



POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

Página: 1 de 12

1. OBJETIVO

La presente Política tiene como objetivo establecer los lineamientos internos mediante los cuales INARPI S.A. garantiza el cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP), su Reglamento General, las resoluciones emitidas por la Superintendencia de Datos Personales y demás normativa aplicable en materia de protección de datos, asegurando que todos los datos personales sean tratados de forma lícita, leal, transparente, segura y respetuosa de los derechos fundamentales de los titulares.

2. ALCANCE

INARPI S.A. ejerce el rol de Responsable de Tratamiento respecto de todos los datos personales que trata en el desarrollo de sus actividades como operador del Terminal Portuario de Guayaquil (TPG).

Esta política es de aplicación obligatoria para:

- Todos los colaboradores de INARPI S.A. (personal propio, en todos los niveles jerárquicos).
- Gerentes, Subgerentes, Jefaturas, Supervisores y demás responsables de área.
- Encargados de tratamiento, proveedores, contratistas y terceros que traten datos personales en nombre o por cuenta de INARPI S.A.
- Clientes, usuarios y visitantes cuyos datos son tratados por la Empresa.

3. MARCO LEGAL Y NORMATIVO

La presente política se fundamenta en la siguiente normativa:

- Constitución de la República del Ecuador (Art. 66 numeral 19 y Art. 92).
- Ley Orgánica de Protección de Datos Personales – LOPDP (Ley 459, R.O. Suplemento 459, 26 de mayo de 2021).
- Reglamento General de la Ley Orgánica de Protección de Datos Personales (Decreto Ejecutivo 864, R.O. Suplemento 205, 27 de enero de 2023).
- Resolución N° SPDP-SPD-2026-0005-R – Norma General sobre el Tratamiento de Datos Personales a Gran Escala (MTGE).
- Normas de la Superintendencia de Protección de Datos Personales (SPDP) aplicables.
- Estándares internacionales aplicables: ISO/IEC 27001 e ISO/IEC 27701.

4. RESPONSABILIDADES

La distribución de responsabilidades en materia de protección de datos personales en INARPI S.A. es la siguiente:

CARGO / ROL	RESPONSABILIDADES
GERENTE GENERAL	• Aprobar y suscribir la Política de Protección de Datos Personales. • Asignar los recursos necesarios para la implementación del programa de protección de datos.
DELEGADO DE PROTECCIÓN DE DATOS (DPD)	• Definir, documentar y mantener actualizada la presente política. • Supervisar el cumplimiento de la LOPDP y normativa aplicable. • Atender los requerimientos de los titulares y de la Superintendencia de Datos Personales. • Mantener actualizados el Registro de Actividades de Tratamiento (RAT) y la Matriz de Riesgos. • Coordinar la capacitación y concientización del personal. • Notificar vulneraciones de datos a la autoridad de control.
SUBGERENTE TI	• Implementar y mantener las medidas técnicas de seguridad informática para la protección de datos personales. • Evaluar servicios de terceros y encargados de tratamiento desde la perspectiva tecnológica. • Garantizar el funcionamiento correcto de los sistemas de seguridad (cifrado, control de acceso, MFA, monitoreo).
JEFE INFRAESTRUCTURA DE SOPORTE TI &	• Asegurar la disponibilidad, integridad y confidencialidad de los sistemas que alojan datos personales. • Ejecutar los procedimientos de eliminación segura de datos cuando corresponda. • Gestionar incidentes de seguridad informática con afectación a datos personales.
GERENTE RRHH	• Supervisar que el tratamiento de datos de empleados y candidatos cumpla la LOPDP. • Incluir cláusulas de confidencialidad y protección de datos en los contratos de trabajo. • Gestionar el ciclo de vida completo de los datos del personal (reclutamiento, empleo, desvinculación).
JEFE COMPENSACIONES	• Garantizar el tratamiento adecuado de datos financieros y de nómina. • Notificar al DPD cualquier cambio en los procesos que implique nuevos tratamientos de datos personales.
GERENTE DE SEGURIDAD	• Supervisar el tratamiento de datos en sistemas de videovigilancia, control biométrico y accesos físicos. • Asegurar que el uso de datos biométricos y de sistemas CCTV cumple con la normativa aplicable.

