# Política de protección de datos personales.

# International Mobile Services.

**Fecha de emisión: 26 de marzo del 2026.**
**Versión 1.0.**
**Aprobado por Gerencial General.**

## 1.) Objetivo

La presente Política de Protección de Datos Personales tiene como objetivo establecer los lineamientos, principios y responsabilidades para garantizar la adecuada gestión, protección, confidencialidad e integridad de los datos personales tratados por la organización, así como identificar, evaluar y mitigar los riesgos asociados a su tratamiento.

## 2.) Alcance y Base del Programa.

Esta política aplica a todos los colaboradores, proveedores, contratistas y terceros que tengan acceso o traten datos personales en nombre de la organización.
El programa de protección de datos se fundamenta en:

- La normativa legal aplicable en materia de protección de datos.
- Los hallazgos identificados en los procesos de debida diligencia.
- Evaluaciones internas periódicas de riesgos.

## 3.) Definiciones

Para efectos de esta política, se entenderá por:

- Datos Personales: Información que identifica o puede identificar a una persona física.

- Tratamiento de Datos: Cualquier operación realizada sobre datos personales (recolección, almacenamiento, uso, transferencia, etc.).
- Titular: Persona a la que pertenecen los datos personales.
- Responsable del Tratamiento: Entidad que decide sobre el tratamiento de los datos.
- Encargado del Tratamiento: Persona o entidad que trata datos por cuenta del responsable.

**4.) <u>Personal Encargado de la Privacidad.</u>**

Se designa un responsable de protección de datos (DPO o encargado interno), quien tendrá las siguientes funciones:

- Supervisar el cumplimiento de esta política.
- Asesorar en materia de privacidad.
- Gestionar incidentes de seguridad.
- Coordinar auditorías y evaluaciones de riesgo.
- Ser punto de contacto para consultas y denuncias por medio del correo: dataprotectionmanager@ims.do

**5.) <u>Protección de Datos por Diseño y por Defecto.</u>**

La organización adopta el principio de Protección de Datos por Diseño y por Defecto, integrando medidas de privacidad y seguridad desde las etapas iniciales de diseño, desarrollo, implementación y operación de todos los procesos, sistemas y servicios que involucren el tratamiento de datos personales.

Esto implica que, antes de iniciar cualquier tratamiento de datos, se deberán identificar los riesgos asociados y establecer controles adecuados para mitigarlos, garantizando que, por defecto, únicamente se traten los datos estrictamente necesarios para cada finalidad específica.

Asimismo, los sistemas y procesos deberán configurarse de manera que, sin intervención del usuario, se asegure el nivel más alto de privacidad posible, limitando el acceso, la recopilación y la exposición de datos personales.

**Medidas implementadas**

**a.) Medidas Físicas**

Se implementan controles orientados a proteger los soportes físicos y las instalaciones donde se almacena o procesa información:

- Control de acceso restringido a instalaciones mediante mecanismos de identificación (tarjetas, biometría, llaves u otros).
- Registro y monitoreo de entradas y salidas de personal y visitantes.
- Resguardo seguro de documentos físicos en archivadores cerrados o áreas protegidas.
- Políticas de escritorio limpio para evitar la exposición de información sensible.
- Eliminación segura de documentos mediante trituración o métodos equivalentes.
- Protección contra riesgos ambientales (incendios, inundaciones, etc.) cuando aplique.

**b.) Medidas Técnicas**

Se establecen controles tecnológicos para garantizar la seguridad de los datos en sistemas informáticos:

- Encriptación de datos personales tanto en tránsito como en reposo.
- Implementación de mecanismos de autenticación robusta (contraseñas seguras, autenticación multifactor, etc.).
- Control de accesos basado en roles y privilegios mínimos necesarios.
- Registro de accesos y actividades (logs) para trazabilidad y auditoría.
- Copias de seguridad periódicas con pruebas de restauración.
- Monitoreo continuo de sistemas para detectar accesos no autorizados o comportamientos anómalos.
- Actualización y parcheo regular de sistemas y aplicaciones.
- Uso de antivirus, firewalls y herramientas de protección perimetral.

