POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES DE GRUPO SEGURITECH

ÍNDICE

1. OBJETIVO

La presente Política de Protección de Datos Personales tiene por objetivo establecer los procedimientos, lineamientos y directrices que deberán observar todos los colaboradores y terceros relacionados con las actividades de Grupo Seguritech Privada S.A.P.I. de C.V., y de sus filiales, subsidiarias o afiliadas (Grupo Seguritech o el Grupo) para el debido Tratamiento y protección de los Datos Personales de los cuales el Grupo sea Responsable en términos de las disposiciones legales aplicables.

2. MARCO REGULATORIO

Esta Política busca implementar de manera amplia y vinculante dentro de Grupo Seguritech lo dispuesto por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, su Reglamento y demás disposiciones legales y regulatorias complementarias en la materia.

3. DEFINICIONES

A lo largo de la presente Política, los siguientes términos tendrán el significado que se indica para cada caso a continuación:

1. **Aviso de Privacidad:** Es el documento a disposición del Titular de la información de forma física, electrónica o en cualquier otro formato generado por el responsable, a partir del momento en el cual se recaben sus Datos Personales, con el objeto de informarle los propósitos del tratamiento que dará Grupo Seguritech a sus Datos Personales, disponible en: https://avisos.seguritech.com.
2. **Base de Datos:** Conjunto ordenado de Datos Personales referentes a una persona identificada o identificable condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.
3. **Consentimiento:** Manifestación de la voluntad libre, específica e informada del Titular de los Datos Personales mediante la cual se efectúa el tratamiento de estos.
4. **Datos Personales:** Cualquier información concerniente a una persona física identificada o identificable.

5. **Derechos ARCO:** Son los derechos de Acceso, Rectificación, Cancelación y Oposición a que tienen derecho los Titulares de Datos Personales en términos de las disposiciones legales aplicables.
6. **Medidas de Seguridad:** Los mecanismos administrativos, técnicos y físicos que toda persona que trate Datos Personales debe implementar de conformidad con lo establecido en la presente política.
7. **Oficial de Protección de Datos:** Persona responsable de dar trámite a las solicitudes de los titulares para el ejercicio de los derechos a que se refiere la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
8. **Responsable:** Es la persona legalmente obligada a salvaguardar los Datos Personales, incluyendo a Grupo Seguritech y a cualquier persona que de Tratamiento a los datos dentro de la misma.
9. **Titular:** La persona física a quien corresponden los Datos Personales y que otorgó su Consentimiento para el Tratamiento generalmente a través del Aviso de Privacidad.
10. **Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.
11. **Transferencia:** Toda comunicación de Datos Personales realizada a persona distinta de la Titular, del responsable o encargado del tratamiento.

4. DATOS SENSIBLES

Los datos sensibles son aquellos Datos Personales que afectan la esfera más íntima del Titular, o cuya utilización indebida puede dar origen a discriminación o conlleve un riesgo grave para éste, incluyendo origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual, entre otros.

Cualquier Tratamiento de Datos Sensibles debe ser reportada inmediatamente a al Grupo a través del Oficial de Protección de Datos.

5. PRINCIPIOS

A lo largo del desempeño de sus actividades del día a día en la organización, se espera que todos los colaboradores y terceros de Grupo Seguritech se adhieran a y guíen cualquier actividad de Tratamiento de Datos Personales de conformidad con los siguientes principios:

PRINCIPIO	OBLIGACIÓN	DESCRIPCIÓN
Licitud	Todo tratamiento conforme a la ley	El principio de licitud obliga al responsable a que el tratamiento sea con apego y cumplimiento a la legislación mexicana y el derecho internacional.
Consentimiento	Se debe obtener previamente el consentimiento del titular	El responsable deberá obtener el consentimiento para el tratamiento de los datos personales. La solicitud del consentimiento deberá ir referida a finalidades determinadas conforme al aviso de privacidad. Cuando los datos se obtengan personalmente o de manera directa del titular, el consentimiento deberá ser previo al tratamiento. Por regla general el consentimiento se obtiene a través de la no oposición al aviso de privacidad.
Información	Se informa el tratamiento a través del aviso de privacidad	El responsable deberá dar a conocer al titular la información relativa a la existencia y características principales del tratamiento a que serán sometidos sus datos personales, lo que se realiza a través del aviso de privacidad.
Calidad	Las bases de datos deben estar actualizadas y correctamente integradas	Se cumple con el principio de calidad cuando las bases de datos personales tratados sean exactas, completas, pertinentes, correctas y actualizadas, según se requiera para la finalidad para la cual son tratados los datos personales.
Finalidad	Solo se pueden tratar datos personales para los fines establecidos en el aviso de privacidad	Los datos personales sólo podrán ser tratados para el cumplimiento de la finalidad establecida en el aviso de privacidad, misma que debe ser una finalidad clara, objetiva e inequívoca.
Lealtad	Se debe privilegiar en todo momento la protección de los datos personales	El principio de lealtad establece la obligación de tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad que debe existir en el tratamiento de cualquier dato personal. En caso de duda sobre si se permite o no realizar cualquier tratamiento, se debe privilegiar la protección de los datos personales.