		• Coordinar la respuesta ante incidentes de seguridad física que comprometan datos personales.
SUB GERENTE HSE		• Gestionar el tratamiento de datos de salud ocupacional, historias clínicas y controles de alcohol/drogas conforme a la normativa especial de salud y la LOPDP. • Asegurar que los datos médicos sean tratados con el nivel de confidencialidad requerido para datos sensibles.
GERENTE ADM. & FINANZAS		• Supervisar el tratamiento de datos financieros y crediticios de clientes y proveedores. • Establecer cláusulas de protección de datos en contratos comerciales y con proveedores. • Garantizar el cumplimiento del tratamiento de datos en procesos de facturación, cobranzas y tesorería.
SUB GERENTE COMERCIAL		• Asegurar que el tratamiento de datos de clientes en procesos comerciales (importaciones/exportaciones) cumple con la LOPDP. • Gestionar el consentimiento de clientes para comunicaciones comerciales y de servicio al cliente (SAC).
GERENTE OPERACIONES		• Supervisar el tratamiento de datos de transportistas, conductores y proveedores en procesos operativos (gate, TPAT, etc.). • Notificar al DPD cuando se implementen nuevos sistemas operativos que involucren tratamiento de datos personales.
JEFATURAS SUPERVISORES LAS ÁREAS)	/ (TODAS	• Comunicar la Política de Protección de Datos al personal a su cargo. • Velar por el cumplimiento de esta política en sus respectivas áreas. • Notificar al DPD cualquier tratamiento nuevo o cambio en los procesos existentes.
TODOS COLABORADORES	LOS	• Conocer, cumplir y ejecutar esta política y los procedimientos asociados. • Tratar los datos personales únicamente para los fines autorizados. • Reportar de forma inmediata cualquier incidente o vulneración de seguridad al DPD.
ENCARGADOS TRATAMIENTO / PROVEEDORES TERCEROS	DE /	• Cumplir los lineamientos establecidos en esta política y en el contrato respectivo. • Aplicar medidas de seguridad equivalentes a las de INARPI S.A. • Autorizar auditorías y revisiones dispuestas por INARPI S.A. • Notificar a INARPI S.A. cualquier vulneración dentro de los 2 días de conocida.

5. DEFINICIONES

TÉRMINO	DEFINICIÓN
---------	------------

AVISO PRIVACIDAD	DE	Instrumento mediante el cual se informa al titular sobre los alcances, fines y condiciones del tratamiento de sus datos personales, a efectos de que pueda tomar decisiones informadas.
CONSENTIMIENTO		Manifestación de voluntad libre, específica, informada e inequívoca del titular de los datos personales, que autoriza al responsable su tratamiento.
DATO PERSONAL		Dato que identifica o hace identificable a una persona natural, directa o indirectamente.
DATOS SENSIBLES		Datos relativos a etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, biométricos, genéticos, y aquellos cuyo tratamiento indebido pueda generar discriminación o afectar derechos fundamentales.
DPD		Delegado de Protección de Datos: Persona encargada de informar, supervisar el cumplimiento normativo y actuar como punto de contacto ante la Superintendencia de Datos Personales.
DESTINATARIO		Persona natural o jurídica que ha sido comunicada con datos personales.
ENCARGADO DE TRATAMIENTO	DE	Persona natural o jurídica, pública o privada, que trata datos personales a nombre y por cuenta del responsable de tratamiento.
EVALUACIÓN DE IMPACTO (EIPD)	DE	Proceso para identificar, analizar y gestionar los riesgos que puede conllevar un tratamiento de datos personales para los derechos y libertades del titular.
PSEUDONIMIZACIÓN		Tratamiento de datos personales de manera que ya no puedan atribuirse a un titular específico sin usar información adicional.
RAT		Registro de Actividades de Tratamiento: documento que detalla todos los tratamientos de datos personales realizados por INARPI S.A.
RESPONSABLE DE TRATAMIENTO	DE	Persona natural o jurídica que decide sobre la finalidad y el tratamiento de datos personales. En este caso: INARPI S.A.
TERCERO		Persona natural o jurídica distinta del titular, del responsable, del encargado y de las personas autorizadas para tratar datos bajo autoridad directa del responsable.
TITULAR		Persona natural cuyos datos son objeto de tratamiento.
TRATAMIENTO		Cualquier operación o conjunto de operaciones sobre datos personales: recopilación, registro, organización, conservación, adaptación, modificación, consulta, uso, cesión, comunicación, eliminación o destrucción, entre otros.
VULNERACIÓN DE DATOS	DE	Violación de la seguridad que provoca la destrucción, pérdida, alteración, revelación o acceso no autorizado a datos personales.

