad (logs)	Datos técnicos de acceso	1 a 3 años	Seguridad de la información y análisis de incidentes

El Responsable podrá ajustar estos plazos cuando exista una obligación legal específica o una necesidad debidamente justificada, la cual deberá ser documentada en el Registro de Actividades de Tratamiento (RAT) y, de ser aplicable, en la Evaluación de Impacto en Protección de Datos (EIPD).

13. PROCEDIMIENTO PARA EJERCICIO DE DERECHOS DE TITULARES

El Responsable establece el siguiente procedimiento formal para garantizar el ejercicio efectivo de los derechos de los titulares, en cumplimiento de la LOPDP, su Reglamento y el principio de responsabilidad proactiva, asegurando trazabilidad, control y evidencia verificable en cada etapa del proceso.

El procedimiento inicia con la recepción de la solicitud del titular, la cual podrá ser presentada a través del correo electrónico institucional o mediante comunicación dirigida al Delegado de Protección de Datos. El responsable de la recepción será el Delegado de Protección de Datos o el área designada de atención, quien deberá registrar la solicitud en un sistema de control interno en un plazo máximo de un (1) día hábil desde su recepción.

Una vez recibida la solicitud, se procederá a la validación de la identidad del titular o de su representante legal. Esta actividad será responsabilidad del Delegado de Protección de Datos, quien contará con un plazo máximo de dos (2) días hábiles para verificar la identidad. En caso de que la solicitud sea incompleta o requiera subsanación, se notificará al titular dentro de este mismo plazo, suspendiéndose el cómputo del tiempo hasta que se complete la información requerida.

Validada la identidad, el Delegado de Protección de Datos remitirá la solicitud al área responsable del tratamiento correspondiente, en un plazo máximo de un (1) día hábil, identificando el tipo de derecho solicitado y las acciones requeridas.

El área responsable del tratamiento deberá analizar la solicitud, ejecutar las acciones necesarias y emitir un informe de respuesta en un plazo máximo de diez (10) días hábiles. En casos complejos o cuando exista una justificación debidamente documentada, este plazo podrá extenderse por cinco (5) días hábiles adicionales, lo cual deberá ser informado oportunamente al titular.

El Delegado de Protección de Datos consolidará la respuesta final y la comunicará al titular dentro del plazo máximo legal aplicable, asegurando que la respuesta sea clara, motivada y conforme a derecho. Esta comunicación deberá realizarse por el mismo medio en que se presentó la solicitud, salvo que el titular indique otro canal.

Durante todo el proceso, el Responsable garantizará la trazabilidad de la solicitud, manteniendo registros que incluyan la fecha de recepción, validación de identidad, actuaciones realizadas, responsables intervinientes, tiempos de respuesta y evidencia de la comunicación final al titular.

En caso de negativa total o parcial a la solicitud, la respuesta deberá estar debidamente motivada, indicando las razones legales y los mecanismos disponibles para que el titular pueda presentar un reclamo ante la Superintendencia de Protección de Datos Personales.

El Delegado de Protección de Datos será responsable de supervisar el cumplimiento de este procedimiento, así como de implementar controles periódicos que aseguren su eficacia y mejora continua.

14. MECANISMOS DE RECLAMO

En caso de considerar que sus derechos han sido vulnerados, el titular podrá presentar un reclamo ante la Superintendencia de Protección de Datos Personales, sin perjuicio de las acciones administrativas o judiciales correspondientes.

15. DECISIONES AUTOMATIZADAS

El Responsable no adopta decisiones automatizadas que produzcan efectos jurídicos sobre los titulares ni realiza perfilamiento sistemático.

16. MEDIDAS DE SEGURIDAD

El Responsable implementa un sistema integral de medidas técnicas, organizativas y jurídicas orientado a garantizar la confidencialidad, integridad y disponibilidad de los datos personales, de conformidad con el principio de seguridad y el enfoque de gestión de riesgos. Dichas medidas se determinan a partir de la identificación, análisis y tratamiento de riesgos documentados en el Registro de Actividades de Tratamiento (RAT) y, cuando corresponda, en las Evaluaciones de Impacto en Protección de Datos (EIPD), manteniéndose evidencia verificable de su implementación, eficacia y mejora continua.

