POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

1. OBJETO

Identificar y proteger los Datos Personales en custodia de RAFAP S.A, evitando la destrucción, divulgación, modificación y utilización no autorizada de toda información relacionada con ellos.

2. ALCANCE

Alcanza los datos personales incluidos en todas las actividades de la organización, y las de aquellos terceros con los que existan relaciones contractuales.

3. RESPONSABLES

La Política de Datos Personales es formulada y su cumplimiento monitoreado por el Gerente de Gestión, el Gerente General, la Supervisora General de Riesgo, el Supervisor General de Auditoría Interna, el Oficial de Seguridad y el Responsable de Base de Datos. A su vez, cada Gerente será responsable de hacer cumplir la presente Política en su área.

4. DESCRIPCIÓN

4.1. Formulación

La Alta Dirección es, a través del Gerente de Gestión, responsable por el desarrollo de las prácticas necesarias para el cumplimiento de la política, así como de su difusión y control.

Los colaboradores, proveedores, dependientes de los proveedores que tengan acceso a información de la empresa, y empresas a las que los mismos subcontraten para realizar tareas en la empresa, deberán notificarse de la política y adherir a ella en el cumplimiento cotidiano de sus actividades. El control de adhesión por parte de los terceros será responsabilidad de la División Administración.

Los eventuales apartamientos de la política deberán ser registrados de acuerdo al PR GT 32– Control de No Conformidades, Incidentes y Oportunidades de Mejora.

4.2. Normativa

La presente política se basa fundamentalmente en la Ley N° 18331 de Protección de Datos Personales, su posterior reglamentación a través del Decreto 414/009, y en la Reglamentación de los artículos 37 a 40 de la Ley N° 19670 de Rendición de Cuentas y Balance de Ejecución Presupuestal.

4.3. Definición de los componentes a proteger.

Dato Personal – Es información de cualquier tipo referida a personas físicas o jurídicas, que permitan identificarla directa o indirectamente. (Por ejemplo: Nombres, Apellidos, Correos Electrónicos, Fotografías, Huellas Dactilares, Voz, RUT, ADN, etc.)

Tratamiento de Datos – Implica una actividad sistemática de Recabar, Elaborar, Modificar, Almacenar, Explotar, Intercambiar o Comunicar Datos. Pueden ser realizadas en forma manual o automática.

Titular de los Datos: persona cuyos datos sean objeto de un tratamiento, y que la hacen identificable.

Disponibilidad - Propiedad de que la información sea accesible y utilizable por solicitud de una persona propietaria del dato o en aquellas situaciones contempladas por la Ley (como por ejemplo solicitudes de BPS, razones de salud o higiene públicas, etc.).

Confidencialidad - Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. Se clasifica a todos los Datos Personales como confidenciales, de acuerdo a la PO 5 - Política de Seguridad de la Información.

Seguridad de la información - Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, responsabilidad con obligación de reportar (accountability), no repudio y confiabilidad.

Evento de Vulneración de seguridad de Datos Personales - Comprende a incidentes de seguridad que ocasionen, entre otras, la divulgación, destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados a dichos datos. Deberá ser comunicado a la URCDP.

Sistema de gestión de la seguridad de la información (SGSI) - Parte del sistema de gestión global, basada en un enfoque hacia los riesgos de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizacional, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos.

Integridad - Propiedad de salvaguardar la exactitud y estado completo de los activos.

5. PRÁCTICAS A CUMPLIR

a. Se le deben establecer al Responsable de BD anualmente objetivos con relación al Tratamiento de Datos Personales.
b. Se debe enmarcar la gestión de datos personales dentro del apetito de riesgo que aprueba la Alta Dirección.
c. Se debe desarrollar un proceso de análisis del riesgo y de acuerdo a su resultado, se implementen las acciones correspondientes con el fin de tratar los riesgos que se consideren inaceptables, según los criterios establecidos en el MAN GT 9 - Manual del Sistema Integrado de Gestión.
d. Se debe contar con adecuada identificación y medición de los riesgos, considerando criterios establecidos por la OTR PGR 290 - Metodología de valuación de riesgos operativos. A partir de los resultados de la identificación y medición de riesgo, y de los límites establecidos para los mismos en la Política de Riesgos, se debe llevar adelante el proceso de control y monitoreo en la Matriz de Tratamiento y Protección de Datos Personales.