6. PRINCIPIOS DEL TRATAMIENTO DE DATOS PERSONALES

INARPI S.A. garantiza que el tratamiento de datos personales se regirá en todo momento por los siguientes principios:

- a) Juridicidad:** Los datos personales se tratarán con estricto apego a la Constitución, los instrumentos internacionales, la LOPDP, su Reglamento y demás normativa aplicable.
- b) Lealtad:** El tratamiento se efectuará de manera leal: los titulares conocerán de forma clara qué datos se recogen, con qué fines y bajo qué condiciones.
- c) Transparencia:** INARPI S.A. ofrecerá información accesible, clara y comprensible sobre el tratamiento de datos, en particular a través de los avisos de privacidad.
- d) Finalidad:** Los datos se recogerán para fines específicos, explícitos y legítimos, y no se tratarán de manera incompatible con dichos fines.
- e) Pertinencia y minimización:** Solo se tratarán los datos adecuados, pertinentes y estrictamente necesarios para la finalidad declarada.
- f) Proporcionalidad:** El tratamiento será adecuado, necesario, relevante y no excesivo en relación con la finalidad perseguida.
- g) Confidencialidad:** Los datos personales no serán utilizados para fines distintos a aquellos para los que fueron recabados, ni divulgados sin autorización.
- h) Calidad y exactitud:** Los datos tratados deberán ser exactos, íntegros, completos, veraces y, cuando sea necesario, actualizados.
- i) Conservación limitada:** Los datos personales se conservarán únicamente durante el tiempo necesario para cumplir con la finalidad del tratamiento y las obligaciones legales aplicables.
- j) Seguridad:** Se implementarán medidas técnicas, organizativas y jurídicas apropiadas para proteger los datos personales frente a accesos no autorizados, pérdida, alteración o destrucción.
- k) Responsabilidad proactiva:** INARPI S.A. acreditará el cumplimiento de estos principios de manera continua, a través de políticas, procedimientos, registros y auditorías.
- l) Aplicación favorable al titular:** En caso de duda, las disposiciones se interpretarán y aplicarán en el sentido más favorable al titular de los datos personales.

7. TIPOS DE DATOS PERSONALES TRATADOS

Conforme al Registro de Actividades de Tratamiento (RAT) de INARPI S.A., la Empresa trata las siguientes categorías de datos personales:

Categoría	Datos
Identificativos:	Nombres y apellidos, documento de identificación, sexo, estado civil, nacionalidad, edad, licencia de conducir, certificado de votación, dirección domiciliaria, correo electrónico personal, número de teléfono y celular, placa de vehículo, RUC, domicilio tributario, razón social
Circunstancias familiares:	Nombres y apellidos de los cónyuges o convivientes en unión de hecho, número de hijos, edad de los hijos menores de edad y discapacidad de los hijos de cualquier edad. Detalles de empleo: Puesto o cargo desempeñado en otras instituciones, ya sean públicas o privadas.

Académicos y Profesionales	Titulaciones, formaciones, experiencia profesional, hoja de vida
Detalles de empleos:	Puesto o cargo desempeñado en otras instituciones, ya sean públicas o privadas.
De control de presencia y seguridad	Fecha y hora de entrada y salida al lugar de trabajo, imágenes de cámaras de seguridad y datos de geolocalización
Financieros	Datos del banco al cual será depositado su remuneración beneficio de ley y utilidades, número de cuenta de la empresa, estados de cuenta, banco, tipo de cuenta, otros.
Categorías especiales:	Condición migratoria, datos de salud física y mental, datos biométricos, huella dactilar, imagen de rostro, GPS.
Información Comercial:	Actividades y negocio, licencias comerciales, suscripciones a medios de comunicación, publicaciones, creación artística, literaria, científica
Judiciales y administrativos	Procedimientos administrativos, reclamaciones y recursos, sanciones, registros, solicitudes, expediente o historial judicial, y procedimientos judiciales, antecedentes penales, demandas, denuncias, y sentencias penales, etc.