Proporcionalidad	Sólo se deben tratar los datos que sean estrictamente necesarios	Sólo podrán ser objeto de tratamiento los datos que resulten necesarios, adecuados y relevantes para el fin para el cual fueron recabados. El responsable deberá realizar los esfuerzos razonables para que los datos personales sean los mínimos necesarios para la finalidad para la cual deben ser tratados.
Responsabilidad	Siempre existirá un responsable del tratamiento de los datos personales	Toda persona que trate datos personales debe velar y responder por los datos personales que se encuentren bajo su custodia o posesión y de adoptar las medidas de seguridad que se establecen más adelante en la presente Política.

6. LINEAMIENTOS PARA BASES DE DATOS

Para cualquier Base de Datos personales que se cree en la organización, todo colaborador o tercero relacionado con las actividades de Grupo Seguritech deberá observar las siguientes obligaciones:

1. Sólo se podrán crear Bases de Datos Personales cuando sea estrictamente necesario para desempeñar una función asignada a un área específica de Grupo y que, para ello, requiera dicha información.
2. Toda Base de Datos Personales será creada formalmente por las instrucciones de un responsable, que normalmente será el director responsable del área en cuestión (el "Responsable de la Base de Datos").
3. El Responsable de la Base de Datos, bajo su más estricta responsabilidad, deberá:
    a. Designar a uno o más Encargado(s) de administrar la Base de Datos, quien gestionará las autorizaciones para acceso a la Base de Datos únicamente dentro de los Usuarios que tengan necesidad de Tratar dicha Información.
    b. Asegurarse que la misma no contenga Datos Sensibles.
    c. Asumir la responsabilidad en último nivel de cualquier tratamiento que se dé a la Base de Datos y de las consecuencias que se deriven del mal uso de la misma.
    d. Establecer de manera formal las Medidas de Seguridad que deberán cumplir el Encargado y los Usuarios en todo momento a lo largo de

su Tratamiento de los Datos Personales contenida en la Base de Datos.

4. Por ninguna circunstancia se podrá compartir una Base de Datos en un correo de distribución general. El compartir una Base de Datos Personales en un correo de distribución general o a cualquier persona que no tengan la necesidad estricta de usar dichos Datos Personales para desempeñar una función concreta en los términos antes indicados, se considerará como una violación grave a lo establecido en la presente Política.
5. Toda Base de Datos debe ser revisada de manera periódica a efecto de asegurarse que la misma se encuentra actualizada y cuenta con los datos pertinentes y las Medidas de Seguridad adecuadas.
6. Toda Base de Datos debe encontrarse sujeta a un periodo de cancelación, después del cual se deberá analizar la necesidad de continuar tratando los Datos Personales, o si se puede proceder a su Bloqueo o eliminación.
7. El Bloqueo se realizará cuando no sea necesario continuar usando los Datos Personales pero tampoco se puedan eliminar. En este caso, solo las personas con las credenciales necesarias podrán acceder a la información para consulta eventual de conformidad con el Aviso de Privacidad.
8. De manera general, e independientemente de cualquier otra Medida de Seguridad que se adopte, toda Base de Datos debe estar protegida por una contraseña y/o debe estar gestionada a través de los mecanismos institucionales (Google Drive) que permitan la asignación de credenciales únicamente a las personas que deben Tratar los Datos Personales para cualquier finalidad legítima de conformidad con el Aviso de Privacidad correspondiente.
9. Todas las áreas que cuenten con Bases de Datos Personales deben reportar de manera formal al Oficial de Protección de Datos la existencia de la base de datos y las Medidas de Seguridad adoptadas, a efectos de que pueda emitir recomendaciones y asesorar respecto al correcto Tratamiento de los Datos Personales en cuestión.

7. MEDIDAS DE SEGURIDAD

Para la correcta implementación y cumplimiento de la presente política, toda persona que Trate Datos Personales dentro de Grupo Seguritech es responsable

de implementar de manera estructurada y formal las siguientes Medidas de Seguridad, que se indican de manera enunciativa pero no limitativa:

Medidas Administrativas de Seguridad

a. Cada área deberá realizar un levantamiento del Tratamiento de Datos Personales dentro de sus actividades ordinarias de trabajo a efecto de identificar la existencia y tipo de Datos Personales, dividiendo los mismos entre: i) Datos Personales, ii) Datos Financieros; y iii) Datos Sensibles.

b. Una vez identificados los Datos Personales que se tratan, cada área o responsable deberá documentar formalmente las Medidas de Seguridad que adoptará para el debido Tratamiento y actualización de los Datos Personales que trata.

c. Las Bases de Datos Personales que se detecten deberán cumplir con los Lineamientos para Bases de Datos establecidos anteriormente en la presente política.

d. Cada área que trate Datos Personales deberá asegurarse de reportar la existencia de sus Bases de Datos Personales al Oficial de Protección de Datos a efecto de contar con la asesoría correspondiente en el mecanismo de supervisión, consulta y vigilancia constante del debido Tratamiento de los Datos Personales.

