PERTIGA GRUPO EMPRESARIAL	**POLÍTICA INTERNA DE PROTECCIÓN DE DATOS PERSONALES**	**CÓDIGO:** PER-PDP-SOP-001
Revisión N°: 01	**PROCEDIMIENTO OPERATIVO ESTANDAR**	**Fecha de elaboración:** 9/06/2026

Elaborado por

Nombre: Torres Padilla Christian Andrés

CARGO: Analista de Gestión de Calidad y Procesos

Christian Andres Torres Padilla
Time Stamping Security Data

Firma / Fecha

Revisado por

Nombre: Ab. Villarroel González María Victoria

En calidad de revisión y conformidad técnica respecto al cumplimiento de la Ley Orgánica de Protección de Datos Personales.

CARGO: Delegada Protección de Datos

Maria Victoria Villarroel Gonzalez
Time Stamping Security Data

Firma / Fecha

Aprobado por

Nombre: Carrera Folleco Carolina de los Ángeles

CARGO: Gerente General

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
CAROLINA DE LOS ANGELES CARRERA FOLLECO

Firma / Fecha

Aceptación de Términos y Condiciones

Confirmo que he leído, comprendido y aceptado los términos y condiciones descritos en este documento. Declaro mi aceptación de estos términos de manera libre y consciente, habiendo revisado y considerado la información proporcionada como adecuada y suficiente para mi comprensión. Además, autorizo que la información proporcionada pueda ser utilizada en las siguientes empresas:

Dirpreleg ☐ Acurio & Asociados Expertos en valor ☒ atrumsit ☐ cuanto Empresa de avalúos ☐

1. OBJETO

La presente política tiene por objeto establecer las directrices internas para garantizar el correcto tratamiento de datos personales en cumplimiento de la Ley Orgánica de Protección de Datos Personales del Ecuador, garantizando los derechos de los titulares y la seguridad de la información.

Esta Política define los principios, roles, responsabilidades, categorías de datos, finalidades, bases legitimadoras, reglas de conservación, medidas de seguridad, lineamientos para encargados y terceros, gestión de derechos, gestión de incidentes, transferencias, privacidad desde el diseño, capacitación, auditoría y régimen interno de cumplimiento.

2. ALCANCE

Esta política es de cumplimiento obligatorio para:

Sujetos obligados	Alcance de la obligación
Directivos y representantes	Deben aprobar, promover, financiar y supervisar el sistema de protección de datos personales.
Trabajadores y colaboradores	Deben tratar datos únicamente para fines autorizados y conforme a esta Política.
Líderes de proceso	Deben mantener actualizados los tratamientos de datos personales de su área y asegurar la ejecución de controles.
Delegada de Protección de Datos	Debe supervisar, coordinar y actuar como punto de contacto en materia de protección de datos.
Proveedores, consultores y peritos externos	Deben cumplir obligaciones contractuales de confidencialidad, seguridad y tratamiento autorizado.
Encargados del tratamiento	Deben tratar datos por cuenta de la Compañía únicamente bajo instrucciones documentadas.
Terceros autorizados	Deben recibir o tratar datos solo cuando exista base legal, contractual o autorización válida.

3. DEFINICIONES

- **Dato personal:** Información que identifica o hace identificable a una persona natural directa o indirectamente.
- **Dato personal sensible:** Dato que, por su naturaleza, puede afectar derechos o libertades del titular y requiere protección reforzada, como datos de salud, biométricos, origen étnico, convicciones, entre otros, cuando corresponda.
- **Titular:** Persona a quien pertenecen los datos.
- **Responsable del tratamiento:** INGENIERÍA PARA EL DESARROLLO ACURIO Y ASOCIADOS S.A.
- **Encargado del tratamiento:** Persona natural o jurídica que trata datos personales por cuenta de la Compañía y bajo sus instrucciones.
- **Tratamiento:** Cualquier operación sobre datos personales, incluyendo recolección, registro, organización, conservación, consulta, uso, análisis, transferencia, comunicación, archivo, bloqueo, eliminación o destrucción.
- **Destinatario:** Persona natural o jurídica, pública o privada, a quien se comunican datos personales de forma legítima.
- **Registro de Actividades de Tratamiento o RAT:** Inventario documentado de tratamientos de datos personales, finalidades, bases legitimadoras, categorías, destinatarios, medidas, conservación y responsables internos.
- **Incidente o vulneración de seguridad:** Evento que ocasiona o puede ocasionar pérdida, destrucción, alteración, divulgación, acceso no autorizado, indisponibilidad o uso indebido de datos personales.

