POLÍTICA DE PRIVACIDAD PARA LA APLICACIÓN MÓVIL DEL SISTEMA DE EVALUACIÓN INICIAL DE NECESIDADES (EVIN)

Versión 1.0 – Año 2025.

EL NUEVO ECUADOR

Secretaría Nacional de Gestión de Riesgos

FIRMAS DE REVISIÓN Y APROBACIÓN

Acción	Nombre / Cargo	Firma
Elaborado por:	Magda Julissa Maya Ruiz / Analista de Asistencia Humanitaria 3	Firmado electrónicamente por: MAGDA JULISSA MAYA RUIZ. Validar únicamente con FirmaEC
	Manuel Víctor Sánchez Chinga/ Analista de Servicios de Tecnologías de la Información 2	Firmado electrónicamente por: MANUEL VICTOR SANCHEZ CHINGA. Validar únicamente con FirmaEC
	Romina Lissette Estrella Quijije / Analista de Servicios, Procesos y Calidad 3	Firmado electrónicamente por: ROMINA LISSETTE ESTRELLA QUIJIJE. Validar únicamente con FirmaEC
Revisión técnica:	Juan Xavier Galarza Cuadros / Director de Operaciones	Firmado electrónicamente por: JUAN XAVIER GALARZA CUADROS. Validar únicamente con FirmaEC
	Mario Alberto Mayorga Terán / Director de Tecnologías de la Información y Comunicación	Firmado electrónicamente por: MARIO ALBERTO MAYORGA TERAN. Validar únicamente con FirmaEC
	Romina Lissette Estrella Quijije / Directora de Servicios, Procesos y Calidad, Subrogante	Firmado electrónicamente por: ROMINA LISSETTE ESTRELLA QUIJIJE. Validar únicamente con FirmaEC
Aprobado por:	Diego Alejandro Ripalda López / Subsecretario de Preparación y Respuesta ante Eventos Adversos	Firmado electrónicamente por: DIEGO ALEJANDRO RIPALDA LOPEZ. Validar únicamente con FirmaEC
	Javier Alejandro Luna Rodríguez / Coordinador General de Planificación y Gestión Estratégica, Subrogante	Firmado electrónicamente por: JAVIER ALEJANDRO LUNA RODRIGUEZ. Validar únicamente con FirmaEC
	Diana Isabel Moreira Figueroa / Asesora ministerial / Delegada de Protección de Datos Personales.	Diana Isabel Moreira Figueroa. Time Stamping Security Data

CONTENIDO

1. OBJETO

La presente Política tiene por objeto definir los principios, responsabilidades y obligaciones que rigen el tratamiento de los datos personales recopilados a través de la aplicación móvil del sistema EVIN (Evaluación Inicial de Necesidades).

El sistema EVIN está orientado a la recolección, almacenamiento, procesamiento y análisis de información de personas afectadas por emergencias y desastres, con el objetivo de que el Estado, a través de la Secretaría Nacional de Gestión de Riesgos (SNGR) y los Gobiernos Autónomos Descentralizados (GAD), en el marco de sus competencias, puedan planificar, coordinar y ejecutar acciones de asistencia humanitaria, recuperación y reducción del riesgo.

2. ABREVIATURAS

EVIN: Evaluación Inicial de Necesidades
GAD: Gobiernos Autónomos Descentralizados
GPS: Sistema de Posicionamiento Global
LOPDP: Ley Orgánica de Protección de Datos Personales
ONG: Organismos no Gubernamentales
SNDGIRD: Sistema Nacional Descentralizado de Gestión Integral del Riesgo de Desastres
SNGR: Secretaría Nacional de Gestión de Riesgos

3. RESPONSABLE DEL TRATAMIENTO

La **Secretaría Nacional de Gestión de Riesgos (SNGR)** es la entidad responsable del tratamiento de los datos personales recopilados y gestionado a través de la aplicación móvil del sistema EVIN (Evaluación Inicial de Necesidades). Se detalla información de contacto institucional:

- Dirección: Edificio Centro Integrado de Seguridad, Av. Samborondón Km 0,5.
- Correo de contacto: atencionciudadana@gestionderiesgos.gob.ec
- Teléfono institucional: 042-593500

4. USUARIOS DE LA APLICACIÓN

Los usuarios autorizados para el uso de la aplicación móvil del sistema EVIN son:

- Funcionarios y técnicos de la Secretaría Nacional de Gestión de Riesgos (SNGR).
- Funcionarios y técnicos de otras entidades públicas competentes, debidamente autorizadas por la Secretaría Nacional de Gestión de Riesgos (SNGR).
- Funcionarios y técnicos de los Gobiernos Autónomos Descentralizados (GAD) provinciales, municipales, parroquiales y de Régimen Especial, en el marco de sus competencias en gestión de riesgos y atención a emergencias.
- Voluntariado de protección civil y representantes de instituciones privadas, que actúan en el ámbito de la gestión de riesgos y atención a emergencias.
- Miembros de organizaciones no gubernamentales adscritas al Sistema de las Naciones Unidas.

Estos usuarios actúan en calidad de encargados o intermediarios de tratamiento, bajo las directrices y supervisión de la Secretaría Nacional de Gestión de Riesgos (SNGR) y son responsables de dar cumplimiento a lo dispuesto en la Ley Orgánica de Protección de Datos Personales (LOPDP), su Reglamento y demás normativa aplicable incluyendo la presente política.

5. OBLIGACIONES DE LOS USUARIOS

Cada usuario autorizado de la aplicación EVIN, se compromete a cumplir con las siguientes obligaciones, en estricto apego a la Ley Orgánica de Protección de Datos Personales (LOPDP), su reglamento, esta Política y demás disposiciones vigentes:

- *Recolectar los datos personales de manera lícita, ética, transparente y respetuosa* de los derechos de los titulares.
- *Informar de forma clara y comprensible a cada persona entrevistada sobre*:
  - La finalidad de la recolección de sus datos;
  - La identidad de los responsables del tratamiento (SNGR y GAD);
  - La posibilidad de que sus datos sean tratados por otras entidades públicas integrantes del Sistema Nacional Descentralizado de Gestión Integral del Riesgo de Desastres (SNDGIRD), dentro del ámbito de sus competencias;
  - La eventual transferencia de datos personales, incluidos datos sensibles, entre instituciones públicas del SNDGIRD para fines relacionados con la gestión de emergencias;
  - El carácter voluntario de su participación;
  - Los derechos que le asisten conforme a la LOPDP.
- *Obtener el consentimiento informado* del titular de los datos antes de su tratamiento, incluyendo la autorización expresa para la posible transferencia de datos sensibles entre entidades públicas competentes.
- *Recolectar datos personales de menores de edad exclusivamente a través de sus representantes legales*, previa obtención del consentimiento informado.
- *Limitar la recolección a los datos estrictamente necesarios* para los fines establecido en el sistema EVIN.
- *Utilizar los datos únicamente para los fines autorizados*, evitando cualquier uso indebido o no contemplado.
- *Garantizar la confidencialidad, integridad y seguridad de los datos en todo momento.*
- *Abstenerse de almacenar información en dispositivos no autorizados.*
- *No divulgar, compartir, ni transferir datos personales a terceros no autorizados.*
- *Reportar de manera inmediata cualquier incidente de seguridad, pérdida o acceso no autorizado de datos personales a la SNGR.*
- *Facilitar el ejercicio de los derechos de los titulares de los datos,* en coordinación con la SNGR.
- Cumplir con todas las obligaciones establecidas en la LOPDP, esta Política de Privacidad y cualquier instrucción oficial por la autoridad competente.