8. TRATAMIENTO DE DATOS PERSONALES

8.1 Avisos de Privacidad

INARPI S.A. informará al titular, con carácter previo o en el momento de la recolección de sus datos, mediante el Aviso de Privacidad correspondiente. Cada aviso deberá contener como mínimo:

- Identidad y datos de contacto del responsable (INARPI S.A.) y, en su caso, del DPD.
- Los fines específicos del tratamiento y la base legal que lo justifica.
- Tipos de datos tratados y fuentes de obtención.
- La existencia de una base de datos en la que constan sus datos personales;
- El origen de los Datos Personales cuando no se hayan obtenido directamente del titular;
- Plazo de conservación previsto.

- Destinatarios o categorías de destinatarios a quienes se comunicarán los datos.
- Transferencias nacionales o internacionales previstas y garantías establecidas.
- Derechos del titular (acceso, rectificación, supresión, oposición, limitación, portabilidad, a no ser objeto de decisiones automatizadas) y cómo ejercerlos.
- Mecanismo de reclamación ante INARPI S.A. y ante la Superintendencia de Datos Personales.
- Posibilidad de revocar el consentimiento cuando el tratamiento se base en este.
- Existencia de decisiones automatizadas o elaboración de perfiles, en su caso.

8.2 Bases Legales y Consentimiento

INARPI S.A. tratará datos personales únicamente cuando exista una base legal habilitante, que puede ser:

- El consentimiento libre, específico, informado e inequívoco del titular.
- La ejecución de una relación contractual o laboral con el titular.
- El cumplimiento de una obligación legal o reglamentaria.
- La protección de intereses vitales del titular o de un tercero.
- Datos personales que consten en una base de datos de acceso público.
- El interés legítimo de la Empresa, siempre que sea proporcional y justificado.

Para datos sensibles, el tratamiento requerirá consentimiento explícito del titular u otra excepción legalmente prevista (obligación laboral, protección de intereses vitales, datos manifiestamente públicos, mandato judicial, fines de salud pública o investigación científica).

Cuando los datos no se obtengan directamente del titular, este será informado dentro de los treinta (30) días siguientes a la obtención o en la primera comunicación que se establezca con él, lo que ocurra primero.

Para el tratamiento de datos personales, se atenderán las siguientes reglas:

1. Las áreas que recaban Datos Personales deben obtener el Consentimiento del Titular para el uso de sus datos personales a través del Aviso de Privacidad, bien sea escrito o en electrónico, pero siempre resguardando prueba que respalde la obtención del consentimiento.
2. El Aviso de Privacidad, revisado por el Delegado de Protección de Datos (DPD), es el que se dará a conocer al Titular.
3. Cuando los Datos Personales no se obtuvieren de forma directa del titular o fueren obtenidos de una fuente accesible al público, el Titular deberá ser informado por el dueño del Proceso, dentro de los siguientes treinta (30) días o al momento de la primera comunicación con el Titular, cualquiera de las dos circunstancias que ocurra primero.

8.3 Uso y Tratamiento

- Las áreas solo recabarán los datos estrictamente necesarios para los fines declarados (principio de minimización).
- Queda prohibido el uso de datos personales para finalidades distintas a las informadas al titular, salvo que concurran los siguientes casos:
 - El titular haya dado su consentimiento explícito para el tratamiento de sus datos personales, especificándose claramente sus fines.
 - El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del titular en el ámbito del Derecho laboral y de la seguridad y protección social.

- El tratamiento es necesario para proteger intereses vitales del titular o de otra persona natural, en el supuesto de que el titular no esté capacitado, física o jurídicamente, para dar su consentimiento.
 - El tratamiento se refiere a datos personales que el titular ha hecho manifiestamente públicos.
 - El tratamiento se lo realiza por orden de autoridad judicial.
 - El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular.
 - Cuando el tratamiento de los datos de salud se sujete a las disposiciones contenidas en la LOPDP.
- La documentación física con datos personales deberá ser almacenada bajo llave por el responsable del proceso correspondiente.
 - La información digital solo se almacenará en los sistemas y plataformas autorizados por la política de Seguridad de la Información de INARPI S.A. (sistemas de gestión corporativa, servidores internos y servicios en la nube aprobados).
 - El tratamiento de datos biométricos (Art. 25 LOPDP) se limitará a las finalidades de control de acceso físico y registro de asistencia, con el consentimiento expreso del titular o la base legal correspondiente.
 - Los datos de videovigilancia (CCTV con IA) se tratarán conforme al Art. 25 LOPDP, y se informará mediante carteles visibles en las zonas monitoreadas.
 - Las pruebas psicotécnicas aplicadas a candidatos constituyen tratamiento de perfilamiento (Art. 25 LOPDP) y requerirán el consentimiento informado del evaluado.