4. PRINCIPIOS RECTORES

El tratamiento de datos se regirá por:

Principio	Aplicación interna
Juridicidad y legalidad	Los datos personales solo serán tratados cuando exista una base legitimadora válida, una obligación legal, una relación contractual, un interés legítimo debidamente ponderado, consentimiento válido u otra causal permitida por la normativa.
Lealtad	Los datos serán obtenidos y utilizados de manera honesta, sin engaños, prácticas abusivas o finalidades ocultas.
Transparencia	Los titulares recibirán información clara, accesible y comprensible sobre el tratamiento de sus datos, mediante avisos de privacidad, contratos, comunicaciones o mecanismos equivalentes.
Finalidad	Los datos serán tratados para finalidades determinadas, explícitas, legítimas y comunicadas, sin usos incompatibles con la finalidad original.
Pertinencia, minimización y proporcionalidad	Solo se solicitarán y utilizarán los datos adecuados, necesarios y no excesivos para cumplir cada finalidad.
Confidencialidad	Los datos personales y la información asociada a expedientes de valoración serán tratados bajo reserva y solo por personas autorizadas.
Calidad y exactitud	Se procurará que los datos sean exactos, completos, actualizados y adecuados para la finalidad del tratamiento.
Conservación limitada	Los datos serán conservados solo durante el tiempo necesario para cumplir la finalidad, obligaciones legales, contractuales, contables, tributarias o defensa de derechos.
Seguridad	Se aplicarán medidas técnicas, organizativas, físicas y jurídicas adecuadas al nivel de riesgo.
Responsabilidad proactiva y demostrada	La Compañía mantendrá evidencias documentadas del cumplimiento, revisará sus controles y adoptará mejoras continuas.
Aplicación favorable al titular	En caso de duda razonable sobre el alcance de los derechos del titular, se aplicará la interpretación más favorable a la protección de sus datos, salvo obligación legal o derecho prevalente.

El tratamiento de datos personales se realizará conforme a las bases jurídicas previstas en la normativa aplicable, según corresponda:

Base legitimadora	Uso típico en la Compañía	Evidencia requerida
Ejecución contractual o medidas precontractuales	Cotizaciones, propuestas, contratos de valoración, órdenes de trabajo, entrega de informes, gestión de proveedores y servicios profesionales.	Contrato, propuesta, orden de servicio, correo de solicitud, acta de entrega o documento equivalente.
Cumplimiento de obligaciones legales	Facturación, contabilidad, tributación, obligaciones laborales, seguridad social, atención de requerimientos de autoridades, conservación legal de documentos.	Norma aplicable, requerimiento, comprobante, registro contable, expediente laboral o comunicación formal.
Consentimiento del titular	Comunicaciones no necesarias para la relación contractual, uso de datos sensibles cuando corresponda, banco de hojas de vida, finalidades voluntarias o adicionales.	Formulario, cláusula aceptada, registro digital, evidencia de revocatoria cuando aplique.
Interés legítimo ponderado	Seguridad de instalaciones y sistemas, prevención de fraude, defensa de derechos, gestión razonable de clientes, análisis interno, continuidad operativa.	Prueba o informe de ponderación, evaluación de impacto cuando corresponda, registro en RAT.
Orden judicial o requerimiento de autoridad competente	Entrega de información a jueces, autoridades administrativas o entes de control.	Oficio, resolución, providencia, orden o requerimiento formal.
Ejercicio o defensa de derechos	Reclamos, controversias contractuales, procesos administrativos, judiciales o arbitrales.	Expediente del caso, comunicación legal, poder, escrito o soporte procesal.
Datos de acceso público	Consulta de registros públicos, información catastral, mercantil, registral o fuentes públicas necesarias para servicios de valoración.	Identificación de fuente, fecha de consulta y finalidad del uso.

