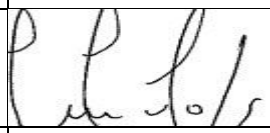
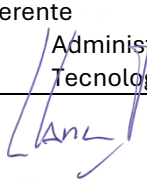
POLÍTICA DE PROTECCION DE DATOS PERSONALES

Elaborado		Revisado		Aprobado	
Cargo	Subgerente Tecnología	**Cargo**	Gerente Administración-Tecnología.	**Cargo**	Gerente General
Firma		**Firma**		**Firma**	
Fecha	19.05.2026	**Fecha**	12.06.2026	**Fecha**	12.06.2026

ÍNDICE

1. Objetivo

La presente Política de Protección de Datos Personales (la "Política") tiene por objeto establecer los principios, lineamientos, obligaciones y medidas que MV S.A., sus trabajadores, contratistas y terceros autorizados deberán cumplir en relación con el tratamiento de datos personales realizado dentro de la organización.

MV S.A. reconoce la importancia de proteger la privacidad, confidencialidad, integridad y seguridad de los datos personales tratados en el desarrollo de sus actividades comerciales y operacionales, especialmente considerando que la empresa presta servicios a terceros y administra información perteneciente a clientes, trabajadores, proveedores y usuarios.

La presente Política se dicta conforme a:

- Ley Nº 18.628 sobre Protección de la Vida Privada.
- Ley Nº 21.719 y futuras actualizaciones normativas aplicables en Chile.
- Obligaciones contractuales de confidencialidad suscritas con clientes y terceros.
- Principios y buenas prácticas internacionales en materia de protección de datos, incluyendo criterios del General Data Protection Regulation (GDPR) como estándar de referencia.

2. Alcance

Esta Política aplica a:

- Todos los trabajadores de MV S.A.
- Personal externo, contratistas y proveedores con acceso a información.
- Clientes y terceros cuyos datos sean tratados por la empresa.
- Todos los sistemas, plataformas, bases de datos, documentos y procesos que involucren tratamiento de datos personales.
- Datos tratados en formato físico, digital, audiovisual o cualquier otro medio.

3. Definiciones

3.1 Datos Personales

Cualquier información relacionada con una persona natural identificada o identificable.

3.2 Datos Sensibles

Aquellos datos referidos a características físicas o morales, vida privada, origen racial, estado de salud, biometría, información financiera, convicciones personales u otros protegidos por la legislación vigente.

3.3 Tratamiento de Datos

Cualquier operación o procedimiento realizado sobre datos personales, incluyendo recopilación, almacenamiento, uso, procesamiento, transferencia, eliminación o modificación.

3.4 Titular de los Datos

Persona natural a quien pertenecen los datos personales tratados por MV S.A.

3.5 Responsable del Tratamiento:

Persona natural o jurídica que decide sobre las finalidades y medios del tratamiento.

3.6 Encargado del Tratamiento:

Persona natural o jurídica que realiza tratamiento de datos por cuenta del responsable, según instrucciones documentadas.

---

4. Roles y Responsables de la Política.

Con el fin de asegurar el adecuado cumplimiento de la presente Política de Protección de Datos, la empresa define los siguientes roles y responsabilidades:

a. Encargado de Protección de Datos (EPO)

El Encargado de Protección de Datos (EPO) será el responsable de velar por el cumplimiento de la normativa vigente en materia de protección de datos personales dentro de la organización.

Responsabilidades principales:

- Supervisar la correcta implementación y cumplimiento de la política de protección de datos.
- Asesorar a la organización y a sus colaboradores respecto de sus obligaciones legales en materia de privacidad.
- Actuar como punto de contacto con las autoridades regulatorias y con los titulares de datos personales.

- Gestionar incidentes de seguridad relacionados con datos personales y coordinar las acciones correctivas.
- Promover la capacitación y concientización en protección de datos dentro de la empresa.

b. Trabajadores – Responsables Operativos

Todos los trabajadores de la empresa son responsables de cumplir con las disposiciones establecidas en la presente política en el desarrollo de sus funciones.