En el plano técnico, el Responsable aplica controles de autenticación robusta, incluyendo autenticación multifactor para accesos privilegiados y remotos, gestión de identidades y control de accesos basado en roles con el principio de mínimo privilegio, cifrado de datos en tránsito mediante protocolos seguros y, cuando resulte pertinente por el nivel de riesgo, cifrado de datos en reposo. Se implementan mecanismos de registro y monitoreo continuo de eventos (logs) que permiten la trazabilidad de accesos y operaciones sobre datos personales, así como la detección temprana de anomalías. Los sistemas se mantienen actualizados mediante gestión de parches y vulnerabilidades, y se ejecutan respaldos periódicos con pruebas de restauración para asegurar la disponibilidad de la información.

En el plano organizativo, el Responsable adopta políticas y procedimientos formales que regulan el acceso y uso de la información, la clasificación de datos, la gestión de incidentes, la continuidad del negocio y la recuperación ante desastres. Se establecen controles de segregación de funciones, revisiones periódicas de accesos, y programas de capacitación continua para el personal en materia de protección de datos y seguridad de la información. Asimismo, se documentan inventarios de activos de información, matrices de riesgo y planes de tratamiento, con responsables asignados y fechas de cumplimiento, los cuales son supervisados por el Delegado de Protección de Datos.

En el plano jurídico, el Responsable suscribe acuerdos de confidencialidad con su personal y terceros, así como contratos de encargo de tratamiento que incluyen obligaciones específicas sobre seguridad, tratamiento conforme instrucciones documentadas, subencargados, notificación de incidentes, auditoría y eliminación o devolución de datos al término de la relación. Se establecen cláusulas de responsabilidad y mecanismos de supervisión para verificar el cumplimiento por parte de los encargados.

De manera transversal, el Responsable aplica el principio de privacidad desde el diseño y por defecto en el desarrollo y operación de sistemas, en particular el sistema SISCOUT, asegurando que solo se traten los datos necesarios para cada finalidad y que las configuraciones iniciales favorezcan el mayor nivel de protección. Las medidas de seguridad son revisadas periódicamente, al menos de forma anual o ante cambios significativos en los riesgos, tecnologías o tratamientos, documentándose los resultados de dichas revisiones y las acciones de mejora correspondientes.

17. GESTIÓN DE INCIDENTES Y BRECHAS

El Responsable implementa un procedimiento formal y documentado para la gestión de incidentes de seguridad que afecten datos personales, alineado al principio de responsabilidad proactiva y a las obligaciones de notificación establecidas en la LOPDP y su Reglamento. Dicho procedimiento contempla las fases de detección, registro, contención, análisis, clasificación del impacto, notificación y remediación, manteniendo evidencia verificable de cada actuación.

Una vez detectado un incidente, el área responsable deberá registrarlo de inmediato en el sistema de gestión de incidentes, activar medidas de contención inicial y notificar al

Delegado de Protección de Datos en un plazo máximo de veinticuatro (24) horas. El Delegado de Protección de Datos coordinará el análisis de impacto para determinar si el incidente constituye una vulneración de seguridad de datos personales y si existe riesgo para los derechos y libertades de los titulares.

Cuando el incidente califique como brecha de seguridad que deba ser reportada, el Responsable notificará a la Superintendencia de Protección de Datos Personales en un plazo máximo de cuarenta y ocho (48) horas desde que tenga conocimiento del hecho, o dentro del plazo que establezca la normativa vigente. En los casos en que la brecha implique un alto riesgo para los titulares, también se procederá a su notificación directa en el menor tiempo posible.

La notificación a la autoridad deberá incluir, como mínimo, la siguiente información: la naturaleza del incidente, las categorías y volumen aproximado de datos personales afectados, el número estimado de titulares impactados, las posibles consecuencias del incidente, las medidas adoptadas o propuestas para mitigar los efectos y prevenir su repetición, así como los datos de contacto del Delegado de Protección de Datos para efectos de seguimiento.

De igual forma, cuando corresponda la notificación a los titulares, esta deberá realizarse en lenguaje claro y comprensible, indicando la naturaleza del incidente, los datos comprometidos, los riesgos potenciales, las medidas adoptadas por el Responsable y las recomendaciones para mitigar posibles efectos adversos.

El Responsable documentará integralmente cada incidente, incluyendo su causa raíz, impacto, acciones correctivas y lecciones aprendidas, incorporando mejoras en los controles de seguridad. El Delegado de Protección de Datos supervisará el cumplimiento del procedimiento, verificará los tiempos de respuesta y reportará periódicamente a la alta dirección sobre la gestión de incidentes y el estado de las medidas implementadas.