CLASIFICACIÓN DE LA INFORMACIÓN

La información tratada por la Compañía se clasifica en:

Categoría	Ejemplos	Controles esperados
Datos identificativos	Nombres, apellidos, cédula, pasaporte, RUC de persona natural, firma, cargo, representante legal.	Validación de necesidad, acceso por rol y custodia documental.
Datos de contacto	Correo electrónico, teléfono, dirección, domicilio, contacto laboral.	Uso limitado a la finalidad comunicada y actualización cuando corresponda.
Datos contractuales	Contratos, propuestas, órdenes de servicio, poderes, autorizaciones, actas, comunicaciones.	Archivo seguro, control de versiones y acceso restringido.
Datos financieros y tributarios	Cuentas bancarias, información de pagos, facturación, retenciones, comprobantes, datos contables.	Acceso restringido a finanzas, cifrado o controles equivalentes y conservación legal.
Datos laborales	Hoja de vida, experiencia, cargo, remuneración, asistencia, cargas laborales, certificados de matrimonio y / o de nacimiento, datos identificativos de hijos o cónyuges cuando corresponda, nómina, información de seguridad social.	Acceso restringido a talento humano y cumplimiento laboral.
Datos patrimoniales	Bienes, activos, propiedad, posesión, avalúos, referencias patrimoniales, situación económica relacionada con la valoración.	Clasificación restringida, minimización, confidencialidad reforzada y registro de destinatarios.
Información técnica de bienes	Ubicación, áreas, linderos, fotografías, características del inmueble, maquinaria, activos, registros catastrales, condiciones técnicas.	Protocolo de visita, control de acceso, protección de imágenes y entrega segura.
Datos geográficos o de ubicación	Dirección del bien, coordenadas, croquis, referencias de acceso.	Tratamiento limitado al expediente y protección contra divulgación no autorizada.

Datos sensibles, cuando corresponda	Información de salud ocupacional, discapacidad, datos biométricos u otros que excepcionalmente sean necesarios.	Base legitimadora reforzada, acceso altamente restringido y evaluación previa.
Datos de terceros relacionados	Ocupantes, copropietarios, garantes, arrendatarios, contactos técnicos, apoderados o personas vinculadas al bien.	Información al titular cuando sea viable, minimización y justificación de fuente indirecta.
Información confidencial corporativa asociada a datos personales	Cartera de clientes, contratos, ingresos, proyecciones, marcas, propiedad intelectual, know-how, documentos estratégicos de valoración de intangibles.	NDA, clasificación, segregación de repositorios y control de transferencia.

El acceso a la información será otorgado conforme a niveles de autorización, necesidad operativa y principio de mínimo privilegio.

5. CONSERVACIÓN, BLOQUEO Y ELIMINACIÓN

Los datos personales serán conservados únicamente durante el tiempo necesario para cumplir la finalidad del tratamiento y conforme a las obligaciones legales aplicables. Una vez cumplida la finalidad:

- Los datos podrán ser bloqueados cuando exista obligación legal de conservación.
- Posteriormente serán eliminados de forma segura cuando no exista obligación legal. En caso de documentos físicos estos deben ser triturados y en el caso de documentos digitales la eliminación completa del sistema.

Se prohíbe la conservación indebida o innecesaria de datos personales.