- Anonimización de datos cuando sea posible.
- Segmentación de redes para proteger información crítica.

**c.) Medidas Organizativas**

Se establecen prácticas y políticas internas para asegurar una gestión adecuada de la información:

- Definición de políticas internas de acceso y manejo de datos personales.
- Clasificación de la información según su nivel de sensibilidad (pública, interna, confidencial, restringida).
- Firma de acuerdos de confidencialidad por parte de empleados y terceros.
- Evaluaciones de riesgo periódicas en materia de protección de datos.
- Evaluaciones de impacto en privacidad (cuando aplique) antes de nuevos proyectos o cambios relevantes.
- Capacitación continua del personal en protección de datos y seguridad de la información.
- Procedimientos documentados para el tratamiento de datos personales.
- Gestión de proveedores que traten datos, asegurando que cumplan con estándares de seguridad.
- Designación de responsables para la supervisión del cumplimiento.

La organización revisará y actualizará estas medidas de forma periódica para adaptarse a cambios tecnológicos, regulatorios y a nuevos riesgos identificados.

## 6.) Tratamiento de Datos Personales

El tratamiento de datos personales dentro de la organización deberá realizarse conforme a principios de legalidad, transparencia y responsabilidad, garantizando en todo momento la protección de los derechos de los titulares de los datos.

Todo tratamiento deberá estar debidamente justificado, documentado y alineado con las finalidades previamente definidas por la organización.

Lineamientos generales

El tratamiento de datos personales deberá cumplir con los siguientes criterios:

- Obtención de consentimiento previo, expreso e informado: Antes de recolectar cualquier dato personal, se deberá contar con la autorización del titular, la cual deberá ser libre, específica, informada e inequívoca. El titular deberá conocer claramente qué datos se recopilan, con qué finalidad y cómo serán utilizados.
- Uso de datos para fines específicos, legítimos y definidos: Los datos personales solo podrán ser utilizados para los fines previamente establecidos y comunicados al titular. Queda prohibido el uso de los datos para finalidades distintas sin contar con una nueva autorización.
- Limitación del tratamiento a lo estrictamente necesario: Se deberán recolectar y tratar únicamente aquellos datos que sean adecuados, pertinentes y no excesivos en relación con la finalidad para la cual se obtienen, evitando la recopilación innecesaria de información.
- Autorización documentada cuando aplique: Toda autorización otorgada por el titular deberá quedar registrada por medios físicos o electrónicos, de manera que pueda ser consultada en caso de auditoría o requerimiento legal.
- Los datos personales deberán mantenerse actualizados y ser exactos en la medida de lo posible.
- Se deberán establecer mecanismos para que los titulares puedan ejercer sus derechos de acceso, rectificación, cancelación y oposición (cuando aplique).
- El tratamiento deberá realizarse bajo condiciones de seguridad que garanticen la confidencialidad e integridad de la información.
- El acceso a los datos estará restringido únicamente al personal autorizado y en función de sus responsabilidades.
- En caso de transferencia de datos a terceros, se deberá asegurar que estos cumplan con estándares adecuados de protección de datos y exista un acuerdo formal que regule dicho tratamiento.

- Los datos personales no deberán conservarse por más tiempo del necesario para cumplir con la finalidad para la cual fueron recolectados, salvo obligación legal.

## 7.) Condiciones del Tratamiento

La organización garantizará que todo tratamiento de datos personales se realice bajo condiciones que aseguren su adecuada protección durante todo su ciclo de vida, desde la recolección hasta su eliminación.

Para ello, se deberán implementar controles y buenas prácticas orientadas a preservar la confidencialidad, seguridad, integridad y disponibilidad de la información.

