POLITICA DE SEGURIDAD DE LA INFORMACION

1. OBJETO

La Dirección de República AFAP reconoce la importancia de identificar y proteger sus activos de información, evitando la destrucción, la divulgación, modificación y utilización no autorizada de toda información relacionada con clientes, colaboradores, precios, bases de conocimiento, manuales, casos de estudio, códigos fuente, estrategia, gestión, y otros conceptos; comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI), como parte integrante del Sistema Integrado de Gestión (SIG).

2. ALCANCE

La Política de Seguridad de la Información es un conjunto de prácticas que deben cumplirse por parte de la organización, sus colaboradores, y aquellos terceros con los que existan relaciones contractuales, con la finalidad de proteger los activos de información propiedad de la empresa, sus afiliados o accionistas.

3. RESPONSABLES

La Política de Seguridad de la Información es formulada por el Gerente de Gestión con apoyo del Oficial de Seguridad, en acuerdo con el Gerente y Subgerente General. Su cumplimiento es monitoreado por el Oficial de Seguridad y los Supervisores Generales de Auditoría Interna y Riesgo.

4. DESCRIPCIÓN

4.1. Formulación

El Gerente de Gestión es responsable por el desarrollo de las prácticas necesarias para el cumplimiento de la política, así como de su difusión y control.

Cada Gerente es responsable de hacer cumplir la presente Política en su área.

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 los Gerentes de los departamentos que administren la relación con el proveedor.

Los eventuales apartamientos de la política deberán ser registrados como no conformidades de acuerdo a los procedimientos vigentes.

4.2. Definición de los componentes a proteger.

Activo - Aquello que tenga valor para la organización.

Disponibilidad - Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Confidencialidad - Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

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

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 seguridad de la información - Ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información o la falla de salvaguardas, o una situación previamente desconocida que pueda ser relevante para la seguridad.

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.

Software de base - Corresponde a programas utilitarios.

4.3. Seguridad Física y Lógica de la Información:

Control de acceso: El acceso físico a las distintas áreas de la empresa donde se encuentran activos de información estará regida por el Procedimiento de Acceso Físico, en el que se detallan los accesos restringidos por zona. – **Este control, por razones de fuerza mayor, está inactivado durante el plazo de vigencia de las medidas sanitarias**

El acceso a los equipos informáticos personales será definido y autorizado por cada Gerente de Departamento y será su responsabilidad que cada equipo se utilice de acuerdo a lo definido, tanto en el personal asignado como en los sistemas o servicios informáticos autorizados. Los escritorios deben permanecer libres de información confidencial que no se esté utilizando para el trabajo (Escritorios limpios), y los equipos informáticos deben permanecer bloqueados en ausencia de sus usuarios.

El acceso a los sistemas informáticos de República AFAP desde dispositivos remotos (sean fijos o móviles) deberá realizarse utilizando canales seguros, de forma tal que el tráfico de datos se

realice de forma cifrada para impedir que los mismos puedan ser accedidos o adulterados por personas no autorizadas.

El equipamiento y sus datos estarán protegidos en todo momento contra ataques del exterior mediante los sistemas de Anti-Virus, firewalls y otro tipo de protección física y lógica que se considere adecuada y quede establecida en los contratos con proveedores o en las instalaciones propias.

Todo el software disponible en la empresa para el cumplimiento de las funciones de sus trabajadores deberá estar respaldado por los contratos de uso (licencias) adecuadas y actualizadas.

La adquisición, arrendamiento o contratación en outsourcing de todos los elementos de informática y manejo de la información se realizarán de acuerdo a los procedimientos vigentes en materia de compras y con proveedores que aseguren la suficiente calidad y seguridad de sus productos y servicios.
Los equipos de propiedad de la República AFAP, no deberán superar una vida útil adecuada a efectos de su eficiencia. Esta vida útil se estima en 5 años y todo equipamiento que supere dicha antigüedad deberá contar con autorización específica. El software de base (Sistemas operativos), el aplicativo específico (MS-Office y otras aplicaciones de escritorio) y en general los programas utilitarios deberán mantener una actualización media de mercado no apartándose más de una versión de la última oficialmente liberada al mercado salvo situaciones especiales.

La asignación de los equipos personales será definida por el personal de la División Tecnología, y eventualmente por el Gerente de Gestión, de acuerdo con la situación particular de cada PC y las necesidades de cada usuario. No se requiere para ello registro.

Los soportes de información obsoletos se formatearán, destruirán o inutilizarán de acuerdo al destino previsto.

5. CLASIFICACIÓN DE LA INFORMACIÓN

Los activos de información en República AFAP S.A. se clasifican de acuerdo a un criterio de confidencialidad. A estos efectos, cada elemento de información es clasificado por su propietario (siendo el propietario de un activo de información el propietario del proceso que lo genera).

Los grados de clasificación de información son los siguientes:

a) Público – Información que puede ser accedida por CUALQUIER persona, pertenezca o no República AFAP S.A.
b) Interno – Información que puede ser accedida por CUALQUIER colaborador de República AFAP S.A.
c) Confidencial – Información que puede ser accedida por un MIEMBRO de un grupo definido por el propietario de la información.

La clasificación se evidencia por el nivel de acceso de cada documento o activo de información.

Los datos personales de afiliados y colaboradores, así como cualquier otra información personal que se recopile en función de la normal actividad de la empresa, es considerada por esta política como “Confidencial”, y no puede utilizarse con ninguna otra finalidad que aquella para la que fue recopilada, respetándose íntegramente la privacidad de las personas.

Esto rige también para todo tipo de comunicaciones, como cartas, correos electrónicos, mensajes de texto, o cualquier otro medio tecnológico que pudiera utilizarse como medio de comunicación.