6. SEGURIDAD DE LA INFORMACIÓN

La compañía implementa medidas técnicas y organizativas para garantizar la protección de los datos personales, incluyendo:

Tipo de control	Medida obligatoria
Control de accesos	Acceso por usuario individual, rol, función y mínimo privilegio. Queda prohibido compartir credenciales.
Autenticación	Uso de contraseñas robustas y doble factor de autenticación en sistemas críticos, incluyendo correo, Microsoft 365, SharePoint, CRM, ERP, ClickUp y accesos administrativos.
Gestión de permisos	Alta, modificación y baja de usuarios con autorización del líder de proceso y revisión periódica de permisos.
Clasificación de información	Identificación de información pública, interna, confidencial, restringida y expedientes de valoración con datos personales o patrimoniales.
Cifrado y transferencia segura	Uso de mecanismos seguros para enviar informes, anexos, fotografías y documentos sensibles.
Copias de seguridad	Respaldos periódicos, protegidos y con pruebas de restauración documentadas.
Registros y trazabilidad	Mantenimiento de logs o registros de actividad en sistemas críticos cuando sea técnicamente posible.
Protección contra malware	Antivirus, actualizaciones, monitoreo y control de software autorizado en equipos corporativos.
Seguridad física	Custodia de archivos físicos, control de acceso a oficinas, gabinetes y documentos.

Dispositivos y trabajo en campo	Uso de equipos autorizados, protección de fotografías, carga segura de archivos y eliminación de copias locales innecesarias.
Confidencialidad contractual	Acuerdos de confidencialidad con personal, proveedores, peritos, consultores y encargados.

Las medidas serán revisadas periódicamente conforme al nivel de riesgo.

7. PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

La compañía incorpora principios de privacidad desde el diseño y por defecto en sus procesos, sistemas y servicios, asegurando que:

- Solo se traten los datos necesarios.
- Se apliquen medidas de seguridad adecuadas.
- Se limite el acceso a la información.
- Se reduzcan riesgos para los titulares.

8. RESPONSABLES INTERNOS

La Compañía mantendrá un sistema interno de protección de datos compuesto por esta Política, el RAT, avisos de privacidad, procedimientos, contratos, matrices, registros de evidencia, capacitaciones y revisiones periódicas. La responsabilidad de cumplimiento será compartida por la gerencia, la DPD, los líderes de proceso, el área tecnológica, talento humano, finanzas, operaciones, comercial y todos los colaboradores.

Rol	Responsabilidades principales
Gerencia General / Representante Legal	Aprobar la Política, asignar recursos, impulsar la cultura de cumplimiento, resolver escalaciones críticas y aprobar planes de mejora.
Delegada de Protección de Datos	Supervisar cumplimiento, coordinar el RAT, revisar riesgos, atender consultas, actuar como punto de contacto y emitir recomendaciones.
Líderes de proceso	Identificar tratamientos de su área, mantener información actualizada, ejecutar controles, reportar incidentes, responder solicitudes internas y custodiar evidencias.
Tecnología / Sistemas	Implementar controles de acceso, seguridad, respaldos, logs, actualizaciones, monitoreo, gestión de incidentes y medidas técnicas aprobadas.
Talento Humano	Gestionar datos laborales, capacitar al personal, conservar evidencias de aceptación de políticas y aplicar medidas disciplinarias cuando corresponda.

Finanzas y Contabilidad	Proteger datos financieros, tributarios, bancarios y contables, y asegurar conservación legal y acceso restringido.
Operaciones / Peritos / Consultores técnicos	Aplicar controles en visitas, expedientes, fotografías, informes, anexos técnicos y entrega de resultados.
Comercial	Usar datos de prospectos y clientes conforme a avisos de privacidad, bases legitimadoras y reglas de comunicaciones autorizadas.
Todo el personal	Guardar confidencialidad, usar datos solo para funciones autorizadas, proteger credenciales, no divulgar información y reportar incidentes.

La DPD deberá tener acceso oportuno a la información necesaria para cumplir sus funciones, relación directa con el nivel directivo, independencia funcional, recursos razonables, capacitación y participación en decisiones relevantes sobre nuevos tratamientos, proveedores, sistemas, herramientas, proyectos o incidentes.

Responsable del tratamiento:
INGENIERÍA PARA EL DESARROLLO ACURIO Y ASOCIADOS S.A.