**Condiciones fundamentales:**

- **Confidencialidad**:

  Los datos personales no serán divulgados, compartidos ni accesados por personas no autorizadas.

  El acceso a la información estará limitado estrictamente al personal que lo requiera para el cumplimiento de sus funciones.

  Asimismo, todos los colaboradores y terceros con acceso a datos deberán suscribir acuerdos de confidencialidad y cumplir con las políticas internas establecidas.

- **Seguridad**:

  Se implementarán medidas técnicas, físicas y organizativas adecuadas para proteger los datos personales contra accesos no autorizados, pérdida, destrucción o divulgación indebida.

  Estas medidas incluirán controles de acceso, autenticación, monitoreo de sistemas, protección perimetral, y gestión de vulnerabilidades, entre otros.

- **Integridad**:

  La organización garantizará que los datos personales se mantengan completos, exactos y sin alteraciones no autorizadas.

Se establecerán mecanismos de validación, control de cambios y trazabilidad que permitan identificar modificaciones y asegurar la calidad de la información.

- **Disponibilidad**:
  Los datos personales deberán estar accesibles para su uso cuando sea necesario y por personal autorizado.
  Para ello, se implementarán medidas como copias de seguridad, planes de recuperación ante desastres y continuidad del negocio, que permitan restablecer el acceso a la información en caso de incidentes.
- Se deberán aplicar controles de seguridad proporcionales al nivel de sensibilidad de los datos tratados.
- Los sistemas que procesen datos personales deberán ser evaluados periódicamente para identificar vulnerabilidades.
- Se deberá mantener un registro de accesos y actividades sobre los datos personales para fines de auditoría.
- En caso de incidentes de seguridad, se deberán activar los protocolos correspondientes para su gestión y mitigación.
- La eliminación de datos personales deberá realizarse de forma segura, evitando su recuperación no autorizada.

## 8.) Principios de Privacidad

La organización rige el tratamiento de datos personales conforme a los siguientes principios fundamentales, los cuales orientan todas las actividades relacionadas con la recolección, uso, almacenamiento y eliminación de la información:

- **Licitud**:
  El tratamiento de datos personales se realizará conforme a la normativa aplicable, garantizando que exista una base legal válida para su procesamiento, como el consentimiento del titular u otra condición legítima establecida por la ley.

- **Lealtad**:
  Los datos personales serán tratados de manera justa y ética, evitando prácticas engañosas, abusivas o contrarias a los intereses del titular. La organización actuará de buena fe en todo momento.
- **Transparencia**:
  Se proporcionará a los titulares información clara, accesible y comprensible sobre el tratamiento de sus datos personales, incluyendo las finalidades, responsables y derechos que les asisten.
- **Minimización de datos**:
  Solo se recopilarán y tratarán los datos personales estrictamente necesarios para cumplir con las finalidades establecidas, evitando la recolección excesiva o innecesaria de información.
- **Exactitud**:
  Los datos personales deberán ser exactos, completos y actualizados. Se adoptarán medidas razonables para rectificar o suprimir aquellos datos que sean inexactos o estén desactualizados.
- **Limitación del plazo de conservación**:
  Los datos personales serán conservados únicamente durante el tiempo necesario para cumplir con las finalidades para las cuales fueron recolectados o mientras exista una obligación legal que lo justifique. Una vez cumplido dicho plazo, los datos serán eliminados o anonimizados de manera segura.
- **Responsabilidad proactiva**:
  La organización asume la responsabilidad de cumplir con estos principios y de poder demostrar dicho cumplimiento en todo momento, mediante la implementación de políticas, controles, auditorías y mecanismos de mejora continua.

## 9.) Protocolo de Atención a Incidentes

La organización establece el presente protocolo para la gestión oportuna y efectiva de incidentes de seguridad que involucren datos personales, tales como fugas, pérdidas, accesos no autorizados, alteraciones o cualquier otro evento que comprometa la confidencialidad, integridad o disponibilidad de la información.