9. CONTRATOS Y ACUERDOS DE TRATAMIENTO

9.1 Encargados de Tratamiento y Terceros

Previamente a toda transferencia de datos personales a un encargado de tratamiento o tercero, INARPI S.A. formalizará un contrato o cláusula contractual que deberá contener:

- Objeto, duración y naturaleza del tratamiento encomendado.
- Finalidad del tratamiento y categorías de datos personales involucrados.
- Identificación de los titulares cuyos datos serán tratados.
- Obligaciones y responsabilidades del encargado, incluyendo la prohibición de sublicenciar el tratamiento sin autorización escrita de INARPI S.A.
- Medidas de seguridad técnicas y organizativas que el encargado deberá implementar.
- Obligación de eliminación o devolución de los datos al término de la relación, con certificado de borrado seguro (estándar DoD 5220.22-M, DIN 66399 o equivalente).
- Obligación de notificar cualquier vulneración de seguridad dentro de los dos (2) días de conocida.
- Habilitación a INARPI S.A. para realizar auditorías y controles.

La Transferencia de Datos Personales solamente se realizarán si:

- a.** INARPI S.A. cuenta con el consentimiento del Titular por escrito;
- b.** Los Encargados de Tratamiento y Terceros que cumplan con la LOPDP; y,
- c.** Los Encargados de Tratamiento y Terceros tienen implementado estándares internacionales o mejores prácticas de Seguridad de la Información, las mismas que deberán ser presentadas ante INARPI S.A. y evaluadas respectivamente.

Una vez validada lo anterior, el Delegado de Protección de Datos (DPD) aprobará la Transferencia de Datos Personales.

El Encargado de Tratamiento y Tercero deberán aplicar los mecanismos necesarios para la ejecución del borrado seguro de información, ya sea lógica o física (Por ejemplo, se recomienda aplicar métodos como el estándar DoD 5220.22-M o la norma DIN 66399 para garantizar la eliminación segura) y entregará a INARPI S.A. la evidencia o certificados de eliminación de los Datos Personales, una vez culminada su relación comercial, a través de un comunicado remitido de forma física o a través de correo o medios electrónicos, con la firma del representante legal.

9.2 Clientes y Proveedores

Los contratos comerciales y de provisión de servicios incluirán cláusulas específicas de protección de datos personales, garantizando el tratamiento legítimo de la información y la confidencialidad de los datos intercambiados.

9.3 Contratos Laborales

Los contratos de trabajo de todos los colaboradores incluirán obligatoriamente cláusulas de protección de datos personales y confidencialidad de la información, adaptadas al cargo y a los datos que el colaborador manejará en el ejercicio de sus funciones.

9.4 Transferencias Internacionales

Toda transferencia internacional de datos personales requerirá que el destinatario garantice un nivel de protección equivalente al establecido por la LOPDP. INARPI S.A. implementará las garantías adecuadas (cláusulas contractuales tipo, certificaciones reconocidas o declaración de nivel adecuado de protección) y obtendrá el consentimiento expreso del titular cuando la ley así lo exija. El DPD validará toda transferencia internacional antes de su ejecución.

10. CONSERVACIÓN Y ELIMINACIÓN DE DATOS

Los datos personales se conservarán únicamente durante el tiempo necesario para cumplir la finalidad para la que fueron recabados, respetando los siguientes criterios generales:

- Datos de empleados (expediente, nómina, contratos): 7 años contados desde la terminación de la relación laboral, o el plazo que determine la normativa laboral o tributaria aplicable, el que sea mayor.
- Datos médicos ocupacionales e historias clínicas: conforme a la normativa del Ministerio de Salud Pública y del IESS.
- Datos biométricos: durante la vigencia de la relación laboral o comercial y hasta la finalización de los procesos de desvinculación y eliminación segura.
- Datos de videovigilancia (CCTV): máximo 30 días calendario, salvo que exista una investigación o proceso legal activo que justifique una conservación mayor.
- Datos de candidatos no seleccionados: máximo 2 años, salvo consentimiento expreso del candidato para conservación prolongada.
- Datos de clientes y proveedores: 7 años desde el último servicio prestado o conforme a obligaciones tributarias y comerciales aplicables.

