1. PRESENTACIÓN Y OBJETO

Sicurex Ltda., con domicilio en Bogotá D.C., y debidamente aprobada por la Superintendencia de Vigilancia y Seguridad Privada mediante Resolución No., 20214440117567 del 30/12/2021, en adelante "La Escuela", reconoce la importancia fundamental de la **protección de datos personales** como un derecho constitucional y un pilar esencial para la confianza en la sociedad digital.

La presente política tiene como objeto desarrollar el derecho constitucional de todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el Artículo 15 de la Constitución Política, así como el derecho a la información consagrado en el Artículo 20 de la misma.

Asimismo, establece los principios, lineamientos y procedimientos aplicables para el **tratamiento adecuado y responsable de la información personal** que recolecta, almacena, usa, circula o suprime, garantizando la seguridad, confidencialidad, integridad y disponibilidad de dichos datos, y **demostrando su responsabilidad** frente a las obligaciones legales y regulatorias. Esta política es de **obligatorio cumplimiento** para La Escuela y todo su personal.

2. MARCO LEGAL APLICABLE

La presente política se rige por las siguientes normas colombianas en materia de protección de datos personales:

- **Artículo 15 de la Constitución Política de Colombia**: Establece el derecho a la intimidad personal y familiar, al buen nombre, y el derecho a conocer, actualizar y rectificar la información recogida en bases de datos.
- **Artículo 20 de la Constitución Política de Colombia**: Garantiza la libertad de expresar, difundir pensamiento y opiniones, e informar y recibir información veraz e imparcial.
- **Ley Estatutaria 1266 de 2008**: Primera ley que establece el hábeas data en Colombia, legislando el derecho a conocer, actualizar y rectificar la información personal, específicamente en el ámbito financiero.

- **Ley Estatutaria 1581 de 2012**: Piedra angular de la protección de datos personales en Colombia. Establece las disposiciones generales para la protección de datos personales, definiendo los principios, derechos y deberes relacionados con el tratamiento de datos personales, y garantiza los derechos de acceso, actualización, rectificación y supresión.
- **Decreto 1377 de 2013**: Regula parcialmente la Ley 1581 de 2012, estableciendo pautas para la autorización del tratamiento de datos y la atención de consultas y reclamos. Fue incorporado en el Decreto Único Reglamentario 1074 de 2015.
- **Ley 2157 de 2021**: Modifica y adiciona la Ley Estatutaria 1266 de 2008.
- **Decreto 1074 de 2015:** Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, que incorpora el Decreto 1377 de 2013.
- **Circular Externa No. 5 de 2017 de la Superintendencia de Industria y Comercio (SIC):** Que establece los estándares y condiciones para la transferencia internacional de datos personales.
- **Circular Externa No. 2 de 2024 de la Superintendencia de Industria y Comercio (SIC):** Que establece directrices sobre el tratamiento de datos personales en sistemas de Inteligencia Artificial (IA).
- **Resolución No. 20221300034257 de la Superintendencia de Vigilancia y Seguridad Privada:** Que modifica el Anexo Técnico de Requisitos y Requerimientos para la Homologación de los Proveedores del Sistema Integrado de Seguridad, especialmente en relación con el uso de biometría y seguridad de la información.
- **Ley 2300 de 2023**: Establece medidas para proteger el derecho a la intimidad de los consumidores.

3. DEFINICIONES

Para la correcta aplicación de esta política, se adoptan las siguientes definiciones:

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de sus datos personales.
- **Base de Datos:** Conjunto organizado de datos personales que es objeto de Tratamiento.