Delegada de Protección de Datos (DPO):
Ab. María Victoria Villarroel González
Correo: **protecciondedatos@grupoacurio.com**

Los líderes de cada proceso serán responsables del tratamiento de datos personales dentro de su área.

9. ENCARGADOS DEL TRATAMIENTO

Todo proveedor, consultor, perito externo, aliado, plataforma tecnológica o tercero que trate datos personales por cuenta de la Compañía deberá estar sujeto a obligaciones documentadas de protección de datos, confidencialidad, seguridad, uso limitado, atención de incidentes, asistencia en derechos, devolución o eliminación de datos y restricciones de subcontratación o transferencia.

Antes de contratar o habilitar acceso a datos, el área responsable deberá coordinar con la DPD y el área legal la revisión del proveedor. Esta revisión deberá considerar tipo de datos, finalidad, ubicación del tratamiento, medidas de seguridad, subencargados, transferencias internacionales, continuidad del servicio, mecanismos de eliminación, auditoría y respuesta ante incidentes.

Proveedor o tercero	Requisito mínimo
Proveedores tecnológicos y nube	Contrato o términos de tratamiento, análisis de seguridad, ubicación de datos y controles de acceso.
Peritos externos y consultores técnicos	Acuerdo de confidencialidad, instrucciones de tratamiento, limitación de uso y devolución o eliminación al cierre.
Bancos y entidades financieras	Transferencia limitada a gestión de pagos, cobranzas u obligaciones contractuales.
Notarías y profesionales autorizados	Comunicación necesaria para formalización de actos o documentos.
Autoridades públicas, administrativas o judiciales	Entrega basada en obligación legal, competencia o requerimiento formal.
Auditores, asesores legales y profesionales de cumplimiento	Acceso limitado a la finalidad de auditoría, asesoría, defensa o cumplimiento.

10.DERECHOS DEL TITULAR

La empresa garantizará el ejercicio de los derechos de:

Derecho	Criterio de atención
Acceso	El titular podrá conocer y obtener información sobre sus datos personales tratados por la Compañía.
Rectificación y actualización	El titular podrá solicitar corrección de datos inexactos o incompletos, aportando soportes cuando corresponda.
Eliminación	El titular podrá solicitar supresión cuando proceda legalmente, sin perjuicio de obligaciones de conservación o defensa de derechos.
Oposición	El titular podrá oponerse a tratamientos permitidos por la ley, especialmente mercadotecnia directa o interés legítimo, cuando corresponda.
Portabilidad	El titular podrá solicitar entrega o transmisión de datos en formato estructurado cuando proceda técnica y legalmente.
Suspensión	El titular podrá solicitar limitación temporal del tratamiento en los casos previstos por la normativa.
No decisiones automatizadas	El titular podrá solicitar revisión cuando existan decisiones basadas únicamente en valoraciones automatizadas con efectos jurídicos o relevantes.

11.CONTROL Y AUDITORÍA

La Compañía podrá realizar auditorías, revisiones internas o evaluaciones de cumplimiento para verificar la aplicación de esta Política, del RAT, de los avisos de privacidad, de los contratos con encargados, de la matriz de conservación, de los controles de seguridad y de los procedimientos relacionados.

Las auditorías podrán ser documentales, técnicas, jurídicas u organizacionales. Los hallazgos deberán clasificarse por criticidad, asignarse a responsables, contar con plazos de corrección y ser objeto de seguimiento. La DPD podrá presentar informes periódicos a Gerencia General con avances, incidentes, solicitudes de titulares, riesgos, brechas, capacitaciones y planes de mejora.

12.INCUMPLIMIENTOS

El incumplimiento de esta Política, de los procedimientos internos, acuerdos de confidencialidad, contratos, instrucciones de tratamiento o normativa aplicable podrá generar medidas disciplinarias, contractuales, administrativas, civiles o penales, conforme a la naturaleza de la relación jurídica, la gravedad del hecho, la reincidencia, el daño ocasionado, el nivel de negligencia y las disposiciones vigentes.

