1. OBJETIVO

Establecer los principios, criterios y responsabilidades que orientan el tratamiento de datos personales en la organización, con la finalidad de garantizar su adecuada protección durante su recolección, registro, uso, almacenamiento, conservación, consulta, transferencia y eliminación, de conformidad con la normativa peruana aplicable.

2. ALCANCE

La presente política es de aplicación obligatoria para todas las áreas, sedes, unidades de negocio y empresas de Swiss Capitals Group que la adopten, así como para sus trabajadores, funcionarios, practicantes y terceros que, en el desarrollo de sus actividades, tengan acceso o realicen tratamiento de datos personales por cuenta de la organización.

Comprende el tratamiento de datos personales de clientes, potenciales clientes, proveedores, representantes y personas de contacto, postulantes, trabajadores, ex trabajadores, visitantes, usuarios, asistentes a eventos, contactos comerciales, público en general y demás personas naturales cuyos datos sean tratados por la organización.

3. REFERENCIAS NORMATIVAS

- Constitución Política del Perú, en lo relativo al derecho fundamental a la protección de la información personal.
- Ley N.° 29733, Ley de Protección de Datos Personales.
- Reglamento de la Ley N.° 29733, aprobado mediante Decreto Supremo N.° 016-2024-JUS,
- Resolución Directoral N.° 019-2013-JUS/DGPDP, Directiva de Seguridad de la Información,
- Resolución Directoral N.° 02-2020-JUS/DGTAIPD, Directiva sobre el Tratamiento de Imágenes a través de Sistemas de Videovigilancia,
- Guía de observancia del deber de informar, emitida por la Autoridad Nacional de Protección de Datos Personales y demás normas complementarias, modificatorias o sustitutorias que resulten aplicables.

La aplicación de esta política deberá adecuarse a las disposiciones legales vigentes en cada momento, sin perjuicio de las obligaciones contractuales o sectoriales que correspondan.

4. DEFINICIONES

- Dato personal: Toda información sobre una persona natural que la identifica o la hace identificable mediante medios que puedan ser razonablemente utilizados.
- Dato sensible: Dato personal que, por su naturaleza, requiere un nivel especial de protección, de acuerdo con la normativa aplicable.
- Titular de datos personales: Persona natural a quien corresponden los datos personales objeto de tratamiento.

- Tratamiento de datos personales: Cualquier operación o conjunto de operaciones que permita recopilar, registrar, organizar, almacenar, conservar, consultar, utilizar, comunicar, transferir, modificar, bloquear, suprimir o eliminar datos personales.
- Banco de datos personales: Conjunto organizado de datos personales, automatizado o no, cualquiera sea la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.
- Responsable del tratamiento: Persona natural, persona jurídica de derecho privado o entidad pública que decide sobre la finalidad y los medios del tratamiento de datos personales, conforme a la normativa aplicable.
- Encargado del tratamiento: Persona natural o jurídica que realiza tratamiento de datos personales por cuenta del responsable.
-

5. PRINCIPIOS

El tratamiento de datos personales deberá sujetarse, como mínimo, a los siguientes principios:

- Legalidad: los datos personales deben ser obtenidos y tratados por medios lícitos y conforme a la normativa aplicable.
- Consentimiento: cuando sea exigible, el tratamiento deberá contar con el consentimiento previo, informado, expreso e inequívoco del titular.
- Finalidad: los datos personales serán recopilados para finalidades determinadas, explícitas y lícitas, y no serán utilizados de manera incompatible con dichas finalidades.
- Proporcionalidad: solo deberán tratarse los datos que resulten adecuados, relevantes y no excesivos respecto de la finalidad para la cual fueron obtenidos.
- Calidad: los datos deberán mantenerse exactos, actualizados, necesarios y pertinentes para la finalidad del tratamiento.
- Seguridad: se adoptarán medidas técnicas, organizativas y físicas razonables para evitar la pérdida, uso indebido, alteración, acceso no autorizado o divulgación de los datos personales.
- Disposición de recurso: los titulares deberán contar con mecanismos para ejercer los derechos que la normativa les reconoce.
- Nivel de protección adecuado: la comunicación o transferencia de datos deberá realizarse preservando un nivel de protección compatible con la normativa aplicable.
-

6. LINEAMIENTOS

6.1. Lineamientos generales

a. Recolección de datos personales

La recolección de datos personales deberá realizarse únicamente cuando exista una finalidad legítima vinculada con las actividades de la organización. El área responsable deberá procurar que la información solicitada sea estrictamente necesaria para la finalidad informada y que se utilicen medios institucionales o previamente autorizados.