Responsabilidades principales:

- Tratar los datos personales de manera confidencial, segura y únicamente para los fines autorizados.
- Cumplir con los procedimientos internos definidos para la gestión de información.
- Informar de inmediato cualquier incidente, brecha o uso indebido de datos personales al DPO o a la jefatura correspondiente.
- Participar en las actividades de capacitación en protección de datos.
- Utilizar adecuadamente los sistemas y herramientas tecnológicas, respetando las medidas de seguridad establecidas.

c. Jefaturas

Las jefaturas tienen un rol clave en la implementación y supervisión del cumplimiento de la política dentro de sus respectivas áreas.

Responsabilidades principales:

- Asegurar que los equipos a su cargo cumplan con las disposiciones de la política de protección de datos.
- Garantizar que los procesos bajo su responsabilidad incorporen medidas de protección de datos desde el diseño.
- Supervisar el correcto tratamiento de los datos personales en sus áreas.
- Facilitar instancias de capacitación y reforzar las buenas prácticas en materia de seguridad de la información.
- Coordinar con el EPO la gestión de riesgos, incidentes o mejoras relacionadas con la protección de datos.

5. Principios Rectores del Tratamiento

MV S.A. realizará el tratamiento de datos personales conforme a los principios establecidos en la legislación chilena vigente sobre protección de datos personales, incluyendo la Ley Nº 18.628 y sus modificaciones introducidas por la Ley Nº 21.719, así como considerando estándares internacionales de buenas prácticas basados en el General Data Protection Regulation (GDPR).

Todos los trabajadores, contratistas y terceros autorizados deberán aplicar estos principios en el desarrollo de sus funciones y durante cualquier actividad que involucre acceso, tratamiento, almacenamiento, transmisión o eliminación de datos personales.

5.1 Licitud, Lealtad y Transparencia

MV S.A. realizará el tratamiento de datos personales únicamente sobre bases legítimas, contractuales, legales o autorizadas, asegurando que dicho tratamiento sea efectuado de forma transparente, trazable y conforme a las instrucciones definidas por la organización y sus clientes.

Todo tratamiento deberá ejecutarse de manera clara, responsable y respetando los derechos de los titulares de los datos.

Obligaciones operativas:

- Acceder y tratar datos personales únicamente cuando exista autorización, necesidad operacional o instrucción formal asociada a las funciones del trabajador.
- Ejecutar actividades de tratamiento exclusivamente dentro del marco contractual y operacional definido por MV S.A.
- Mantener registro y trazabilidad de actividades que involucren acceso o manipulación de información.
- Abstenerse de utilizar datos personales para fines distintos a los autorizados.
- Informar inmediatamente cualquier instrucción ambigua, no documentada o que pueda representar un incumplimiento normativo.
- Utilizar únicamente plataformas, sistemas y canales aprobados por la empresa.

5.2 Limitación de la Finalidad

Los datos personales tratados por MV S.A. deberán utilizarse exclusivamente para fines específicos, explícitos y legítimos previamente definidos en el contexto de la prestación de servicios, cumplimiento contractual u obligaciones legales.

- Queda prohibido reutilizar información para finalidades distintas sin autorización previa y formal.

Obligaciones operativas:

- Verificar previamente el propósito autorizado antes de acceder o utilizar datos personales.
- Utilizar la información exclusivamente para las actividades asignadas dentro de las funciones laborales.
- Evitar el uso de datos para fines personales, pruebas, análisis internos no autorizados o actividades ajenas al servicio contratado.
- Restringir consultas, reportes y accesos sólo a la información necesaria para la tarea encomendada.
- Solicitar validación formal cuando exista duda respecto del uso permitido de la información.

5.3 Minimización de Datos o Principio de Proporcionalidad

MV S.A. promoverá el tratamiento limitado y proporcional de datos personales, asegurando que sólo se recopile, utilice y almacene la información estrictamente necesaria para cumplir la finalidad autorizada.