6. DATOS PERSONALES QUE SE RECOGEN

En el marco de la implementación del sistema EVIN, los usuarios autorizados podrán recolectar, entre otros, los siguientes datos personales:

- *Datos de identificación:* nombres, apellidos, número de cédula u otro identificador oficial.
- *Datos de contacto:* número telefónico, correo electrónico.
- *Información sobre núcleo familiar*: composición del hogar y vínculos de parentesco.
- *Ubicación geográfica*: coordenadas GPS, dirección del lugar afectado.
- *Condición de salud:* enfermedades, discapacidades, condiciones médicas relevantes.
- *Información económica:* ingresos individuales del grupo familiar.
- *Actividad económica:* ocupación y medios de sustento de los miembros del hogar.
- *Necesidades específicas de asistencia humanitaria*
- *Material visual:* fotografías del sitio afectado y de la persona entrevistada.
- *Firma de la persona entrevistada.*
- *Otros datos previstos en el formulario oficial del EVIN* vigente al momento de la recolección.

Importante: En el caso de menores de edad, la información deberá ser proporcionada exclusivamente por sus representantes legales (padres, tutores o responsables legales), asegurándose se contar con el correspondiente consentimiento informado previo al tratamiento de dichos datos.

El tratamiento de *datos sensibles* se realizará con respeto y estricto apego a los principios de proporcionalidad y necesidad, garantizando su confidencialidad y protección conforme a lo establecido en la Ley Orgánica de Protección de Datos Personales (LOPDP).

En caso de inconsistencias, errores u observaciones, que den lugar a quejas o reclamos por parte de los titulares de los datos personales, estos podrán presentar una solicitud de revisión a través del correo electrónico institucional: atencionciudadana@gestionderiesgos.gob.ec.

7. FINALIDAD DEL TRATAMIENTO

Los datos personales recopilados a través de la aplicación EVIN serán tratados exclusivamente para los siguientes fines:

- Identificar a personas y familias afectadas por emergencias o desastres naturales o antrópicos;
- Evaluar de manera oportuna las necesidades de asistencia humanitaria;
- Planificar, coordinar y ejecutar acciones institucionales, tanto estatales como locales, orientadas a la atención, recuperación y reducción del riesgo;
- Generar estadísticas e informes técnicos que contribuyan al fortalecimiento de la política pública de gestión de riesgos;
- Dar cumplimiento a las obligaciones legales y normativas en el ámbito de la gestión de riesgos y emergencias.
- Atender cualquier otra finalidad que se derive del cumplimiento estricto de las competencias de la Secretaría Nacional de Gestión de Riesgos (SNGR).

8. SEGURIDAD DE LA INFORMACIÓN

La Secretaría Nacional de Gestión de Riesgos (SNGR) implementa medidas técnicas, administrativas y legales para garantizar la seguridad, integridad y confidencialidad de los datos personales, tratados a través del sistema EVIN.

En este marco, los usuarios autorizados deberán cumplir con las siguientes disposiciones:

- *Utilizar exclusivamente dispositivos institucionales* durante el desarrollo del operativo. La autorización para el uso de dichos dispositivos será responsabilidad de los GAD correspondientes, en función de los recursos disponibles.
- *Proteger sus credenciales de acceso*, evitando su divulgación o uso indebido.
- *Abstenerse de almacenar información fuera del sistema EVIN*.
- *No copiar, transferir ni compartir datos personales* con terceros no autorizados, bajo ninguna circunstancia.
- *Reportar de manera inmediata cualquier incidente de seguridad*.

9. CONSERVACIÓN DE LOS DATOS

Los datos personales recopilados serán conservados en los sistemas oficiales, durante el tiempo estrictamente necesario para cumplir con las finalidades del levantamiento de la evaluación inicial de necesidades, en conformidad con la normativa vigente sobre gestión documental, archivos y protección de datos personales.