- **Dato Personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Dato Público:** Es el dato que no sea semiprivado, privado o sensible, y que puede ser consultado por cualquier persona de manera directa sin el consentimiento del titular.
- **Dato Semiprivado:** Dato cuyo conocimiento o divulgación puede interesar no solo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio.
- **Dato Privado:** Dato que por su naturaleza íntima o reservada solo es relevante para el Titular o su entorno más cercano.
- **Datos Sensibles:** Aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación. Incluyen, entre otros, el origen racial o étnico, orientación política, convicciones religiosas o filosóficas, pertenencia a sindicatos, organizaciones sociales, datos de salud, vida sexual y **datos biométricos**.
- **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realiza el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.
- **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decide sobre la base de datos y/o el Tratamiento de los datos.
- **Titular:** Persona natural cuyos datos personales son objeto de Tratamiento.
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- **Transferencia:** Ocurre cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor que también es Responsable del Tratamiento y se encuentra dentro o fuera del país.
- **Transmisión:** Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el Encargado por cuenta del Responsable.

SICUREX INSTITUTO DE SEGURIDAD METIS

- **Sistema Integrado de Seguridad (SIS):** Infraestructura tecnológica operada por una compañía del sector de Tecnologías de la Información, homologada por la Superintendencia de Vigilancia y Seguridad Privada, utilizada para la expedición de certificados de aptitud psicofísica, garantizando la identificación y validación de las personas mediante el uso de biometría dactilar, registro fotográfico, firma digital y geolocalización, entre otros.

4. PRINCIPIOS RECTORES DEL TRATAMIENTO DE DATOS PERSONALES

La Escuela, en su rol de Responsable del Tratamiento de Datos Personales, actúa con la diligencia de un **buen hombre de negocios** y se compromete a cumplir los siguientes principios:

- **Legalidad en materia de Tratamiento de datos:** El Tratamiento de datos es una actividad reglada que se sujeta a lo establecido en la ley y demás disposiciones que la desarrollan.
- **Finalidad:** El Tratamiento obedece a una finalidad legítima y específica, la cual será siempre informada al Titular. Los datos recolectados serán pertinentes y adecuados para el fin establecido.
- **Libertad:** El Tratamiento solo puede ejercerse con el **consentimiento previo, expreso e informado del Titular**. No se obtendrán o divulgarán datos personales sin esta autorización, salvo en los casos previstos por la ley.
- **Veracidad o Calidad:** La información sujeta a Tratamiento debe ser **veraz, completa, exacta, actualizada, comprobable y comprensible**. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
- **Transparencia:** Se garantiza el derecho del Titular a obtener información sobre la existencia y Tratamiento de sus datos en cualquier momento y sin restricciones.
- **Acceso y Circulación Restringida:** El Tratamiento se sujeta a los límites derivados de la naturaleza de los datos personales y la ley. Solo podrá hacerse por personas autorizadas y los datos no estarán disponibles en medios de divulgación masiva, salvo que el acceso sea técnicamente controlable.
- **Seguridad:** La información se manejará con **medidas técnicas, humanas y administrativas razonables** para otorgar seguridad a los registros, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Esto

incluye una **ciberseguridad activa** que va más allá del cumplimiento normativo, implicando detección, monitoreo, respuesta y prevención constantes.

- **Confidencialidad:** Todas las personas que intervengan en el Tratamiento de datos personales están obligadas a garantizar la reserva de la información, incluso después de finalizada su relación con La Escuela.

5. CATEGORÍAS ESPECIALES DE DATOS Y SU TRATAMIENTO

La Escuela recolecta datos personales de diferentes formas y a través de distintos canales, dependiendo de la naturaleza de la relación con el Titular (aspirantes, estudiantes, personal administrativo, docentes, proveedores, entre otros).