Una vez vencidos los plazos de conservación, los datos serán eliminados de forma segura, aplicando métodos de borrado certificado para soportes digitales (DoD 5220.22-M o norma DIN 66399) y destrucción física controlada para soportes físicos.

Los plazos específicos por tipo de tratamiento se detallan en el Registro de Actividades de Tratamiento (RAT) y en el Manual de Políticas de Seguridad de la Información de INARPI S.A.

11. PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO

INARPI S.A. incorporará la protección de datos personales como un requisito desde las fases iniciales del diseño de cualquier nuevo proceso, sistema, producto o servicio que implique tratamiento de datos personales. Para ello, aplicará las siguientes medidas:

- Reducción al máximo de los datos personales tratados (minimización).
- Pseudonimización de datos personales en cuanto resulte técnicamente viable.
- Implementación de controles de acceso restrictivos por defecto (necesidad de saber / mínimo privilegio).
- Transparencia en el tratamiento: los titulares serán informados de forma proactiva.
- Realización de Evaluaciones de Impacto (EIPD) cuando se identifiquen tratamientos de alto riesgo o que superen el umbral del MTGE.
- Consulta previa al DPD antes de la implementación de nuevas tecnologías que impliquen tratamiento de datos personales.

12. EVALUACIÓN DE IMPACTO DE PROTECCIÓN DE DATOS (EIPD)

INARPI S.A. realizará una Evaluación de Impacto de Protección de Datos cuando:

- El tratamiento sea calificado como Gran Escala conforme al MTGE.
- Se realice monitoreo sistemático de zonas de acceso público (videovigilancia con IA).
- Se traten datos sensibles de categorías especiales (Art. 25 LOPDP) a gran escala.
- Se implementen nuevas tecnologías que impliquen alto riesgo para los derechos del titular.
- La Superintendencia de Datos Personales lo requiera expresamente.

La EIPD será supervisada por el DPD e incluirá: descripción del tratamiento, evaluación de necesidad y proporcionalidad, evaluación de riesgos para los titulares, y medidas previstas para mitigar dichos riesgos.

13. DERECHOS DE LOS TITULARES

INARPI S.A. facilitará el ejercicio de los siguientes derechos de los titulares de datos personales, de conformidad con los Arts. 12 al 22 de la LOPDP:

- **Acceso:** El titular podrá solicitar confirmación de si sus datos son tratados y obtener una copia de los mismos.
- **Rectificación:** El titular podrá solicitar la corrección de datos inexactos o incompletos.
- **Supresión / Eliminación:** El titular podrá solicitar la eliminación de sus datos cuando ya no sean necesarios, cuando el tratamiento sea ilícito o cuando retire su consentimiento.

- **Oposición:** El titular podrá oponerse al tratamiento de sus datos basado en interés legítimo o con fines de marketing directo.
- **Limitación del tratamiento:** El titular podrá solicitar la suspensión del tratamiento en tanto se resuelva una controversia sobre exactitud o licitud.
- **Portabilidad:** El titular podrá recibir sus datos en formato estructurado, de uso común y lectura mecánica, o solicitar su transmisión a otro responsable.
- **No ser objeto de decisiones automatizadas:** El titular podrá oponerse a ser objeto de decisiones basadas únicamente en tratamientos automatizados, incluida la elaboración de perfiles.
- **Revocación del consentimiento:** El titular podrá revocar en cualquier momento su consentimiento, sin que ello afecte la licitud del tratamiento previo a la revocación.

Los titulares podrán ejercer sus derechos mediante solicitud escrita dirigida al Delegado de Protección de Datos (DPD) de INARPI S.A. al correo electrónico: protecciondatos@tpg.com.ec o en las oficinas de la Empresa. INARPI S.A. atenderá las solicitudes dentro del plazo máximo de quince (15) días establecido por la LOPDP.