b. Información al titular y consentimiento

Antes o al momento de la recolección, el titular deberá recibir la información que resulte exigible respecto del tratamiento de sus datos, conforme a lo establecido en los artículos 14 y 18 de la Ley N.° 29733. Cuando el consentimiento constituya la base que habilita el tratamiento, este deberá obtenerse de manera válida, inequívoca y expresa y conservarse evidencia suficiente que permita acreditarlo.

c. Uso y finalidad

Los datos personales solo podrán utilizarse para las finalidades que justificaron su obtención o para aquellas permitidas por ley. Queda prohibido utilizar información personal para fines particulares, ajenos a las funciones asignadas o incompatibles con la finalidad comunicada al titular. En caso se requiera realizar el tratamiento para finalidades adicionales, deberá solicitarse el consentimiento del titular en cumplimiento con la normativa aplicable.

d. Almacenamiento y custodia

Los datos personales deberán ser almacenados en medios físicos o digitales autorizados por la organización, bajo condiciones que permitan preservar su confidencialidad, integridad y disponibilidad. Los documentos físicos deberán mantenerse en espacios seguros y los registros digitales deberán conservarse en sistemas o repositorios institucionales.

e. Acceso y confidencialidad

El acceso a datos personales se otorgará exclusivamente a quienes lo requieran para el cumplimiento de sus funciones, aplicando criterios de necesidad de conocer y mínimo privilegio. Las personas autorizadas deberán mantener la confidencialidad de la información incluso después de concluida su relación laboral, contractual o comercial con la organización. Para ello, se deberán suscribir los compromisos de confidencialidad correspondientes.

f. Actualización y calidad de la información

Las áreas responsables deberán procurar que los datos personales se mantengan actualizados y sean corregidos cuando se detecten inexactitudes o cuando el titular comunique información válida que requiera rectificación.

g. Comunicación, transferencia y tratamiento por terceros

La comunicación o transferencia de datos personales a terceros deberá responder a una finalidad legítima, contar con la habilitación legal correspondiente y observar las medidas de protección exigibles. Los terceros que traten datos por cuenta de la organización deberán asumir obligaciones de confidencialidad y seguridad acordes con la naturaleza de la información tratada.

h. Comunicación de datos a autoridades competentes

La organización podrá comunicar o proporcionar datos personales a autoridades administrativas, judiciales, fiscales, policiales, regulatorias u otras entidades públicas competentes cuando exista una obligación legal, mandato judicial, requerimiento válido emitido en ejercicio de sus competencias o cuando la normativa aplicable lo autorice. La entrega de información se limitará a los datos que resulten necesarios y pertinentes para atender el requerimiento correspondiente y se realizará observando las medidas de confidencialidad y seguridad aplicables.

i. Conservación y eliminación

Los datos personales se conservarán durante el tiempo necesario para cumplir la finalidad que motivó su tratamiento y las obligaciones legales o contractuales aplicables. Una vez cumplida dicha finalidad y vencidos los plazos de conservación correspondientes, los datos deberán ser eliminados, destruidos, anonimizados o bloqueados, según corresponda y resulte legalmente procedente.

j. Medidas de seguridad

La organización deberá implementar medidas legales, técnicas, organizativas, humanas y físicas razonables para proteger los datos personales frente a accesos no autorizados, pérdida, destrucción, alteración, copia, divulgación o cualquier tratamiento indebido. Estas medidas deberán revisarse cuando existan cambios relevantes en los sistemas, procesos o riesgos identificados.

k. Incidentes de seguridad

Cualquier trabajador o tercero autorizado que tome conocimiento de una pérdida, acceso indebido, envío erróneo, exposición, sustracción o cualquier evento que pueda comprometer datos personales deberá comunicarlo de inmediata su jefatura y a las áreas internas designadas para su evaluación, contención y tratamiento.

Se deberá notificar a la Autoridad Nacional de Datos Personales los incidentes de seguridad producidos, dentro del plazo máximo de cuarenta y ocho (48) horas contadas desde que se haya tomado conocimiento del incidente.

6.2. Derechos de los titulares

La organización reconoce y garantiza el ejercicio de los derechos que la normativa de protección de datos personales concede a los titulares, incluyendo los derechos de información, acceso, actualización, inclusión, rectificación, supresión o cancelación, oposición y portabilidad, cuando corresponda conforme a la normativa vigente.