13. ACTUALIZACIÓN

La presente Política podrá ser actualizada por cambios normativos, operativos o mejoras en los procesos internos.

14.FINALIDADES

- Prestación de servicios de tasación, valoración de bienes, valoración de intangibles y análisis patrimonial.
- Elaboración de peritajes técnicos, informes especializados y estudios profesionales.
- Prestación de servicios de consultoría técnica y asesoría especializada.
- Gestión contractual con clientes, proveedores y terceros relacionados.
- Procesos de facturación, cobranzas y gestión contable–financiera.
- Cumplimiento de obligaciones legales, regulatorias, tributarias y societarias.
- Administración de talento humano, incluyendo selección, contratación, nómina y cumplimiento laboral.
- Gestión administrativa interna y operativa.
- Gestión de seguridad de la información, control de accesos y prevención de incidentes.
- Conservación, archivo y custodia documental física y digital conforme a la normativa aplicable.
- Atención de solicitudes de ejercicio de derechos de los titulares de datos personales.

- Ejercicio y defensa de derechos en sede administrativa, judicial o arbitral cuando corresponda.

15.DEBERES DEL PERSONAL

Todo el personal deberá:

- Mantener la confidencialidad de la información:

No compartir datos personales con personas no autorizadas, dentro o fuera de la organización.

- Usar los datos solo para fines laborales autorizados:

Utilizar la información únicamente para las actividades propias de su función y conforme a lo definido en los procesos.

- Evitar la divulgación de información:

No enviar, copiar o difundir datos personales sin justificación ni autorización.

- Proteger sus credenciales de acceso:

Mantener en reserva usuarios y contraseñas, evitando compartirlos o dejarlos expuestos.

- Reportar incidentes o irregularidades:

Informar de inmediato cualquier pérdida, acceso indebido o uso incorrecto de datos personales.

- Cumplir con los acuerdos de confidencialidad:

Respetar los compromisos firmados relacionados con la protección de la información de la empresa y de los clientes.

16.MEDIDAS DE SEGURIDAD

Técnicas

Para garantizar la protección de los datos personales y la información sensible, la empresa implementa las siguientes medidas técnicas en sus sistemas y aplicaciones:

- **Microsoft (correo, archivos, SharePoint)**
  - Acceso mediante usuario y contraseña personal.
  - Verificación en dos pasos (doble autenticación) para mayor seguridad.
  - Control de permisos por carpetas y documentos, asignados según roles.
  - Respaldo automático en la nube con redundancia en múltiples servidores.

- **CRM (gestión de clientes)**
  - Acceso controlado mediante credenciales individuales y roles definidos.
  - Restricción de visibilidad según función del usuario, protegiendo información sensible de clientes.
  - Registro de actividades dentro del sistema para auditoría y seguimiento.

- **Base de datos / ERP**
  - Acceso restringido mediante usuario y contraseña, con controles adicionales por ubicación o dispositivo autorizado.
  - Diferentes niveles de permisos: consulta, edición y administración según el rol.
  - Respaldo diario de la información, con almacenamiento interno y externo seguro.
  - Registro de todas las acciones realizadas para control y trazabilidad.

- **ClickUp (gestión de tareas y proyectos)**
  - Acceso mediante usuario y contraseña personal.
  - Control de permisos por proyecto y tarea, asignados según el rol del usuario.
  - Historial de cambios que permite recuperación de versiones anteriores.
  - Restricción de acceso a información confidencial solo al equipo involucrado en el proyecto.