- **Datos Sensibles:**
    - La Escuela podrá recolectar y tratar datos sensibles, definidos como aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar discriminación (ej. origen racial o étnico, convicciones políticas/religiosas/filosóficas, pertenencia a organizaciones, datos de salud, vida sexual y **datos biométricos**).
    - El **tratamiento de datos sensibles está prohibido**, **excepto** cuando el Titular haya dado su **autorización explícita** a dicho Tratamiento. Otras excepciones incluyen salvaguardar el interés vital del Titular (si está física o jurídicamente incapacitado), actividades legítimas de fundaciones/ONGs (con garantías y sin suministro a terceros), reconocimiento/ejercicio/defensa de un derecho en un proceso judicial, o fines históricos/estadísticos/científicos (con supresión de identidad).
    - **En particular, dada la naturaleza de La Escuela y la Resolución No. 20221300034257 de la Superintendencia de Vigilancia y Seguridad Privada, se requerirá el uso de biometría dactilar, registro fotográfico (reconocimiento facial ISO/IEM19794-5) y firma digital para la validación de identidad en los procesos de certificación de aptitud psicofísica de vigilantes, escoltas y supervisores**. **Estos son datos sensibles**, y su tratamiento se realizará **únicamente con la autorización previa, libre, informada, voluntaria y explícita del Titular**, informándole que no está obligado a autorizar su tratamiento. La finalidad de su uso será la validación

de identidad para la prevención de fraude, lavado de activos, financiación del terrorismo y otras actividades ilegales para la contratación de servicios.

- La Escuela conservará prueba del cumplimiento de lo previsto en la obtención de esta autorización.

- **Datos de Niños, Niñas y Adolescentes:**
  - Está **proscrito el Tratamiento de datos personales de niños, niñas y adolescentes**, **salvo aquellos datos que sean de naturaleza pública**.
  - El Tratamiento de su información se realizará **únicamente con el consentimiento de sus padres, tutores o personas con patria potestad**, asegurando en todo momento el respeto a sus derechos prevalentes y proporcionando información sobre el uso responsable y seguro de sus datos personales.
- **Uso de Algoritmos, Inteligencia Artificial y Big Data:**
  - En caso de utilizar IA para análisis de tendencias, predicción de comportamiento, elaboración de perfiles o mejora de servicios, La Escuela garantizará **transparencia** sobre las finalidades, obtendrá el **consentimiento explícito** de los usuarios, y desarrollará mecanismos para **monitorear y auditar** el uso de la IA para asegurar el respeto a los derechos de los Titulares.
  - Se aplicarán técnicas de **anonimización** y **seudonimización** siempre que sea posible para reducir riesgos.
  - Se realizarán **Evaluaciones de Impacto en la Protección de Datos (PIA)** antes de implementar nuevos sistemas de IA si conllevan un alto riesgo para los derechos y libertades de los Titulares.

6. RESPONSABILIDADES Y GESTIÓN INTERNA

La Escuela ha adoptado un **Programa de Protección de Datos Personales** y, como administrador societario, cumple un papel esencial en la protección de datos.

- **Principio de Responsabilidad Demostrada ("Accountability"):** La Escuela adoptará **medidas útiles, oportunas, eficientes y demostrables** para acreditar el cumplimiento total y correcto de la regulación, siendo capaz de demostrar, a petición

de la Superintendencia de Industria y Comercio (SIC), que ha implementado medidas apropiadas y efectivas.

- **Políticas Internas Efectivas:** La Escuela cuenta con **políticas internas claras y procedimientos** para el Tratamiento de datos personales, incluyendo un **manual interno de políticas y procedimientos** para la atención de consultas y reclamos.
- **Equipo de Protección de Datos Personales:** Se ha designado un **Oficial de Protección de Datos Personales** y un equipo multidisciplinario para liderar el Programa de Protección de Datos Personales. Sus funciones incluyen definir e implementar políticas, fomentar la cultura de protección de datos, identificar y evaluar amenazas y riesgos, diseñar estrategias de prevención, realizar auditorías y atender solicitudes de Titulares.
- **Gestión de Riesgos y Evaluación de Impacto:** El manual interno de políticas incluye un componente de **gestión de riesgos** para identificar vulnerabilidades y enfocar recursos en su mitigación. Se realizan evaluaciones de riesgos y de impacto en la protección de datos (PIA).
- **Fortalecimiento Continuo de Medidas de Seguridad de la Información:** Se manejará la información con **medidas técnicas, humanas y administrativas razonables** para evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Esto incluye:
    - **Controles de acceso** verificación e identificación del personal que ingresa a las instalaciones.
    - **Conexiones cifradas y seguras (se contará con software antivirus actualizado)**.
    - **Protección contra código malicioso**. **(se contará con software antivirus actualizado)**.
    - **Separación de ambientes** (desarrollo, calidad, pruebas) con software de seguridad.
    - **Registros de auditoría o *logs***.
    - **Respaldo de la información** de las bases de datos y la aplicación.
    - Un plan de respuesta a incidentes.

