1. OBJETIVO:

Definir la política de protección de datos personales de la Compañía, aplicable a todas las personas, naturales y jurídicas, que tengan relación con esta. Dicha política está encaminada a proteger la información personal de clientes, proveedores y colaboradores que reposa en las bases de datos administradas por la Compañía, dando cumplimiento a la ley 1581 de 2012 que constituye el marco general de la protección de datos personales.

OBJETIVOS ESPECÍFICOS:

- Generar seguridad y privacidad en los procesos de la Compañía con los diferentes grupos de interés (clientes, proveedores y colaboradores).
- Definir los lineamientos en materia de seguridad, haciendo de éstos una práctica habitual dentro del quehacer diario de la Compañía con relación a la protección de datos personales.
- Orientar la adopción de la normatividad vigente relacionada con la protección de datos personales.

2. ALCANCE:

Esta política es aplicable a todos los datos personales administrados por la Compañía que son susceptibles de protección bajo los lineamientos de la Ley 1581 de 2012. Esta política es vinculante y está dirigida a todo el personal relacionado con la Compañía.

Es necesario contar con un recurso humano capacitado en la atención de incidentes de seguridad, quien tendrá la función de definir los procedimientos adecuados para la gestión de incidentes y manejar relaciones con las partes interesadas.

3. DEFINICIONES:

Habeas Data. El derecho que tiene toda persona de conocer, actualizar y rectificar la información que se haya recogido sobre ella en archivos y bancos de datos de naturaleza pública o privada

Base de Datos. Es un conjunto organizado de datos personales que se utiliza para llevar el registro y la administración de los mismos, bien sea en medio físico (un archivo) o en medio electrónico (archivos en cualquier formato como hojas electrónicas, tratamiento de texto, con el uso o no de motores de bases de datos) e independientemente de la cantidad de datos personales que contenga. El registro y administración de datos personales implica desde almacenarlos, hasta consultarlos, actualizarlos, compartirlos con terceros y/o eliminarlos, para los fines que decida la empresa.

Por lo general, las empresas tienen las siguientes bases de datos:

- Base de Datos de empleados
- Base de Datos de clientes
- Base de Datos de proveedores

Datos de Identificación. Todos los Ítems que puedan aplicar para la identificación de un dato, estos pueden ser: Nombre, apellido, tipo de identificación, número de identificación, fecha y lugar de expedición, estado civil, sexo, firma, nacionalidad, datos de familia, firma electrónica, otros documentos de identificación, lugar y fecha de nacimiento o muerte, edad, huella, ADN, iris, geometría facial o corporal, fotografías, videos, fórmula dactiloscópica, voz y los demás que apliquen.

Dato Privado. Es el dato que por su naturaleza íntima o reservada sólo es relevante para el Titular.

Dato Semiprivado. Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la Ley 1266.

Dato Público. Es el dato calificado como tal según los mandatos de la Ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la Ley 1266 de 2008. Son públicos, entre otros, los datos contenidos en

documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

Dato Sensible. Son aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el estado de salud de la persona en cuanto a órdenes y relación de pruebas complementarias como laboratorio, imágenes diagnósticas, endoscópicas, patológicas, estudios, diagnósticos médicos generales o especializados, psicológicos o psiquiátricos, medicamentos y/o tratamientos médicos o terapéuticos de cualquier tipo, los relacionados al origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la vida sexual y los datos biométricos, personas de la tercera edad o menores de 18 años en condición de pobreza, datos sobre personas en situación de discapacidad personas con limitaciones sicomotoras, auditivas y visuales en condiciones de pobreza, personas víctimas de la violencia, personas en situación de desplazamiento forzado por violencia, madres gestantes o lactantes o cabeza de familia en situación de vulnerabilidad, menores en condición de abandono o protección y los demás aplicables.

Datos de Ubicación. Como los relacionados con la actividad comercial o privada de las personas como dirección, teléfono, correo electrónico entre otros.