En este contexto, toda la información confidencial que se transporta en medios físicos fuera de las instalaciones de República AFAP se protege cifrándose con algoritmos simétricos, utilizando claves que deben ser comunicadas por separado.

6. DEL CONTROL Y LA RESPONSABILIDAD

6.1. Del Oficial de Seguridad: Están establecidos en su Perfil de Cargo, y en particular, es el responsable operativo directo del cumplimiento y control de la presente Política, así como de sugerir las medidas tendientes a mejorar el Sistema Integrado de Gestión.
6.2. Del Usuario: El usuario final es responsable por el uso indebido del equipo a su disposición y por el incumplimiento de la presente política en el resultado de sus acciones. (acceso a sitios o a información no autorizada; descarga de software no autorizado expresamente y/o sin licencia adecuada, transmisión de información eventualmente ofensiva; etc.).

6.3. Todos: Está prohibido usar el usuario y contraseña de otra persona o compartir su usuario y contraseña con otra persona.

6.4. De la Div. Tecnología: La División será responsable de implementar reportes de uso de los diferentes equipos personales y de programas utilitarios privilegiados que puedan estar en capacidad de anular el sistema y los controles de aplicación, elevando antecedentes de uso indebido a los respectivos Gerentes de Departamento.

En estos reportes deberá indicarse:

6.4.1. Software en uso, sin autorización de la empresa y/o sin licencia habilitante.

6.4.2. Mal uso del equipo entendiendo por tal una exigencia técnica para la que el equipo no está dimensionado y puede aparejar mal funcionamiento del mismo.

6.4.3. Desconocimiento técnico del usuario respecto al uso adecuado de los equipos y el software específico para la función que desempeña, de forma de prever la capacitación adecuada.

En cada caso, el Gerente de Departamento definirá las acciones necesarias de acuerdo con el Gerente de Gestión.

7. PRÁCTICAS A CUMPLIR

a. Se deben establecer anualmente objetivos con relación a la Seguridad de la Información.
b. El Área de Prevención y Gestión del Riesgo, según sus criterios establecidos, debe desarrollar un proceso de análisis del riesgo y de acuerdo a su resultado, indicar que se implementen las acciones correspondientes con el fin de tratar los riesgos que se consideren inaceptables.
c. 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.
d. Se debe cumplir con los requisitos del negocio, legales o reglamentarios y las obligaciones contractuales de seguridad y tratamiento de la información.
e. Se debe brindar concientización y entrenamiento en materia de seguridad de la información a todo el personal.
f. Se deben establecer los medios necesarios para garantizar la continuidad del negocio de la empresa.
g. Se registrará cualquier apartamiento de esta política o cualquier política o procedimiento del SGSI.
h. Todo colaborador es responsable de reportar las violaciones a la seguridad, confirmadas o sospechadas.
i. Todo colaborador es responsable de preservar la confidencialidad, integridad y disponibilidad de los activos de información en cumplimiento de la presente política y de las políticas y procedimientos inherentes al Sistema de Gestión de la Seguridad de la Información.
j. El Oficial de Seguridad de la Información es responsable directo sobre el mantenimiento de esta política, por brindar consejo y guía para su implementación, e investigar toda violación reportada por el personal.
k. Contar con los elementos de resguardo de los sistemas de información necesarios para eliminar o minimizar todos los riesgos sobre la información y la continuidad de su procesamiento de acuerdo a los sistemas definidos.
l. Contar con elementos de detección para los riesgos de seguridad en los sistemas de información, los que deberán ser analizados y evaluados a fin de lograr una rápida respuesta minimizando las consecuencias de la posible falla.
m. 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 invitados a suscribirla. Para aquellos proveedores cuya relación contractual comience luego de la vigencia de esta política, esta suscripción será obligatoria.
n. 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.

o. Los usuarios están impedidos de realizar la instalación en sus equipos personales de cualquier software o hardware no autorizado por la Empresa, y que no que no cuente con las licencias adecuadas cuando esto sea aplicable.
p. No se permite la copia de bases de datos en equipos de terceros, independientemente de los acuerdos de confidencialidad firmados, salvo cuando es un requisito propio del servicio. Los colaboradores de RAFAP tienen vedado transportar bases de datos de la empresa en equipos o soportes de propiedad personal salvo en situaciones de emergencia.
q. Se debe definir, establecer, implementar, controlar, mantener y mejorar un procedimiento que permita mantener un ambiente seguro de desarrollo.
r. Los proyectos, desarrollos y cambios a sistemas deben involucrar al Oficial de Seguridad para control.

La Alta Dirección considera como parte de la Política de Seguridad de la Información el cumplimiento de las prácticas generales presentes en el **Código de ética,** así como las particulares que se enumeran en el **Manual del Sistema Integrado de Gestión**.

8. DIFUSIÓN

Esta Política y sus documentos relacionados deben revisarse y difundirse como mínimo una vez por año a toda la organización. Respecto a los nuevos ingresos de colaboradores, cuando falten más de 1 mes para la instancia de difusión, recibirán, además de la presente política, una charla de inducción sobre este tema. Esta charla también se realizará en los casos de colaboradores que por promoción o cambio de área pasen a tener acceso de mayor privilegio a información confidencial.

9. Implantación de la política

El Departamento de Gestión apoyará a los demás Departamentos en el cumplimiento de esta política, realizando las capacitaciones que sean necesarias, sin perjuicio de la obligación de cada Gerente de asegurar que el personal a su cargo cumpla con esta política (4.1), así como que disponga de los permisos necesarios para el desarrollo de sus tareas.

10. Clasificación de la presente política.

La Política de Seguridad de la Información de República AFAP S.A. es de carácter público, 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.

11. 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.