SICUREX INSTITUTO DE SEGURIDAD METIS

- **Monitoreo Continuo:** Se realiza un monitoreo continuo para controlar, administrar e informar sobre el riesgo asociado con las prácticas de gestión de datos personales y para determinar el grado de cumplimiento de políticas y prácticas.
- **Capacitación y Sensibilización:** Se asegura que las herramientas de implementación, entrenamiento y programas de sensibilización sean conocidos y promovidos. El personal es **capacitado y consciente de sus responsabilidades legales**.

7. AUTORIZACIÓN DEL TITULAR

- **Consentimiento Informado:** El Tratamiento de datos solo se hará con el **consentimiento previo, expreso e informado del Titular**, que se obtendrá por cualquier medio que pueda ser consultado posteriormente.
- **Deber de Informar:** Al momento de solicitar la autorización, La Escuela informará al Titular de manera clara y expresa sobre el Tratamiento y finalidad de sus datos personales, el carácter facultativo de la respuesta a preguntas sobre datos sensibles o de niños/as y adolescentes, sus derechos como Titular y la información de contacto de La Escuela.
- **Excepciones a la Autorización:** La autorización del Titular no será necesaria en casos como información requerida por entidad pública o judicial, datos de naturaleza pública, urgencia médica/sanitaria, fines históricos/estadísticos/científicos (con supresión de identidad) o datos relacionados con el Registro Civil.
- **Revocatoria y Supresión:** Los Titulares podrán solicitar en todo momento la supresión parcial o total de sus datos y/o revocar la autorización otorgada, mediante un reclamo. Esta solicitud **NO PROCEDERÁ CUANDO EL TITULAR TENGA UN DEBER LEGAL O CONTRACTUAL DE PERMANECER EN LA BASE DE DATOS**.

8. DERECHOS DE LOS TITULARES

Los Titulares de los datos personales tienen los siguientes derechos:

- **Conocer, actualizar y rectificar** sus datos personales frente a La Escuela o su Encargado del Tratamiento.
- **Solicitar prueba de la autorización** otorgada, salvo excepciones legales.

SICUREX INSTITUTO DE SEGURIDAD METIS

- **Ser informado** sobre el uso dado a sus datos personales, previa solicitud.
- **Presentar quejas** ante la Superintendencia de Industria y Comercio por infracciones a la ley.
- **Revocar la autorización y/o solicitar la supresión** del dato cuando el Tratamiento no respete los principios, derechos y garantías constitucionales y legales.
- **Acceder en forma gratuita** a sus datos personales que hayan sido objeto de Tratamiento.

9. PROCEDIMIENTOS PARA EL EJERCICIO DE LOS DERECHOS

Los Titulares o sus causahabientes podrán presentar consultas y/o reclamos ante La Escuela, previa validación de su identidad, a través de los canales que La Escuela disponga (ej. página web, correo electrónico, dirección física, etc.).

- **Consultas:**
  - La Escuela responderá las consultas en un término máximo de **diez (10) días hábiles** contados a partir de la fecha de recibo.
  - Si no es posible atender la consulta en dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá, la cual no superará los **cinco (5) días hábiles** siguientes al vencimiento del primer término.
  - Las consultas son gratuitas al menos una vez por mes calendario o por modificaciones sustanciales de la Política. Para consultas más frecuentes, se podrán cobrar costos de envío y reproducción.
- **Reclamos:**
  - Los reclamos por corrección, actualización, supresión o presunto incumplimiento de la ley se presentarán con la información requerida (nombre, identificación, hechos, objeto, dirección, documentos).
  - Si el reclamo está incompleto, se requerirá al interesado subsanar las fallas en **cinco (5) días hábiles**. Si en dos (2) meses no se subsana, se entenderá que ha desistido.