Obligaciones operativas:

- Solicitar y utilizar únicamente los datos mínimos necesarios para ejecutar las funciones asignadas.
- Evitar generar copias innecesarias de información personal.
- Aplicar medidas de anonimización, ocultamiento o seudonimización cuando la operación lo permita.
- Restringir descargas masivas, exportaciones o almacenamiento local no autorizado.
- No incorporar campos, atributos o antecedentes adicionales que no sean requeridos operacionalmente.
- Utilizar configuraciones de acceso basadas en el principio de mínimo privilegio.

5.4 Exactitud o Principio de Calidad

MV S.A. procurará mantener los datos personales correctos, íntegros, actualizados y consistentes, evitando errores que puedan afectar a los titulares o la calidad del servicio prestado.

Obligaciones operativas:

- Verificar la información utilizada durante los procesos operacionales.
- No modificar registros sin autorización o procedimiento definido.
- Reportar oportunamente inconsistencias, duplicidades o errores detectados en los datos.
- Mantener actualizados los registros bajo responsabilidad del área correspondiente.
- Utilizar únicamente fuentes oficiales o sistemas autorizados para consultas y actualizaciones.
- Registrar observaciones o hallazgos relevantes conforme a los procedimientos internos.

5.5 Limitación del Plazo de Conservación

Los datos personales deberán conservarse únicamente durante el período necesario para cumplir la finalidad del tratamiento, obligaciones legales, contractuales o regulatorias aplicables.

Una vez cumplido dicho período, la información deberá eliminarse, anonimizarse o bloquearse según corresponda.

Obligaciones operativas:

- Respetar los plazos de conservación definidos por contratos, normativas o políticas internas.
- No almacenar información personal en dispositivos locales, correos o medios externos sin autorización.
- Eliminar o devolver información cuando finalice la necesidad operacional o contractual.
- Evitar mantener respaldos informales o copias no autorizadas.
- Aplicar procedimientos seguros de eliminación documental y digital.
- Coordinar con TI y Seguridad de la Información cualquier proceso de depuración o destrucción de datos.

5.6 Integridad y Confidencialidad (Seguridad)

MV S.A. implementará medidas técnicas, organizacionales y administrativas destinadas a resguardar la seguridad, confidencialidad, disponibilidad e integridad de los datos personales tratados por la organización.

Todos los trabajadores deberán proteger la información frente a accesos no autorizados, pérdidas, alteraciones, filtraciones o usos indebidos.

Obligaciones operativas:

- Mantener resguardo de credenciales, contraseñas y mecanismos de autenticación.
- Utilizar únicamente dispositivos, redes y sistemas autorizados por la empresa.
- Cumplir las políticas de seguridad de la información vigentes.
- Aplicar el principio de mínimo privilegio en el acceso a información.
- Bloquear sesiones y resguardar equipos cuando no estén en uso.
- No compartir accesos, usuarios ni credenciales.
- No transferir información a plataformas externas, herramientas de IA o servicios no autorizados.
- Reportar inmediatamente incidentes de seguridad, pérdida de dispositivos o accesos indebidos.
- Respetar las restricciones sobre uso de dispositivos externos y almacenamiento portátil.

5.7 Principio de Responsabilidad

MV S.A. asume el compromiso de implementar controles, procedimientos y mecanismos permanentes destinados a asegurar el cumplimiento de la normativa de protección de datos personales y la mejora continua de sus prácticas de seguridad y privacidad.

La organización no sólo declara proteger los datos personales, sino que mantiene medidas concretas para demostrar cumplimiento y trazabilidad.

Medidas y controles aplicados:

- Política de Protección de Datos Personales.
- Política de Seguridad de la Información.
- Política de Uso de Herramientas de Inteligencia Artificial.

- Acuerdos de confidencialidad para trabajadores y terceros.
- Controles de acceso lógico y físico.
- Gestión de perfiles y privilegios.
- Monitoreo y trazabilidad de accesos.
- Capacitaciones periódicas sobre privacidad y seguridad.
- Procedimientos de gestión de incidentes.
- Evaluaciones y auditorías internas periódicas.
- Gestión documental y control de retención de información.
- Supervisión de proveedores con acceso a datos personales.
- Medidas de ciberseguridad y protección tecnológica implementadas por TI.