Medidas Técnicas de Seguridad

a. El acceso a las bases de datos lógicas o a la información en formato lógico única y exclusivamente será realizado por usuarios identificados y autorizados. Lo anterior, amparado bajo el superior directo que haya encomendado dicha actividad.

b. Se restringirán todos los accesos a las bases de datos, se entregarán usuarios con privilegios dependiendo su función, las bases de datos serán encriptadas y con acceso mediante password, se elaborará carta de entrega de clave.

c. Para proteger los equipos móviles, portátiles o de fácil remoción que contengan Datos Personales y que se encuentren situados dentro o fuera de las instalaciones, los colaboradores que tengan asignados a su cargo equipos de esta naturaleza, firmarán un acta responsiva que ampare la protección de dichos equipos. Asimismo, cuando el equipo cambie de propietario, se eliminará todo el contenido del equipo, asegurándose que no quede ningún dato susceptible de apropiación.

Medidas Físicas de Seguridad

a. Se prevendrá mediante los controles de acceso que tenga implementado Grupo Seguritech el acceso no autorizado al lugar donde se almacenen físicamente los Datos Personales (servidores y carpetas).

b. Para evitar los daños o interferencias (intrusiones) al lugar donde se almacenan Datos Personales (servidores y carpetas) la información impresa que contenga Datos Personales será ubicada en una gaveta con cerradura y sólo se podrá tener acceso a ella mediante la validación del director correspondiente y registrando el acceso y motivo por el cual se le permite la revisión de la información.

8. COHERENCIA NORMATIVA

La presente Política y los Avisos de Privacidad de cada entidad del Grupo son instrumentos complementarios: los Avisos de Privacidad informan a los Titulares sobre el tratamiento de sus Datos Personales, mientras que esta Política establece los procedimientos, controles y medidas internas para garantizar dicho tratamiento conforme a la legislación aplicable. Ambos instrumentos deberán mantenerse alineados en todo momento. En caso de que se identifique cualquier inconsistencia entre ellos, el Oficial de Protección de Datos coordinará la revisión y actualización correspondiente para asegurar su coherencia. Todos los colaboradores y terceros relacionados con el Grupo son responsables de conocer tanto la presente Política como los Avisos de Privacidad aplicables, y de reportar al Oficial de Protección de Datos cualquier inconsistencia o incumplimiento que identifiquen.

9. OFICIAL DE PROTECCIÓN DE DATOS PERSONALES

La presente política es administrada y su cumplimiento es supervisado por el Oficial de Protección de Datos de Grupo Seguritech, quien funge como la persona designada para los efectos establecidos en las disposiciones legales aplicables.

Cualquier actividad relacionada con el Tratamiento de Datos Personales dentro de Grupo Seguritech debe ser reportado al Oficial de Protección de Datos de manera previa a su realización, a efecto de que supervise el correcto cumplimiento de las disposiciones legales aplicables en la materia.

El Oficial de Protección de Datos dará trámite a las solicitudes de Derechos ARCO conforme a lo establecido en los Avisos de Privacidad de Grupo Seguritech. Asimismo, el Oficial de Protección de Datos tiene encomendado fomentar la cultura de protección de los Datos Personales dentro de la organización, lo que realizará llevando a cabo procesos de vigilancia y capacitación a lo establecido en la presente política.

El Oficial de Protección de Datos de Grupo Seguritech puede ser contactado a través de los siguientes medios:

Nombre del Oficial de Protección de Datos: Lic. Mario Shai Aguado González.

Correo para asuntos Datos Personales: datospersonales@seguritech.com

10. CUMPLIMIENTO Y SANCIONES

Cada uno de los colaboradores del Grupo es responsable del cumplimiento de esta Política. El incumplimiento de la misma podrá conllevar para los colaboradores la adopción de las medidas disciplinarias previstas en la Ley Federal del Trabajo, el Reglamento Interior de Trabajo de la empresa que corresponda, el Código de Ética de Grupo Seguritech y demás normativa interna aplicable.

11. DENUNCIA Y NO REPRESALIAS

Cualquier persona que tenga conocimiento de hechos que impliquen o pudieren implicar violación directa o indirecta de la presente Política, deberán denunciarlo por medio del Canal de Denuncia CLEC a través del correo clec@ecbmexico.com.

Grupo Seguritech prohíbe las represalias por la presentación de reportes donde se denuncien violaciones o aparentes violaciones a esta Política.

12. VIGENCIA

La presente Política entra en vigor con su aprobación por el Comité de Integridad y permanecerá vigente hasta su actualización, revisión o derogación.

Aprobado por:

ADRIANA PERALTA RAMOS
Presidenta del Comité de Integridad
y Compliance Officer

YAGO BAZACO PALACIOS
Vocal del Comité de Integridad y
Director General Corporativo

RICARDO PAVEL MEZA
Vocal del Comité de Integridad y
Director Jurídico