POLÍTICA DE **PROTECCIÓN DE DATOS PERSONALES**

PRESENTACIÓN

El presente documento tiene por objeto establecer los procedimientos, lineamientos y directrices que deberán observar todos los empleados, colaboradores y terceros relacionados con las actividades de Seguritech (la “Compañía”) para el debido tratamiento y protección de los Datos Personales de los cuales la Compañía sea Responsable en términos de las disposiciones legales aplicables.

MARCO REGULATORIO

Esta Política busca implementar de manera amplia y vinculante dentro de la Compañía 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 emitidas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

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 en el cual se informa a los Titulares, el Tratamiento que dará la Compañía a sus Datos Personales, disponible en: https://avisos.seguritech.com
2. Base de Datos: Cualquier conjunto ordenado de Datos Personales, independientemente de la forma en que se recaben o almacenen.
3. Consentimiento: Manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos, misma que se otorga, por regla general, mediante el Aviso de Privacidad
4. Datos Personales: Cualquier información concerniente a una persona física identificada o identificable.
5. Derechos ARCO: Son los derechos de acceso, rec!cación, 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. Responsable: Es la persona legalmente obligada a salvaguardar los Datos Personales, incluyendo a la Compañía y a cualquier persona que de Tratamiento a los datos dentro de la misma.
8. 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.
9. Tratamiento: La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales. Este término se refiere usualmente a lo largo de la presente Política a través de las diferentes conjugaciones del verbo “tratar”.
10. Transferencia: Toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento.

DATOS SENSIBLES

Los datos sensibles son aquellos Datos Personales que afectan la esfera más íntima de su 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, afiliación sindical, opiniones políticas y preferencia sexual, entre otros (los “Datos Sensibles”).

En la Compañía no Tratamos ningún Dato Sensible y se encuentra totalmente prohibido el uso de Datos Sensibles para cualquier fin, incluyendo su recolección, almacenamiento, Tratamiento o cualquier actividad relacionada, inclusive cualquier actividad temporal o accesoria. La creación de cualquier Base de Datos con Datos Sensibles se considerará como una violación grave a la presente Política.

Cualquier Tratamiento de Datos Sensibles debe ser reportada inmediatamente a la Compañía a través de la Función CLEC.

PRINCIPIOS

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

PRINCIPIO	ABSTRACTO	OBLIGACIÓN
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	Sólo podrán ser objeto de tratamiento los datos que resulten necesarios, adecuados y

	estrictamente necesarios	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	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.

LINEAMIENTOS PARA BASES DE DATOS

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

1. Sólo se podrán crear Bases de Datos Personales cuando sea estrictamente necesario para desempeñar una función haciendo uso de 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 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 de la Compañía.
9. Todas las áreas que cuenten con Bases de Datos personales deben reportar de manera formal a la Función CLEC la existencia de la base de datos y las Medidas de Seguridad adoptadas, a efectos de que la Función CLEC pueda fungir como órgano permanente de consulta, vigilancia y auditoría con respecto al correcto tratamiento de los Datos Personales en cuestión.

MEDIDAS DE SEGURIDAD

Para la correcta implementación y cumplimiento de la presente Política, toda persona que Trate datos personales dentro de la Compañía es responsable de implementar de manera estructurada y formal las siguientes Medidas de Seguridad, que se indican de manera enunciativa pero no limitativa, independientemente de las demás medidas que implemente cada responsable o cada área para proteger los Datos Personales de conformidad con la presente Política:

1. 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 solicitará periódicamente a la Dirección de Sistemas Corporativos una auditoría a sus equipos de cómputo asignados a efecto de identificar el correcto Tratamiento de los Datos Personales por cada usuario, levantando para cada caso una acta de revisión y una acta de destrucción de los Datos Personales que se encuentren en violación a lo establecido en la presente Política.

e. Cada área que trate datos personales deberá asegurarse de reportar la existencia de sus Bases de Datos Personales a la Función CLEC a efecto de ser incluidos en el mecanismo de auditoría, consulta y vigilancia constante del debido tratamiento de los Datos Personales, incluyendo el programa de capacitación anual de protección de Datos Personales.

2. 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 restringirá 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.

3. Medidas Físicas de Seguridad
   a. Se prevendrá mediante los controles biométricos de la Compañía 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 de operaciones y registrando el acceso y motivo por el cual se le permite la revisión de la información.

PRELACIÓN

En caso de cualquier conflicto entre las presentes Políticas y el Aviso de Privacidad de la Compañía, prevalecerá lo dispuesto en el Aviso de Privacidad de la Compañía disponible en: https://avisos.seguritech.com . Todos los empleados, colaboradores y terceros relacionados con la Compañía son responsables de conocer el Aviso de Privacidad y de informar cualquier aspecto relacionado con el mismo a la Función CLEC.

DEPARTAMENTO DE PROTECCIÓN DE DATOS PERSONALES

La presente Política es administrada y su cumplimiento es vigilado por el la Función de Cumplimiento Legal y Ética Corporativa (Función CLEC) de la Compañía, quien funge como Departamento de Protección de Datos Personales de la Compañía para los efectos establecidos en las disposiciones legales aplicables.

Cualquier actividad relacionada con el Tratamiento de Datos Personales dentro de la Compañía debe ser reportado a la Función CLEC de manera previa a su realización, a efecto de que la Función CLEC verifique y valide el correcto cumplimiento de las disposiciones legales aplicables en la materia.

La Función CLEC dará trámite a las solicitudes de Derechos ARCO (según dicho término se define adelante), conforme a lo establecido en el Aviso de Privacidad de la Compañía. Asimismo, la Función CLEC tiene encomendado fomentar la cultura de protección de los Datos Personales dentro de la organización, lo que realizará llevando a cabo procesos anuales de auditoría y capacitación a lo establecido en las presentes Políticas.

El Departamento de Protección de Datos Personales de la Compañía puede ser contactado a través de la Función CLEC en los siguientes medios:

Nombre del funcionario responsable:	Lic. Emmanuel A. Cárdenas R.
Cargo:	Director Jurídico Corporativo del grupo
Teléfono:	(+5255) 5083.0000 ext. 342
Correo para asuntos datos personales:	datospersonales@seguritech.com
Página Función CLEC	clec@ecbmexico.com

CUMPLIMIENTO Y SANCIONES

Cada uno de los colaboradores es responsable del cumplimiento y la implementación de esta política. El no cumplimiento de esta política dará lugar para que se tomen medidas disciplinarias que pueden llegar a la terminación de la relación con dicho tercero para todos los efectos a que haya lugar.

CAPACITACIÓN

Todos los empleados de la Compañía están obligados a asistir todos los años a los talleres de capacitación sobre las políticas anticorrupción, lineamientos de conducta y las directrices aplicables por áreas.

INFORMACIÓN Y NO REPRESALIAS

Los directores, empleados y terceros deben informar sobre toda conducta que, de buena fe, consideren que es una violación o aparenta ser una violación de esta Política a través de la función de Cumplimiento Legal y Ética Corporativa (CLEC) de la Compañía.

Cada uno de estos informes deberá tratarse como confidencial en la medida que lo permita la ley y en forma consistente con una investigación adecuada. La Compañía prohíbe las represalias por la presentación de informes donde se sospecha de conductas indebidas realizados de buena fe. En el caso de no estar seguro si se le está pidiendo que realice un pago indebido, no debe realizar ese pago. Debe consultar a su supervisor, la gerencia superior, al apoyo legal que opera en su empresa o a la función CLEC.