Todos los trabajadores y terceros autorizados deberán colaborar activamente en el cumplimiento de estas medidas y reportar cualquier situación que pueda afectar la seguridad o privacidad de la información.

---

6. Medidas de Seguridad

MV S.A. implementa medidas técnicas, administrativas, organizacionales y de ciberseguridad destinadas a proteger los datos personales y la información confidencial tratada en el desarrollo de sus operaciones, considerando la naturaleza de los servicios prestados, los riesgos asociados al tratamiento de información y las obligaciones legales y contractuales aplicables.

Las medidas descritas a continuación buscan prevenir accesos no autorizados, pérdidas, alteraciones, divulgaciones indebidas, destrucción de información o cualquier tratamiento no autorizado de datos personales.

---

a. Control de accesos y gestión de privilegios

MV S.A. mantiene controles de acceso lógico sobre sistemas, plataformas, aplicaciones y repositorios de información que contienen datos personales o información confidencial.

Los accesos son asignados según funciones, responsabilidades y necesidad operacional, aplicando el principio de mínimo privilegio.

Medidas aplicadas:

- Asignación individual de cuentas de usuario.
- Restricción de accesos según perfil y cargo.
- Segregación de funciones críticas.
- Bloqueo y revocación de accesos ante desvinculación o cambios de funciones.
- Validación de autorizaciones por jefaturas y TI.
- Registro y trazabilidad de accesos relevantes.

---

b. Autenticación multifactorial

MV S.A. implementa mecanismos de autenticación reforzada para accesos críticos, plataformas externas, servicios remotos y sistemas que procesan información sensible.

Medidas aplicadas:

- Uso de autenticación multifactorial (MFA) en plataformas críticas.
- Validación adicional para accesos remotos.
- Renovación de contraseñas.
- Restricción de reutilización de credenciales.
- Bloqueo automático ante intentos fallidos reiterados.

---

c. Cifrado de datos en tránsito y en reposo.

La organización aplica mecanismos de protección criptográfica sobre información sensible y comunicaciones electrónicas cuando el riesgo o la naturaleza del servicio lo requiere.

Medidas aplicadas:

- Uso de protocolos seguros de comunicación.
- Protección de información transmitida mediante canales cifrados.
- Cifrado de dispositivos corporativos autorizados cuando corresponde.

- Resguardo seguro de respaldos e información almacenada.
- Restricción de almacenamiento de información en medios no autorizados.

---

d. Monitoreo continuo y registro de actividades relevantes

MV S.A. mantiene mecanismos de monitoreo orientados a detectar actividades inusuales, accesos indebidos, incidentes de seguridad o incumplimientos de políticas internas.

Medidas aplicadas:

- Registro de accesos y eventos relevantes.
- Supervisión de actividades administrativas críticas.
- Monitoreo de accesos remotos y conexiones externas.
- Revisión de alertas de seguridad.
- Trazabilidad de modificaciones relevantes en sistemas autorizados.

---

e. Gestión de parches, vulnerabilidades y actualizaciones

La empresa mantiene procesos de actualización y corrección de vulnerabilidades sobre infraestructura tecnológica, dispositivos y aplicaciones corporativas.

Medidas aplicadas:

- Aplicación periódica de actualizaciones de seguridad.
- Evaluación de vulnerabilidades detectadas.
- Gestión de software autorizado.
- Control de versiones y soporte de sistemas críticos.
- Restricción de instalación de software no autorizado.

f. Uso de VPN para accesos remotos autorizados

Los accesos remotos a recursos corporativos son controlados mediante mecanismos seguros de conexión.

Medidas aplicadas:

- Uso de conexiones VPN autorizadas para accesos externos.
- Validación de identidad previa al acceso remoto.
- Restricción de accesos desde dispositivos no autorizados.
- Monitoreo de sesiones remotas.
- Aplicación de controles de seguridad sobre conexiones externas.