- **Protección mediante antivirus y software de seguridad**
  - Todos los equipos de la empresa cuentan con antivirus actualizado y monitoreo continuo para detectar malware, ransomware y otros riesgos.
  - Los sistemas reciben actualizaciones automáticas de seguridad para prevenir vulnerabilidades.
  - Se realizan escaneos periódicos de los equipos y servidores para identificar amenazas.
  - Revisión de log mediante consola centralizada de herramienta de antivirus y escaneo de mails.
  - El acceso a internet y a dispositivos externos está controlado para minimizar riesgos de infección.
- **Aplicativos internos y sistemas corporativos**
  - Se implementan controles de acceso y permisos, asegurando que cada usuario vea únicamente la información necesaria para su rol.
  - Se restringe la instalación de software no autorizado en los equipos corporativos, garantizando que solo aplicaciones aprobadas puedan ejecutarse.

Medidas organizativas

- **Protocolos internos:**

Aplicación de normas y procedimientos internos para el manejo adecuado de datos personales en cada proceso.

- **Capacitación:**

Formación periódica a los colaboradores sobre el uso correcto de la información y la protección de datos personales.

- **Control de acceso físico:**

Restricción del acceso a instalaciones, archivos y áreas donde se almacena información, permitiendo el ingreso solo a personal autorizado.

- **Custodia de documentos:**

Almacenamiento seguro de documentos físicos, evitando su pérdida, daño o acceso por personas no autorizadas.

17. PROCEDIMIENTO PARA DERECHOS ARCO

1. Recepción de la solicitud:
El titular envía su solicitud al correo de protección de datos de la organización,

2. Verificación de identidad:
Se valida que quien realiza la solicitud sea el titular de los datos o esté debidamente autorizado.

3. Registro de la solicitud:
Se registra internamente para su control y seguimiento.

4. Atención y respuesta:
Se analiza la solicitud y se responde dentro de los plazos establecidos por la normativa.

5. Archivo del proceso:
Se conserva el registro de la solicitud y la respuesta como respaldo.

18.GESTIÓN DE INCIDENTES

Todo colaborador, proveedor, perito externo o encargado que conozca o sospeche de una pérdida, acceso no autorizado, divulgación, alteración, destrucción, envío erróneo, indisponibilidad, malware, robo de equipo, exposición de credenciales o uso indebido de datos personales deberá reportarlo de inmediato al canal interno definido por la Compañía, a su líder de proceso, al área tecnológica y a la DPD.

La Compañía gestionará los incidentes conforme al procedimiento interno de vulneraciones de seguridad, que deberá incluir reporte, registro, preservación de

evidencia, clasificación, contención, análisis de riesgo, decisión de notificación, comunicación, remediación y lecciones aprendidas.

Etapa	Acción interna	Responsable
Reporte	Informar inmediatamente la sospecha o confirmación del incidente.	Cualquier persona obligada por esta Política.
Registro	Abrir registro interno con fecha, hora, sistema, datos afectados y personas involucradas.	DPD / Tecnología / Líder del proceso.
Contención	Bloquear accesos, recuperar información, aislar equipos, corregir destinatarios o limitar exposición.	Tecnología / Líder del proceso.
Evaluación	Analizar categorías de datos, titulares afectados, volumen, impacto, probabilidad y medidas existentes.	DPD / Tecnología / Legal / Gerencia.
Notificación	Determinar si procede comunicar a autoridad, ARCOTEL, titulares, clientes o responsables.	DPD / Gerencia / Legal.
Corrección	Implementar medidas correctivas y preventivas.	Área responsable / Tecnología.
Cierre	Documentar resultados, evidencias y lecciones aprendidas.	DPD

Cuando la Compañía actúe como responsable, notificará las vulneraciones a la Autoridad de Protección de Datos Personales y a la Agencia de Regulación y Control de las Telecomunicaciones cuando corresponda, tan pronto sea posible y dentro de los plazos legales aplicables. Cuando exista riesgo para los derechos fundamentales y libertades individuales de los titulares, se notificará a los titulares conforme a la normativa. Cuando la Compañía actúe como encargada, informará al responsable del tratamiento dentro del plazo legal aplicable desde que tenga conocimiento del incidente.

19.TRANSFERENCIA DE DATOS

Solo se transferirán datos a:

- Entidades financieras y bancarias para gestión de pagos, cobranzas y obligaciones contractuales.
- Notarías y profesionales autorizados cuando sea necesario para formalización de actos o documentos.