Datos de Contenido Socio Económico. Como estrato, propiedad de la vivienda, Datos financieros, crediticios y/o de carácter económico de las personas, Datos patrimoniales como bienes muebles e inmuebles, ingresos, egresos, inversiones, historia laboral, experiencia laboral, cargo, fechas de ingreso y retiro, anotaciones, llamados de atención, nivel educativo, capacitación y/o historial académico de la persona entre otros.

Encargado del Tratamiento. Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice 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, decida sobre la base de datos y/o el Tratamiento de los datos.

Titular. Persona natural cuyos datos personales sean objeto de Tratamiento.

Tratamiento. Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión de los mismos.

4. RESPONSABILIDADES:

4.1. Deberes de la Compañía

- Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular.
- Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a éste se mantenga actualizada.
- Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.
- Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley.
- Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.
- Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley.

- Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos.
- Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.
- Informar a solicitud del Titular sobre el uso dado a sus datos.
- Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
- Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.
- Cumplimiento de los requisitos legales y contractuales.
- Identificación de la legislación aplicable y de los requisitos contractuales.
- Contar con la asesoría de consultores y personal que esté relacionado con el manejo de la norma.
- Estar atento a las recomendaciones de abogados en la implementación de nuevas normas que hayan de salir.

4.2. Obligaciones y funciones

- El encargado de la información de clientes es el Especialista de Apoyo Comercial, quien será el responsable de informar al Encargado de Protección de Datos cualquier modificación que se realice sobre la base de datos.
- El encargado de la información de proveedores es el Coordinador de Compras y Contratos, quien será el responsable de informar al Encargado de Protección de Datos cualquier modificación que se realice sobre la base de datos.
- El encargado de la información de colaboradores es el Área de Talento Humano, quienes serán los responsables de informar al Encargado de Protección de Datos cualquier modificación que se realice sobre la base de datos.
- El encargado de los prospectos de clientes es el Coordinador de Mercadeo, quien será el responsable de informar al Encargado de Protección de Datos cualquier modificación que se realice sobre la base de datos.

4.3. Plan de mejora continua

La Compañía tendrá la responsabilidad de estar en constante mejora en cuanto a la búsqueda de nuevos productos o desarrollo de nuevas soluciones de protección para combatir las brechas de seguridad.

4.4. Deberes cuando se actúa como responsable

- Solicitar y conservar, en las condiciones previstas en esta política, copia de la respectiva autorización otorgada por el Titular.
- Informar de manera clara y suficiente al Titular sobre la finalidad de la recolección y los derechos que le asisten en virtud de la autorización otorgada. El responsable de esta labor es el Encargado de Protección de Datos.
- Informar, a solicitud del Titular, sobre el uso dado a sus datos personales.
- Tramitar las consultas y reclamos formulados en los términos señalados por la presente política según procedimiento de la Compañía.
- Velar por el cumplimiento de los principios de veracidad, calidad, seguridad y confidencialidad establecidos en esta política.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Actualizar la información cuando sea necesario.
- Rectificar los datos personales cuando ello sea procedente.

4.5. Deberes con la Superintendencia de Industria y Comercio

- Informar las violaciones a los códigos de seguridad y la existencia de riesgos en la administración de la información de los titulares.
- Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

5. POLÍTICAS:

5.1. Requisitos generales

Esta política es aplicable a todas las personas, naturales y jurídicas, que tengan relación con la Compañía y está orientada a proteger la información personal de clientes, proveedores y colaboradores administrada por la Compañía, dando cumplimiento a la ley 1581 de 2012 que constituye el marco general de la protección de datos personales.

5.2. Descripción de las políticas

- Las políticas de seguridad, descritas en este documento, deben actualizarse regularmente con el fin de verificar que se encuentran alineadas con las tecnologías de seguridad y control utilizadas.
- Todo el software que se encuentre instalado en los equipos de cómputo de la Compañía debe estar aprobado por el área de tecnología, alineado con la política de adquisición de bienes de la Compañía.
- Se debe contar con un firewall que permita controlar las posibles intrusiones a la red.
- Las conexiones remotas, como VPN y Escritorios remotos, deben estar controladas por el área de tecnología.
- Todos los líderes de proceso deben velar por el cumplimiento de las políticas de seguridad.