SICUREX INSTITUTO DE SEGURIDAD METIS

- Una vez recibido el reclamo completo, se incluirá la leyenda "reclamo en trámite" en la base de datos en un término no mayor a **dos (2) días hábiles**.
- El término máximo para atender el reclamo será de **quince (15) días hábiles**. Si no es posible, se informará la demora y la nueva fecha, que no superará los **ocho (8) días hábiles** adicionales.
- El Titular solo podrá elevar queja ante la Superintendencia de Industria y Comercio una vez haya agotado el trámite de consulta o reclamo ante La Escuela.

10. TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES

- Toda transmisión de datos personales se regulará mediante un instrumento jurídico idóneo que identifique obligaciones y responsabilidades.
- La Escuela podrá **transmitir datos** a autoridades competentes, proveedores y aliados que cumplan con los mismos estándares de privacidad, y operadores de bancos de datos crediticios y financieros, para la prestación de servicios, cumplimiento de obligaciones contractuales, prevención de fraude, lavado de activos, financiación del terrorismo y otras actividades ilegales.
- Se **prohíbe la transferencia de datos personales a países que no proporcionen niveles adecuados de protección**. Un país ofrece un nivel adecuado de protección si su legislación cuenta con principios, derechos de titulares, deberes de Responsables/Encargados, procedimientos de protección y autoridades efectivas.
- La prohibición no regirá si el Titular ha autorizado expresamente la transferencia, por razones médicas, operaciones bancarias, tratados internacionales, ejecución de contratos o medidas precontractuales con autorización, o por exigencia legal para la salvaguarda del interés público/defensa judicial.
- La Superintendencia de Industria y Comercio (SIC) ha emitido un listado de países que considera con un nivel adecuado de protección (ej. Unión Europea, México, República de Corea, Costa Rica, Serbia, Perú, Noruega, Islandia, Estados Unidos).
- Incluso a países con un nivel adecuado, La Escuela, en virtud del principio de responsabilidad demostrada, debe ser capaz de demostrar medidas apropiadas y efectivas para garantizar el adecuado Tratamiento y seguridad de los datos transferidos.

SICUREX INSTITUTO DE SEGURIDAD METIS

11. CONSERVACIÓN DE LA INFORMACIÓN PERSONAL

La Escuela conservará los datos personales por los períodos necesarios para cumplir con las finalidades informadas y las obligaciones contractuales y legales. Los datos personales serán almacenados en las bases de datos de La Escuela:

- Mientras subsista la obligación legal, reglamentaria o regulatoria que obligue al almacenamiento y conservación, con una vigencia máxima de **diez (10) años**.
- Diez (10) años luego de culminado el vínculo contractual con el Titular.
- El Tratamiento de datos personales en la nube (cloud computing) solo se realizará en una nube ubicada en Colombia, o en su defecto, en los países que cuentan con un nivel adecuado de protección de datos personales según la Circular Externa No. 5 de 2017 de la SIC.

12. MODIFICACIONES A LA POLÍTICA

La Escuela se reserva el derecho de modificar esta Política de Tratamiento de la Información, en su totalidad o parcialmente. En caso de **cambios sustanciales** que afecten la identificación de La Escuela o la finalidad del Tratamiento de los datos personales, los cuales puedan afectar el contenido de la autorización, La Escuela comunicará estos cambios a los Titulares, antes o al momento de implementar las nuevas políticas, y **obtendrá una nueva autorización** cuando el cambio se refiera a la finalidad del Tratamiento.

13. VIGENCIA

La presente Política de Tratamiento de Datos Personales entra en vigor a partir de la fecha de su publicación y será actualizada periódicamente según los cambios normativos y operacionales.

SICUREX INSTITUTO DE SEGURIDAD METIS

JOSE DAVID AMORTEGUI JIMÉNEZ

Representante Legal

SICUREX
INSTITUTO DE SEGURIDAD METIS