18. PRIVACIDAD POR DISEÑO Y DEFECTO

Los sistemas y procesos del Responsable, incluido SISCOUT, se desarrollan e implementan bajo el enfoque de privacidad desde el diseño y por defecto, garantizando la minimización de datos y la configuración de niveles adecuados de protección desde su concepción. Previo a la implementación de nuevos tratamientos de datos personales, cambios sustanciales en las finalidades, incorporación de nuevas tecnologías o modificaciones relevantes en los flujos de información, el Responsable deberá realizar una Evaluación de Impacto en Protección de Datos (EIPD/DPIA) cuando exista riesgo alto o potencial para los derechos y libertades de los titulares.

La EIPD deberá documentar, como mínimo, la descripción sistemática del tratamiento previsto, el análisis de necesidad y proporcionalidad, la identificación y valoración de riesgos, y las medidas técnicas y organizativas previstas para mitigarlos. La realización de la EIPD será coordinada por el área responsable del tratamiento con la participación obligatoria del Delegado de Protección de Datos.

La aprobación de la EIPD será requisito previo para la puesta en producción del tratamiento o cambio significativo, debiendo contar con el visto bueno expreso del Delegado de Protección de Datos, quien verificará la adecuación de las medidas propuestas y la conformidad con la LOPDP, su Reglamento y las directrices de la SPDP. En caso de identificarse riesgos residuales altos, el Responsable deberá abstenerse de iniciar el tratamiento hasta implementar medidas adicionales o, cuando corresponda, gestionar las consultas o notificaciones a la autoridad competente.

El Responsable mantendrá un repositorio de EIPD actualizado y trazable, y revisará periódicamente dichas evaluaciones cuando cambien los riesgos, las tecnologías o las finalidades del tratamiento, asegurando la mejora continua del enfoque de privacidad por diseño y por defecto.

19. REGISTRO DE ACTIVIDADES DE TRATAMIENTO

El Responsable mantiene un Registro de Actividades de Tratamiento (RAT) actualizado, que documenta las finalidades, categorías de datos, bases legales, encargados, medidas de seguridad y niveles de riesgo asociados a cada tratamiento.

La responsabilidad del mantenimiento, actualización y control del RAT recae en el Delegado de Protección de Datos, en coordinación con las áreas responsables de cada proceso de tratamiento, quienes deberán proporcionar información actualizada, veraz y completa.

El RAT será revisado y actualizado con una periodicidad mínima trimestral, así como de manera obligatoria cuando se produzcan cambios relevantes en las finalidades del tratamiento, incorporación de nuevas categorías de datos personales, implementación de nuevas tecnologías, modificaciones en los encargados del tratamiento o cualquier otro cambio que implique variación en el nivel de riesgo.

El Responsable garantizará la trazabilidad de las actualizaciones del RAT, manteniendo control de versiones, fecha de actualización, responsables intervinientes y justificación de los cambios realizados, como parte del principio de responsabilidad proactiva.

20. EVALUACIONES DE IMPACTO

Se realizarán evaluaciones de impacto en protección de datos cuando el tratamiento implique un alto riesgo para los derechos y libertades de los titulares, particularmente en el caso de tratamiento de datos sensibles o implementación de nuevas tecnologías.

21. CONTROL Y AUDITORÍA

El Responsable implementa mecanismos de control interno y auditoría periódica para verificar el cumplimiento de la normativa aplicable, bajo la supervisión del Delegado de Protección de Datos.

22. RESPONSABILIDAD PROACTIVA

El Responsable adopta un enfoque de responsabilidad proactiva, asegurando la existencia de evidencia documental, registros y controles que permitan demostrar el cumplimiento de la normativa en cualquier momento.

23. ACTUALIZACIÓN DE LA POLÍTICA

La presente política será revisada y actualizada periódicamente en función de cambios normativos, tecnológicos u organizacionales.

24. PUBLICACIÓN

La política se encuentra disponible para consulta en el siguiente enlace: https://scoutsecuador.org/biblioteca/politica-proteccion-datos-personales

APROBACIÓN INSTITUCIONAL

La presente política ha sido debidamente revisada y aprobada por el Consejo Nacional de la Asociación de Scouts del Ecuador, en ejercicio de sus atribuciones y conforme a los procedimientos internos establecidos, mediante resolución adoptada en sesión extraordinaria de fecha 22 de abril de 2026.

Certifica:

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JORGE LUIS ARAY DE LA CRUZ

Jorge Aray De la Cruz
Director Ejecutivo / Secretario Consejo Nacional

REGISTRO DE CONTROL DE VERSIONES

Versión	Fecha	Descripción del cambio	Elaborado por	Revisado por	Aprobado por
1	22/04/2026	Emisión inicial de la política	IMS Ecuador	Jorge Aray, Director Ejecutivo	Consejo Nacional Scout