---

g. Política de escritorio limpio y medidas físicas de protección

MV S.A. aplica controles físicos y organizacionales destinados a proteger información en formato físico y digital dentro de las instalaciones de la empresa.

Medidas aplicadas:

- Política de escritorio limpio.
- Bloqueo de equipos desatendidos.
- Restricción de acceso físico a áreas críticas.
- Resguardo seguro de documentación física.
- Eliminación segura de documentos confidenciales.
- Control de visitas y terceros en áreas restringidas.

---

h. Prohibición del uso de herramientas o servicios no autorizados (Shadow IT)

La organización restringe el uso de aplicaciones, plataformas, servicios cloud o herramientas tecnológicas no aprobadas formalmente por el área TI.

Medidas aplicadas:

- Bloqueo o restricción de aplicaciones no autorizadas.
- Evaluación previa de herramientas tecnológicas.
- Restricción de uso de plataformas personales para fines laborales.
- Controles sobre transferencia de información a servicios externos.
- Política específica para uso de herramientas de Inteligencia Artificial.

---

i. Registro actualizado de perfiles de acceso y usuarios autorizados

MV S.A. mantiene control y trazabilidad sobre los usuarios que poseen acceso a sistemas o información que contienen datos personales.

Medidas aplicadas:

- Inventario de usuarios y perfiles activos.
- Registro de autorizaciones de acceso.
- Gestión centralizada de cuentas cuando corresponde.
- Revisión de vigencia de accesos.
- Documentación de altas, modificaciones y bajas de usuarios.

---

j. Revisiones periódicas de perfiles y accesos

La organización realiza revisiones periódicas o específicas sobre los permisos otorgados a usuarios y perfiles con acceso a información personal.

Medidas aplicadas:

- Revisiones periódicas de privilegios.
- Validación de accesos vigentes con jefaturas.
- Identificación de cuentas inactivas o innecesarias.
- Ajustes de permisos según cambios operacionales.

- Auditorías internas sobre controles de acceso.

---

k. Registro actualizado de incidencias de seguridad

MV S.A. mantiene mecanismos para registrar, gestionar y dar seguimiento a incidentes relacionados con seguridad de la información o protección de datos personales.

Medidas aplicadas:

- Registro de incidentes y eventos de seguridad.
- Documentación de pérdidas o accesos indebidos.
- Registro de incidentes relacionados con dispositivos corporativos.
- Seguimiento de medidas correctivas implementadas.
- Escalamiento de incidentes relevantes a las áreas responsables.

---

l. Medidas correctivas y notificación de incidentes

La empresa adopta acciones correctivas y de contención frente a incidentes que puedan comprometer la confidencialidad, integridad o disponibilidad de datos personales.

Medidas aplicadas:

- Contención y análisis de incidentes detectados.
- Evaluación del impacto asociado al incidente.
- Implementación de acciones correctivas y preventivas.
- Notificación a clientes afectados cuando corresponda contractual o legalmente.
- Coordinación con áreas legales, TI y Seguridad de la Información.
- Registro formal de las acciones ejecutadas.

---

m. Inventario actualizado de bases de datos y activos de información

MV S.A. mantiene control sobre los activos de información y repositorios que contienen datos personales o información sensible.

Medidas aplicadas:

- Inventario de bases de datos y sistemas críticos.
- Identificación de propietarios de información.
- Clasificación de información según criticidad.
- Registro de medios de almacenamiento autorizados.
- Identificación de respaldos y ubicaciones de resguardo.

---

n. Copias de seguridad y recuperación de información

La organización ejecuta procesos de respaldo orientados a asegurar la disponibilidad y recuperación de información ante incidentes operacionales o tecnológicos.