Las solicitudes deberán ser atendidas a través de los canales institucionales que la organización establezca. Antes de entregar, modificar o suprimir información personal, deberá verificarse la identidad del solicitante, mediante la entrega de copia de DNI o documento equivalente,y observarse los requisitos y plazos previstos por la normativa aplicable.

6.3. Tratamiento según la relación con la organización

La organización podrá tratar datos personales en el marco de sus relaciones e interacciones comerciales, laborales, contractuales, administrativas, institucionales y de seguridad, así como cuando una persona interactúe con sus instalaciones, actividades, eventos, formularios, plataformas o canales de atención, siempre que exista una finalidad legítima y se respeten los principios establecidos en esta política.

- Clientes y potenciales clientes: para gestionar relaciones comerciales, contractuales, atención, prestación de servicios, facturación y demás actividades vinculadas con la relación de negocio.
- Proveedores y terceros: para evaluar, contratar, gestionar, pagar y dar seguimiento a bienes o servicios, así como para administrar la relación contractual correspondiente.
- Postulantes: para desarrollar procesos de selección y evaluación de candidatos a puestos de trabajo.

- Trabajadores y ex trabajadores: para administrar la relación laboral, obligaciones legales, planillas, beneficios, seguridad y demás actividades propias de la gestión de personas.
- Visitantes: para gestionar su ingreso, permanencia y salida de las instalaciones, así como para fines de seguridad, identificación y control de acceso.
- Participantes de eventos y actividades: para gestionar su registro, inscripción, participación, atención y demás actividades vinculadas con los eventos, talleres, charlas, activaciones u otras actividades organizadas o gestionadas por la organización.
- Público en general y usuarios de canales de atención: para atender consultas, solicitudes u otras interacciones realizadas mediante formularios, sitios web, redes sociales, plataformas u otros canales habilitados por la organización, de acuerdo con las finalidades informadas y la normativa aplicable.
- Las categorías específicas de datos, medios de recolección, repositorios, responsables, plazos de conservación y controles operativos podrán ser desarrollados en documentos internos posteriores y en las políticas de privacidad correspondientes respetando en todo momento los criterios establecidos en la presente política.

7. ROLES Y RESPONSABILIDADES

La Alta Dirección es responsable de promover el cumplimiento de la presente Política y asegurar la disponibilidad de los recursos necesarios para la adecuada protección de los datos personales.

Las áreas que, por la naturaleza de sus funciones, recopilen, utilicen, almacenen o tengan acceso a datos personales son responsables de efectuar su tratamiento conforme a la presente Política y a la normativa vigente.

Todo trabajador, colaborador o tercero autorizado que tenga acceso a datos personales deberá mantener su confidencialidad, utilizar la información únicamente para las finalidades autorizadas y cumplir las medidas de seguridad establecidas por la Organización.

El área competente en materia de tecnología y seguridad de la información brindará soporte para la implementación y mantenimiento de las medidas técnicas necesarias para proteger los datos personales.

8. RIESGOS Y CUMPLIMIENTO

El incumplimiento de la presente política podrá dar lugar a medidas administrativas, disciplinarias, contractuales o legales, según la naturaleza de la infracción y la relación del responsable con la organización, sin perjuicio de las responsabilidades previstas por la normativa aplicable.

9. COMUNICACIÓN Y CAPACITACIÓN

La organización promoverá actividades de inducción, capacitación o sensibilización para las personas que, por la naturaleza de sus funciones, tengan acceso o realicen tratamiento de datos personales. La periodicidad y profundidad de dichas actividades se definirán según el nivel de exposición y responsabilidad de cada puesto.

10. MONITOREO

La presente política constituye el marco general para la protección y tratamiento de datos personales dentro de la organización. A partir de sus disposiciones, las áreas responsables deberán desarrollar, documentar y mantener los procedimientos, instructivos, formatos, registros y controles operativos que resulten necesarios para aplicar estos lineamientos en sus respectivos procesos.

Todo documento posterior relacionado con recolección, almacenamiento, acceso, uso, conservación, transferencia, seguridad o eliminación de datos personales deberá guardar concordancia con esta política. En caso de diferencia, deberá prevalecer la normativa aplicable y revisarse el documento interno correspondiente.

Se realizará una auditoría de cumplimiento al menos una vez al año, o ante cambios normativos o tecnológicos relevantes

Giannoni Melosevich Pierre
Gerente General

Giannoni Melosevich Carolina
Gerente General Adjunta