5.3. Políticas de usuario

Objetivo

Asegurar la información de la Compañía por parte de todos los colaboradores.

Políticas

- El acceso a todos los equipos de cómputo de la Compañía debe contar con medidas mínimas de seguridad, como usuario y contraseña. Esta información es de uso personal e intransferible y es responsabilidad de cada colaborador las acciones que se realicen desde su usuario asignado.

- Todo el software que se encuentre instalado en los equipos de cómputo de la Compañía debe estar aprobado por el área de tecnología, alineado con la política de adquisición de bienes de la Compañía.
- Cada colaborador es responsable de los recursos de la Compañía que le sean asignados y del buen uso que se le dé a los mismos.
- Todos los colaboradores de la Compañía tienen la obligación de velar por la seguridad y buen manejo de la información organizacional. Su divulgación a terceras personas o para beneficio propio acarreará las medidas disciplinarias a las que haya lugar.
- Todo evento seguridad que afecte la seguridad o integridad de la información personal deberá ser reportado a los Líderes de Proceso.

5.4. Políticas de Colaboradores y contratistas del área de tecnología

Objetivo

Generar estándares de seguridad para la protección de información personal por parte de los colaboradores de la Compañía.

Políticas

- La información de acceso a los equipos de cómputo de la Compañía es de uso personal e intransferible. Es responsabilidad de cada colaborador las acciones que se realicen desde su usuario asignado.
- El nivel de complejidad de las contraseñas debe ser alto. Esto significa que, por lo menos, debe contener un dígito, un carácter especial, una letra minúscula y una letra mayúscula.
- Cuando un equipo de cómputo o un dispositivo de almacenamiento de la Compañía vaya a ser dado de baja, su información deberá ser eliminada y los discos formateados.
- Todos los colaboradores de la Compañía tienen la obligación de velar por la seguridad y buen manejo de la información organizacional. Su divulgación a terceras personas o para beneficio propio acarreará las medidas disciplinarias a las que haya lugar.

- Todas las aplicaciones informáticas de la Compañía estarán restringidas por defecto. Los niveles de acceso y las acciones que cada colaborador pueda realizar en cada una de ellas dependerán de su rol y de las funciones asociadas a su cargo.
- El acceso a los servidores y bases de datos de la empresa estarán restringidos únicamente a personal autorizado por la Compañía.

6. CONTENIDO Y DESARROLLO:

6.1. Información de la Compañía

SOLUCIONES TECNOLOGÍA Y SERVICIOS S.A.S - STS S.A.S
NIT. 830.505.521-5
Dirección. Calle 126 No. 7-26 Oficina 503. Bogotá DC - Colombia
Teléfono. (571) 7450145
Página web. www.stssa.com.co

6.2. Privacidad y protección de información de datos personales

Conforme a los lineamientos de la ley 1581 de 2012, cada persona que esté registrada en una lista de distribución tiene el derecho de solicitar darse de baja de la misma. La Compañía debe conservar, en las condiciones previstas en la Ley 1581 de 2012, copia de la autorización otorgada por el titular para su suscripción en listas de distribución.
La información personal de clientes, proveedores y colaboradores debe ser usada por la Compañía, únicamente para los fines para lo cual fue autorizado por el Titular.

6.3. Establecimiento y gestión del SGSI

Alcance

El alcance del SGSI incluye a los colaboradores del área de tecnología de la Compañía, administradores y manejadores de base de datos, así como los clientes que utilizan el producto final.

Políticas

El acceso a los servidores, bases de datos y aplicaciones informáticas de la Compañía debe hacerse a través de usuarios nombrados para permitir la trazabilidad de las acciones.

Las actividades de creación, actualización y eliminación de usuarios en las aplicaciones informáticas de la Compañía deben ser ejecutadas por los Líderes de Aplicación y administradores asignados para tal fin. La modificación de perfiles sobre usuarios específicos que involucren la adición y/o eliminación de privilegios deberá ser aprobada por los Líderes de Proceso correspondientes.

La inactivación de usuarios por desvinculación laboral debe hacerse efectivo el mismo día en el que se termine la relación laboral con la Compañía. Debe mantenerse registro de la acción.