Medidas aplicadas:

- Ejecución periódica de respaldos de información crítica.
- Protección y resguardo seguro de copias de seguridad.
- Restricción de acceso a respaldos.
- Verificación periódica de integridad de respaldos.
- Procedimientos de recuperación ante incidentes o contingencias.
- Coordinación con planes de continuidad operacional y recuperación tecnológica

---

7. Derechos de los Titulares

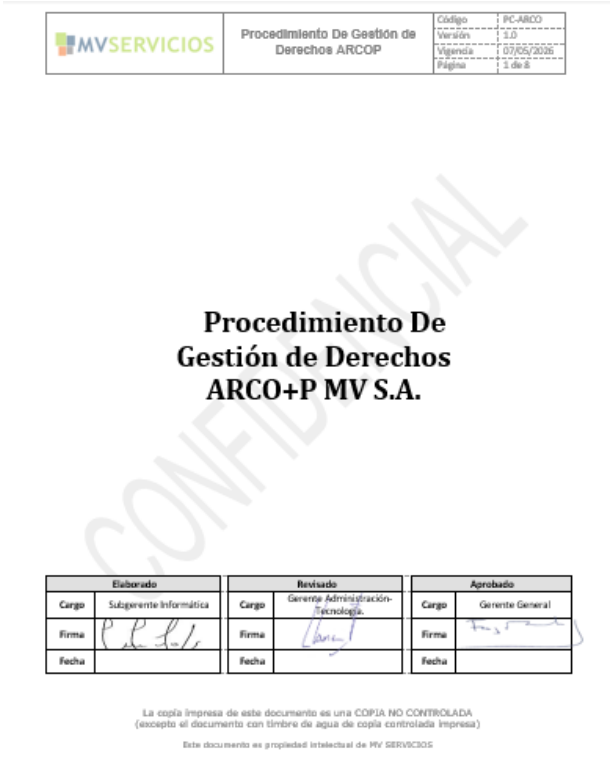
El presente Procedimiento ARCOP establece las directrices internas para que los titulares de datos personales puedan ejercer sus derechos respecto del tratamiento de su información personal realizado por MV S.A.

Este procedimiento regula la recepción, validación, análisis, gestión, respuesta y cierre de solicitudes relacionadas con los derechos de:

- Acceso.
- Rectificación.
- Cancelación.
- Oposición.
- Portabilidad de datos personales.

MV S.A. reconoce el derecho de toda persona a mantener control sobre sus datos personales y adopta medidas destinadas a garantizar una gestión transparente, segura, trazable y oportuna de dichas solicitudes, conforme a la legislación vigente y buenas prácticas internacionales de protección de datos.

En función de lo anterior, hemos definido un procedimiento que regula dicha gestión



MVSERVICIOS	Procedimiento De Gestión de Derechos ARCOP	Código	PC-ARCO
		Versión	1.0
		Vigencia	07/05/2026
		Página	1 de 8

CONFIDENCIAL

Procedimiento De Gestión de Derechos ARCO+P MV S.A.

Elaborado		Revisado		Aprobado	
Cargo	Subgerente Informática	Cargo	Gerente Administración-Tecnología.	Cargo	Gerente General
Firma		Firma		Firma	
Fecha		Fecha		Fecha	

8. Transferencias internacionales y Subcontratación.

MV S.A de RUT 95.785.210- K que presta servicios a empresas del Grupo Santander y que, en virtud de estos actúe como Encargado del Tratamiento, a tenor de lo establecido en el Reglamento (UE) 2016/679 General de Protección de Datos (RGPD), (en adelante, el Encargado)

Certifico que en caso de que la prestación de los servicios implique el tratamiento de datos por parte de terceras empresas (en adelante los Sub-encargados), se observarán en todo caso los siguientes requisitos:

La contratación de los Sub-encargados se ajustará a un procedimiento de revisión y control internos que verifique y garantice en la medida de lo posible que los Sub-encargados cumplen con las garantías exigidas por el RGPD y demás normativa aplicable.

En todo caso la relación con los Sub-Encargados, en lo que al tratamiento de datos se refiere, estará regulada en un contrato escrito que recogerá como mínimo las mismas obligaciones que las asumidas por el Encargado.