14. GESTIÓN DE VULNERACIONES DE SEGURIDAD

Ante cualquier vulneración de seguridad que afecte datos personales, INARPI S.A. aplicará el siguiente protocolo:

- Los encargados de tratamiento deberán notificar a INARPI S.A. cualquier vulneración dentro de las 48 horas de conocida.
- Cualquier colaborador que detecte o sospeche de una vulneración deberá notificarlo de inmediato al DPD y al Subgerente TI.
- El DPD notificará a la Superintendencia de Datos Personales y a ARCOTEL dentro de los cinco (5) días hábiles siguientes a tener constancia de la vulneración, salvo que sea improbable que constituya riesgo para los titulares.
- El DPD notificará a los titulares afectados dentro de los tres (3) días siguientes al conocimiento del riesgo, cuando la vulneración conlleve un riesgo para sus derechos y libertades fundamentales.

La notificación de vulneración deberá contener:

- Naturaleza y tipo de vulneración.
- Identificación de los titulares o categorías de titulares afectados.
- Detalle de los sistemas comprometidos.
- Causa presunta de la vulneración.
- Volumen y tipos de datos expuestos o comprometidos.
- Medidas adoptadas y previstas para la contención y remediación.
- Evaluación del riesgo que representa la vulneración para los derechos de los titulares.
- Cualquier otro aspecto requerido por la Superintendencia de Datos Personales.

15. MEDIDAS DE SEGURIDAD

INARPI S.A. se compromete a implementar medidas de seguridad técnicas, organizativas y administrativas de vanguardia para salvaguardar la confidencialidad, integridad y disponibilidad de los datos personales, protegiéndolos contra accesos no autorizados, pérdida, alteración o destrucción.

INARPI S.A. asegura la estricta observancia de estas medidas por parte de sus responsables y encargados del tratamiento. Todas las acciones se alinearán con:

- El estado actual de la técnica (estándares internacionales de ciberseguridad y seguridad de la información).
- La normativa técnica emitida por la Autoridad de Protección de Datos Personales.

16. CAPACITACIÓN Y CONCIENTIZACIÓN

INARPI S.A. implementará un programa anual de capacitación y concientización sobre protección de datos personales, dirigido a todos los colaboradores, con especial énfasis en aquellos que tratan datos sensibles o que tienen acceso a sistemas críticos. El programa incluirá:

- Capacitación inicial obligatoria para nuevos ingresos.
- Sesiones periódicas de actualización (mínimo una vez al año).
- Formación especializada para el DPD y para las áreas con tratamientos de alto riesgo (RRHH, HSE, Seguridad, TI).
- Difusión de la presente política y de los procedimientos relacionados a través de los canales internos de comunicación.

El DPD, con apoyo del área de RRHH (Jefe de Desarrollo Organizacional), coordinará el diseño, ejecución y evaluación del programa de capacitación.

17. RELACIÓN CON LA SUPERINTENDENCIA DE DATOS PERSONALES

INARPI S.A. atenderá con plena colaboración y dentro de los plazos establecidos por la ley todas las visitas de inspección, solicitudes de información, requerimientos de investigación y sanciones que disponga la Superintendencia de Datos Personales.

El DPD actuará como punto de contacto oficial entre INARPI S.A. y la Superintendencia de Datos Personales, coordinando la respuesta institucional con las áreas involucradas.

18. MEDIDAS CORRECTIVAS Y SANCIONES INTERNAS

El incumplimiento de las disposiciones de esta política por parte de los colaboradores de INARPI S.A. será objeto de medidas correctivas conforme al Reglamento Interno de Trabajo y al Código de Ética de la Empresa, pudiendo incluir:

- Llamado de atención escrito.
- Capacitación obligatoria.
- Restricción o suspensión del acceso a sistemas de información.

- Sanción disciplinaria según la gravedad del incumplimiento.
- Terminación del contrato en los casos de incumplimiento grave o reiterado.

Los incumplimientos por parte de encargados de tratamiento, proveedores o terceros darán lugar a la resolución del contrato y a las acciones legales que correspondan.

19. REVISIÓN, CUMPLIMIENTO Y DIVULGACIÓN

- Esta política será revisada y actualizada por el DPD al menos una vez al año o cuando se produzcan cambios relevantes en la legislación, en los tratamientos de datos o en la estructura organizativa de INARPI S.A.
- Toda modificación sustancial deberá ser aprobada por el Gerente General.
- INARPI S.A. divulgará esta política a todos los colaboradores, encargados de tratamiento y terceros relevantes, manteniéndola disponible en los canales internos de comunicación.
- Para consultas sobre esta política o para ejercer derechos como titular, contactar al DPD: protecciondatos@tpg.com.ec.