10. DERECHOS DE LOS TITULARES DE LOS DATOS

Las personas titulares de los datos personales tratados por medio de la aplicación EVIN podrán ejercer los derechos que les reconoce la Ley Orgánica de Protección de Datos Personales (LOPDP), entre ellos:

- Derecho de acceso
- Derecho de rectificación y actualización
- Derecho de eliminación
- Derecho de oposición
- Derecho de portabilidad
- Derecho de suspensión del tratamiento

Las solicitudes para el ejercicio de estos derechos deberán dirigirse a la SNGR, mediante el correo electrónico institucional: atencionciudadana@gestionderiesgos.gob.ec.

11. SANCIONES

El incumplimiento de esta Política por parte de los usuarios podrá derivar en:

- Suspensión o cancelación de las credenciales de acceso;
- Responsabilidad administrativa, civil o penal conforme a la LOPDP y demás normativa aplicable.

La Secretaría Nacional de Gestión de Riesgos se reserva el derecho de iniciar las acciones administrativas, civiles y/o penales que correspondan contra cualquier usuario que haga

un uso indebido de la aplicación o de los datos personales obtenidos mediante el sistema EVIN.

12. MEDIDAS DE SEGURIDAD

Con el fin de garantizar la protección adecuada de los datos personales, se implementarán medidas técnicas y organizativas alineadas con los principios de seguridad de la información.

Medidas Técnicas

1. *Control de acceso*
   - Autenticación robusta (contraseñas seguras, autenticación multifactor).
   - Asignación de permisos bajo el principio de mínimo privilegio.
   - Registro y auditoría de accesos.

2. *Cifrado de datos*
   - Cifrado en tránsito (TLS/SSL) y en reposo (AES-256).
   - Uso de VPN seguras para accesos remotos.

3. *Copias de seguridad*
   - Backups periódicos (diarios o semanales según criticidad de la información).
   - Pruebas regulares de restauración de respaldos.
   - Almacenamiento seguro y cifrado de respaldos.

4. *Actualizaciones y parches*
   - Mantenimiento actualizado de software, sistemas operativos y antivirus.
   - Aplicación oportuna de parches de seguridad.

5. *Protección perimetral y antimalware*
   - Uso de Firewalls, sistemas de detección y prevención de intrusos (IDS/IPS)
   - Soluciones antimalware en todos los dispositivos.

6. *Seguridad en dispositivos*
   - Políticas de bloqueo automático.
   - Cifrado de discos duros en dispositivos portátiles.
   - Control del uso de dispositivos externos (USB, entre otros).

Medidas Organizativas

1. *Políticas de seguridad de la información*
   - Desarrollo y mantenimiento de políticas claras sobre manejo de datos personales.
   - Inclusión de Reglamento de uso aceptable de sistemas y dispositivos.

2. *Gestión de Incidentes*
   - Emisión de procedimiento de respuesta a incidentes de seguridad.
   - Designación de responsables y tiempos de actuación.

3. *Capacitación y concienciación*
   - Formación periódica sobre protección de datos personales y buenas prácticas digitales para los funcionarios.

4. *Confidencialidad y contratos*
   - Inclusión de cláusulas de confidencialidad en contratos con personal y proveedores.
   - Establecimiento de obligaciones de protección de datos en contratos con terceros.

5. *Evaluaciones y auditorías*
   - Ejecución de auditorías internas de seguridad.
   - Evaluaciones de impacto para nuevos sistemas que involucren tratamiento de datos personales.

6. *Inventario de datos y sistemas*
   - Mantenimiento de un inventario actualizado de sistemas y bases de datos que contienen información personal.
   - Clasificación de la información según su nivel de sensibilidad.

13. DECLARACIÓN Y ACEPTACIÓN

El uso de la aplicación EVIN implica que el usuario declara haber leído, comprendido y aceptado íntegramente la presente Política de Privacidad, y se compromete a su cumplimiento en todas las etapas del tratamiento de datos personales.