En caso de que el Encargado desee contratar a cualquier otro Sub-encargado que no haya sido identificado en la fase contractual, deberá recabar la autorización previa expresa del responsable del tratamiento.

Que el Encargado almacenará y procesará los datos personales (incluso las copias de seguridad) en países del Espacio Económico Europeo o en alguno de los siguientes países (Andorra, Argentina, Canadá (Sector privado), Suiza, Islas Feroe, Guernsey, Israel, Japón, Isla de Man, Jersey, Nueva Zelanda y Uruguay.

En el caso de que el tratamiento de los datos del responsable del Tratamiento tenga lugar fuera de los países anteriormente mencionados, implementará las garantías necesarias para llevar a cabo dichas transferencias internacionales de datos de acuerdo con los requisitos exigidos en el RGPD y demás normativa aplica.

8.1 Uso de Terceros y Servicios Externalizados

MV S.A. no externaliza ni terceriza actividades asociadas a la ejecución de sus procesos de negocio, prestación de servicios, atención de clientes, gestión de cobranzas o funciones de BackOffice.

La totalidad de las actividades operacionales y de servicio son ejecutadas por personal contratado directamente por MV S.A., manteniendo el control y la responsabilidad sobre los procesos críticos de la organización.

Los proveedores externos utilizados por la empresa se limitan exclusivamente al suministro de infraestructura tecnológica de carácter genérico, tales como servicios de conectividad, alojamiento, plataformas tecnológicas o recursos informáticos de uso común, sin intervenir en la ejecución de procesos de negocio ni tener participación operativa en la prestación de los servicios de MV S.A.

8. Auditorías, Cumplimiento y Consecuencias

En MV S.A facilitaremos auditorías técnicas, administrativas y de cumplimiento; mantener evidencia disponible; y adoptar medidas disciplinarias internas por incumplimientos. Asumiendo responsabilidades contractuales y regulatorias derivadas de infracciones.

9. Vigencia y Actualización

La presente Política entrará en vigor a partir de su aprobación y será objeto de revisión anual dentro del proceso de Revisión por la Dirección del Sistema de Gestión de Seguridad de la Información implementado en MV S.A., o cuando se produzcan cambios regulatorios relevantes. Todas las modificaciones realizadas quedarán registradas en el punto 12, correspondiente al Control de Cambios y Aprobaciones de esta Política.

10. Procedimientos Anexos a la Política de Protección de Datos Personales

- Procedimiento de Gestión de Derechos ARCOP
- Procedimiento de Gestión de Accesos y Privilegios de Usuario.
- Instructivo para la Implementación y Uso de Autenticación Multifactor (MFA).
- Procedimiento de Cifrado y Protección de la Información en Tránsito y en Reposo.
- Procedimiento de Monitoreo, Registro y Trazabilidad de Eventos de Seguridad.
- Procedimiento de Gestión de Vulnerabilidades, Parches y Actualizaciones de Seguridad.
- Instructivo para el Uso Seguro de Accesos Remotos mediante VPN.
- Procedimiento de Escritorio Limpio, Pantalla Limpia y Protección Física de la Información.
- Procedimiento para el Control y Prevención del Uso de Herramientas No Autorizadas (Shadow IT).
- Procedimiento para la Gestión y Mantención de Perfiles de Acceso a Sistemas y Datos Personales.
- Procedimiento de Revisión Periódica de Accesos y Privilegios sobre Datos Personales.
- Procedimiento de Registro, Control y Gestión de Incidentes que Afecten Datos Personales.
- Procedimiento de Gestión de Incidentes y Notificación de Brechas de Seguridad y Datos Personales.
- Procedimiento para la Gestión e Inventario de Activos de Información Sujetos a Respaldo.
- Procedimiento de Respaldo, Recuperación y Verificación de Copias de Seguridad.

11. Control de Cambios y Aprobaciones

Versión	Fecha	Responsable	Razón del Cambio	Nivel de Confidencialidad
1.0	19/05/2026	Mario Vofs	Creación del Documento	Alto