- Autoridades públicas, administrativas (como por ejemplo SRI, IESS, Ministerio de Trabajo), judiciales o de control, en cumplimiento de obligaciones legales o requerimientos formales.
- Proveedores tecnológicos, encargados del tratamiento o terceros autorizados que presten servicios necesarios para la operación.
- Auditores, asesores legales o profesionales vinculados al cumplimiento normativo cuando corresponda.

Toda transferencia se realizará bajo las siguientes condiciones:

- Existencia de base legal válida o habilitación normativa.
- Suscripción de contratos de confidencialidad y acuerdos de tratamiento de datos cuando corresponda.
- Aplicación de medidas técnicas y organizativas adecuadas de seguridad.
- Prohibición de uso de los datos para finalidades distintas a las instruidas.
- Limitación del acceso a la información estrictamente necesaria.
- Evaluación previa cuando la transferencia implique riesgo relevante para los titulares.
- Cumplimiento de los requisitos legales en caso de transferencias internacionales de datos.
- Registro interno de las transferencias efectuadas para efectos de trazabilidad y cumplimiento.

No se realizarán transferencias de datos personales que no se encuentren justificadas, autorizadas o respaldadas por la normativa aplicable.

20.SANCIONES INTERNAS

El incumplimiento de la presente Política y de las obligaciones en materia de protección de datos personales podrá generar responsabilidades conforme a la naturaleza de la relación jurídica y a la normativa aplicable.

Según corresponda, podrán adoptarse las siguientes medidas:

• Amonestaciones escritas o medidas disciplinarias internas.
• Sanciones laborales conforme a la normativa vigente y reglamentos internos.
• Terminación de la relación laboral o contractual cuando el incumplimiento sea grave o reiterado.
• Resolución inmediata de contratos con proveedores o encargados del tratamiento.
• Reclamo de daños y perjuicios ocasionados por negligencia, uso indebido, divulgación o tratamiento no autorizado de datos personales.
• Acciones administrativas ante la Autoridad de Protección de Datos Personales cuando corresponda.
• Acciones civiles o penales en caso de infracciones que así lo ameriten.

El personal y terceros que tengan acceso a datos personales responderán por el uso indebido, divulgación no autorizada, conservación indebida o incumplimiento de medidas

de seguridad establecidas en la presente Política y en los instrumentos contractuales suscritos.

La Compañía podrá ejercer las acciones legales necesarias para la protección de los derechos de los titulares y de sus propios intereses.

21.CAPACITACIÓN

La Compañía ejecutará capacitaciones periódicas en protección de datos personales, confidencialidad y seguridad de la información. La capacitación deberá ser proporcional al rol y riesgo de cada área. La participación será obligatoria y se conservará evidencia de asistencia, evaluación y aceptación de políticas.

Audiencia	Contenido mínimo
Todo el personal	Principios, confidencialidad, derechos, incidentes, credenciales, herramientas autorizadas y uso seguro de información.
Comercial	Avisos de privacidad, CRM, comunicaciones con prospectos, bases legitimadoras y consentimiento.
Operaciones, peritos y consultores	Captura de información en campo, fotografías, terceros vinculados, expedientes e informes.
Finanzas y contabilidad	Datos bancarios, tributarios, facturación, cobranza, conservación y control de acceso.
Talento humano	Datos laborales, candidatos, expedientes, datos sensibles, financieros y confidencialidad.
Tecnología	Accesos, logs, backups, incidentes, cifrado, seguridad de endpoints y privacidad por diseño.
Directivos y líderes	Responsabilidad proactiva, riesgos, auditorías, toma de decisiones y recursos.

22.VIGENCIA

La presente política entra en vigencia desde su aprobación y es de cumplimiento obligatorio para todas las personas sujetas a su alcance, sin excepción.

Su observancia es condición esencial para el adecuado tratamiento de datos personales y para el cumplimiento de las obligaciones legales de la compañía.