6.4. Revisiones de seguridad de la información

En la Compañía, la persona encargada del cumplimiento de las políticas de seguridad es el Encargado de Protección de Datos, quien es el responsable de formular las recomendaciones frente a los incidentes de seguridad. De igual modo, los Líderes de Proceso deben revisar el cumplimiento de las políticas y procedimientos de la Compañía.

6.5. Gestión de los incidentes de la seguridad de la información

Es necesario contar con un recurso humano capacitado en la atención de los incidentes de seguridad, quien tendrá la función de definir los procedimientos adecuados para la gestión de incidentes y manejar relaciones con las partes interesadas.

6.6. Políticas de gestión de incidentes de seguridad de la información

6.6.1. Detección temprana de incidentes de seguridad

Verificar periódicamente los controles de acceso en las bases de datos con el fin de detectar los posibles incidentes de seguridad de la información.

6.6.2. Plan de mejora continua

La Compañía tendrá la responsabilidad de estar en constante mejora en cuanto a la búsqueda de nuevos productos o desarrollo de nuevas soluciones de protección para combatir las brechas de seguridad.

6.7. Normatividad legal y ámbito de aplicación

La presente política de protección de datos personales es elaborada de conformidad con lo dispuesto en la Constitución Política, la Ley 1581 de 2012, el Decreto Reglamentario 1377 de 2013, Circular Externa 02 de 2015, Decreto Único 1074 de 2015, Decreto 1759 de 2016 y demás disposiciones complementarias, que serán aplicadas por la Compañía respecto de la recolección, almacenamiento, uso, circulación, supresión y todas aquellas actividades que constituyan el tratamiento de datos personales.

6.8. Principios aplicables al tratamiento de datos personales

El tratamiento de datos personales en la Compañía se regirá por los siguientes principios:

Principio de Finalidad. El tratamiento de los datos personales recogidos debe obedecer a una finalidad legítima, la cual debe ser informada al Titular.

Principio de Libertad. El tratamiento sólo puede llevarse a cabo con el consentimiento previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

Principio de Veracidad o Calidad. La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. No será efectuado el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

Principio de Transparencia. El tratamiento de información que realiza la Compañía debe garantizar el derecho del Titular a solicitar, en cualquier momento y sin restricciones, la información acerca de la existencia de los datos que le conciernen.

Principio de Acceso y Circulación Restringida. El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente Ley y la Constitución.

Los datos personales, salvo la información pública y lo dispuesto en la autorización otorgada por el Titular del dato, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados.

Principio de Seguridad. La información sujeta a tratamiento por parte de la Compañía se deberá proteger mediante el uso de las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Principio de Confidencialidad. Todas las personas que intervengan en el tratamiento de datos personales están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento. En el evento que se recolecten datos personales sensibles, el Titular podrá negarse a autorizar su tratamiento.

6.9. Limitaciones temporales al tratamiento de los datos personales

Solo podrá recolectar, almacenar, usar o circular los datos personales durante el tiempo que sea razonable y necesario, de acuerdo con las finalidades que justificaron el tratamiento, atendiendo a las disposiciones aplicables a la materia de que se trate y a los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.

Una vez cumplida la o las finalidades del tratamiento y sin perjuicio de normas legales que dispongan lo contrario, procederá a la supresión de los datos personales en su posesión. No obstante, los datos personales deberán ser conservados cuando así se requiera para el cumplimiento de una obligación legal o contractual.

7. CONTROL DE CAMBIOS:

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1	15/Feb/2022	Se realiza revisión general de la Política. Actualización de dirección y razón social S.A.S. Cambio de código del proceso Administrativo a Talento Humano.

ELABORÓ		REVISÓ		APROBÓ	
Nombre:	Vanira Isley Montes Buelvas	**Nombre:**	Nubia Gutiérrez	**Nombre:**	Mauricio Amaya
CARGO:	Coordinador de Calidad	**CARGO:**	Gerente de Talento Humano	**CARGO:**	Gerente General
Fecha:	15/Feb/2022	**Fecha:**	28/Feb/2022	**Fecha:**	28/Feb/2022