Este protocolo tiene como finalidad minimizar el impacto del incidente, proteger a los titulares de los datos y asegurar el cumplimiento de las obligaciones legales y regulatorias aplicables.

### 9.1 Definición de incidente

Se considerará incidente de seguridad cualquier evento que:

- Comprometa o pueda comprometer datos personales.
- Vulnere los controles de seguridad establecidos.
- Genere riesgo para los derechos y libertades de los titulares.

### 9.2 Procedimiento de atención

En caso de detectarse un incidente, se deberán seguir las siguientes etapas:

1. **Identificación del incidente**:

   Detectar y reportar de manera inmediata cualquier evento sospechoso o confirmado que afecte la seguridad de los datos.

   Todo el personal está obligado a notificar cualquier incidente al responsable de protección de datos o al área correspondiente.

2. **Contención inmediata**:

   Adoptar medidas urgentes para limitar el alcance del incidente, tales como:

   - Bloqueo de accesos comprometidos.
   - Desconexión de sistemas afectados.
   - Suspensión temporal de operaciones relacionadas.

3. **Evaluación del impacto**:

   Analizar la naturaleza y alcance del incidente, incluyendo:

   - Tipo de datos comprometidos.
   - Número de titulares afectados.

- Nivel de sensibilidad de la información.
- Posibles consecuencias para los titulares.

4. **Notificación a autoridades y titulares**:

   Cuando corresponda, se deberá notificar:

   - A las autoridades regulatorias dentro de los plazos establecidos por la normativa aplicable.
   - A los titulares de los datos afectados, proporcionando información clara sobre el incidente, sus posibles efectos y las medidas adoptadas.

5. **Documentación del incidente**:

   Registrar de manera detallada toda la información relacionada con el incidente, incluyendo:

   - Fecha y hora de detección.
   - Descripción del evento.
   - Sistemas y datos afectados.
   - Acciones realizadas.
   - Resultados de la investigación.

6. **Implementación de medidas correctivas**:

   Definir y aplicar acciones para evitar la recurrencia del incidente, tales como:

   - Mejora de controles de seguridad.
   - Actualización de políticas y procedimientos.
   - Capacitación adicional al personal.
   - Refuerzo de monitoreo y auditoría.

**9.3 Seguimiento y mejora continua**

Posterior a la gestión del incidente, la organización deberá:

- Realizar un análisis de causa raíz.
- Evaluar la efectividad de la respuesta.
- Actualizar los controles de seguridad según los hallazgos.
- Incorporar mejoras en los procesos internos.

---

**10.) Canal de Denuncias**

La organización dispone de un canal confidencial para reportar incumplimientos:

- Correo electrónico: denuncias@ims.do
- Canal interno o plataforma designada https://www.ims.do/denuncias/page.html

Se garantiza la confidencialidad y no represalias.

**11.) Régimen Sancionador**

El incumplimiento de esta política podrá dar lugar a:

- Sanciones disciplinarias internas.
- Terminación de contratos.
- Acciones legales conforme a la normativa aplicable.

**12.) Supervisión y Verificación**

Se realizarán auditorías periódicas para verificar el cumplimiento de esta política:

- Evaluaciones internas.
- Auditorías externas (cuando aplique).
- Revisión continua de controles.

**13.) Capacitación y Difusión**

Todos los colaboradores deberán recibir capacitación en protección de datos:

- Inducción inicial.
- Capacitación periódica.
- Actualizaciones ante cambios normativos.

Esta política ha sido aprobada por la dirección de la organización y es de cumplimiento obligatorio.

Este documento es aprobado por la Gerencial General de IMS.

CARLOS LUIS POLONIO LOBO (FIRMA)

Digitally signed by CARLOS LUIS POLONIO LOBO (FIRMA)
Date: 2026.04.08 17:15:23 -06'00'

Nombre: Carlos Luis Polonio Lobo.

Cargo: Gerente General

International Mobile Services

Fecha: 26 de marzo del 2026.