e. Se deben establecer los objetivos de control y los controles correspondientes, en virtud de las necesidades que en materia de riesgos surjan del proceso de Análisis de riesgos manejado.
f. Se debe cumplir con los requisitos del negocio, legales o reglamentarios y las obligaciones contractuales sobre el Tratamiento de Datos Personales.
g. Se debe brindar concientización en materia de Tratamiento de Datos Personales.
h. Todo empleado, cuya función implique el trabajo con estos datos, es responsable de reportar las violaciones al incorrecto Tratamiento de Datos Personales, confirmadas o sospechadas.
i. El Responsable de Base de Datos es responsable sobre el mantenimiento de esta política, por brindar asesoramiento y guía para su implementación, e investigar toda violación reportada por el personal.
j. Contar con elementos de detección para los riesgos de seguridad de Datos Personales, los que deberán ser analizados y evaluados a fin de lograr una rápida respuesta minimizando las consecuencias de la posible falla.
k. Todos los proveedores externos que participen o afecten de cualquier forma los sistemas de información manuales o informáticos deberán ser informados de esta política e exhortados a suscribirla.
l. La información de la organización se hace disponible de acuerdo al principio de la necesidad de saber o necesidad de hacer. Está prohibido el acceso o el intento de acceso a la información, y el uso de los recursos, más allá de los privilegios asignados de acuerdo al rol funcional de cada uno de sus miembros.
m. Los proyectos, desarrollos y cambios a sistemas deben involucrar al Responsable de Base de Datos para asesoramiento en políticas de Protección de Datos Personales, desde su fase inicial y durante su transcurso, aplicando así la privacidad por Diseño y por Defecto.
n. Ninguna Base de Datos puede tener como finalidad atentar contra los derechos humanos, ser contraria a la moral pública y las leyes.
o. Los datos deben ser Verdaderos, Objetivos y Adecuados.
p. Los datos deben ser rectificados o actualizados cuando corresponda.
q. Los datos no pueden ser obtenidos de forma ilegal o abusando de su posición a su titular, ni violando la Ley.
r. Los datos personales no pueden ser utilizados para fines diferentes para los que se obtuvieron.
s. Es necesario contar con el consentimiento del titular de los datos personales, incluso aquellos no relativos específicamente a la administración de su cuenta individual.
t. El Responsable de las Bases de Datos deberá adoptar medidas para garantizar que los Datos Personales permanezcan seguros y confidenciales. Por ejemplo: Políticas de Seguridad, Evaluaciones de impacto, Auditorías, Respaldos.
u. Los colaboradores de RAFAP deberán guardar secreto profesional.
v. Se deberán registrar ante la URCDP la creación, modificación o supresión de las Bases de Datos que contengan Datos Personales.
w. Responder en un plazo máximo de 5 días hábiles a la solicitud de un titular que quiera ejercer el derecho de acceso, rectificación, actualización, inclusión o supresión de sus datos, como se establece en el ITGT 192 - Ejercicio del derecho de rectificación, actualización, inclusión o supresión de los datos del titular.

La Alta Dirección considera como parte de la Política de Datos Personales el cumplimiento de las prácticas generales presentes en el **Código de ética** y en la **PO GG 5 - Política de Seguridad de la Información,** así como las particulares que se enumeran en el **MAN GT 9 - Manual del Sistema Integrado de Gestión**.

6. DIFUSIÓN

Esta Política y sus documentos relacionados deben revisarse y difundirse como mínimo una vez por año a toda la organización.

7. Implantación de la política

El Departamento de Gestión apoyará a los demás Departamentos en el cumplimiento de esta política.

8. Clasificación de la presente política.

La Política de Datos Personales de República AFAP S.A. es de carácter interno, con las siguientes particularidades:

a) Los proveedores deben suscribirla del modo en que se describa en los documentos correspondientes del SIG.

b) Estará disponible para entregar a un interesado que la solicite.

9. Comunicación entre la Gestión y Prevención y Gestión de Riesgos

En caso que se detecte un error, desvío o cualquier situación potencialmente riesgosa, que pueda generar o materializar un riesgo para República AFAP, se deberá informar a través de la herramienta BOLT, al Área de Prevención y Gestión de Riesgo en un plazo no mayor a 2 días hábiles contados a partir del conocimiento del hecho por parte del colaborador. El Área deberá analizar el evento y gestionar los riesgos asociados en caso de ser necesario. Los factores de riesgos a considerar son los siguientes: riesgo operativo (procesos, seguridad de la información y cumplimiento de normas internas y externas), financiero, lavado de activos y financiamiento del terrorismo, reputacional, soborno y estratégico.