1. ALCANCE:

La compañía **SNIDER & CIA S.A.S**, empresa de almacenamiento de mercancías bajo control aduanero, mercancías nacionales, nacionalizadas y especialista en administración de inventarios; está comprometida en la prestación de sus servicios bajo estándares de calidad y asignación de recursos esenciales que permitan la satisfacción de las necesidades de sus clientes y partes interesadas, así como el cumplimiento de los requisitos legales y reglamentarios aplicables, a través del seguimiento y monitoreo de la planeación estratégica de los procesos que conlleven al mejoramiento continuo del sistema de gestión de calidad.

2. OBJETIVOS:

- Prestar nuestros servicios bajo estándares de calidad y asignación de recursos necesarios.
- Satisfacer las necesidades de nuestros clientes y partes interesadas.
- Cumplir con los requisitos legales y reglamentarios aplicables a las actividades.
- Realizar seguimiento y monitoreo de la planeación estratégica de los procesos.
- Mejora continua.

2.1. Indicadores

- Encuesta de satisfacción al cliente.
- Seguimiento de requisitos legales.
- Seguimiento de gestión mejora.

3. RESPONSABILIDADES.

La Alta Dirección de **SNIDER & CIA S.A.S**, asume la responsabilidad de velar por la comunicación a sus colaboradores, la publicación a sus partes interesadas, así como garantizar el cumplimiento, revisión, actualización de esta política de manera anual.

Sanciones: El incumplimiento de cualquiera de las condiciones establecidas en esta política acarreará a los colaboradores sanciones disciplinarias según lo establecido en el reglamento interno de trabajo.

4. FIRMA

1. ALCANCE:

Snider & CIA S.A.S. especializada en almacenamiento de mercancías bajo control aduanero, mercancías nacionales, administración de inventarios, usuario comercial en zona franca, se compromete a implementar un sistema de Gestión de Seguridad y Riesgos integral que permite aplicar controles de manera efectiva para garantizar el cumplimiento de los objetivos estratégicos, los requisitos legales dentro de la cadena de suministro, con base en lo establecido en el Sistema de Administración del Riesgo de Lavado de Activos, Financiación del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva (LA/FT FPADM) – SAGRILAFT y a promover la seguridad en el uso de las tecnologías de la información.

Desde la Alta Dirección y todas sus partes interesadas tienen el compromiso de mantener el principio de autocontrol, entendido como la capacidad de las personas en los diferentes procesos, de considerar el control como parte inherente de sus responsabilidades, campos de acción y toma de decisiones, por ende, es responsabilidad de cada colaborador conocer y participar en el Sistema de Gestión de Seguridad y Riesgos, dando cumplimiento a las políticas establecidas y especialmente obrando con toda diligencia en la ejecución de las actividades que les han sido asignadas y reportando cualquier riesgo u operación inusual a los entes establecidos en la empresa para su canalización.

La empresa está comprometida en tener un sistema de administración de Riesgos y Seguridad enfocado en su cadena de suministro internacional, que prevea actividades ilícitas tales como lavado de activos, contrabando, tráfico de estupefacientes, tráfico de sustancias para el procesamiento de narcóticos, terrorismo, financiación del terrorismo y tráfico de armas entre otras.

2. OBJETIVO GENERAL:

Generar estrategias en la empresa Snider & CIA S.A.S, ofreciendo seguridad en la cadena de suministro, identificando los riesgos a los que está expuesta, con el propósito de mitigarlos a través de la implementación y monitoreo de controles, asegurando la continuidad del negocio y la adaptabilidad a los cambios del entorno.

2.1. Estructura de Despliegue.

Dentro del documento *FT-PE-13 Estructura de Despliegue,* se encuentran establecidos los Objetivos específicos, indicadores, metas, periodicidad de revisión, responsable, programas y su detalle.

3. CONTENIDO

3.1. PROPÓSITO

La empresa cuenta con un equipo humano con valores, experiencia, conocimientos y habilidades. Consciente de la importancia de estar preparados para responder a los eventos que ocurran durante en la prestación de sus servicios y el desarrollo de cada uno de sus procesos, la empresa optó por implementar un sistema de Gestión de Seguridad y Riesgo el cual tiene como propósito asegurar el cumplimiento de los objetivos Estratégicos. Dicha gestión se sustenta en una adecuada identificación, evaluación, medición y monitoreo del riesgo, así como la determinación de planes de acción que mitiguen su materialización.

Como parte esencial de dicho sistema, está la gestión de la Continuidad del Negocio que propende por la protección de los colaboradores, los servicios críticos, la información, la infraestructura y los procesos que permiten cumplir con los compromisos y las expectativas de los actores de la cadena de valor, así como la de sus accionistas.

3.2. GENERALIDADES

a. Establecer políticas y procedimientos para la supervisión y gestión de Seguridad y Riesgos.

b. La administración es responsable de diseñar e implementar el programa de Gestión de Seguridad y Riesgos, así como la de reportar al Comité de Control y Auditoría los resultados de dicha implementación y comportamiento, periódicamente.

c. La presente política debe ser revisada y actualizada anualmente, o cada vez que los cambios en la regulación lo requieran, dando así cumplimiento a la regulación local, financiera y de la industria.

d. Todo colaborador en Snider & CIA S.A.S es responsable por la identificación y comunicación de los riesgos asociados a sus labores, teniendo en cuenta la prevención y el autocontrol como mecanismos principales para tratar los riesgos, generando confiabilidad y seguridad en los procesos.

e. La Gestión de Seguridad y Riesgos de Snider & CIA S.A.S debe estar integrada con todas las políticas y procesos de la empresa, razón por la cual en ningún momento se podrán estructurar los procesos sin considerar la presente política, y por tanto los riesgos y controles que pueden afectar el cumplimiento de los objetivos estratégicos y del área y su operación.

f. La severidad de los riesgos debe ser evaluada con base en los criterios de probabilidad e impacto definidos por la Snider & CIA S.A.S.

4. RESPONSABILIDADES.

A continuación, se describen las responsabilidades de las áreas o cargos involucrados en la Gestión de Seguridad y Riesgos de Snider & CIA S.A.S:

4.1. La Alta Dirección

Es responsable por:

a. La aprobación de la política de la Gestión de Seguridad y Riesgos de Snider & CIA S.A.S, en todas sus modificaciones o actualizaciones.

b. Promover una cultura que fomente la seguridad física y psicológica de todos los colaboradores y por tanto orientada a la gestión del riesgo y seguridad en todos los niveles de la empresa.

c. Asignar anualmente los recursos para la Gestión de Seguridad y Riesgos en la empresa.

d. El conocimiento y monitoreo periódico de los riesgos que se identifiquen.

e. Velar por la existencia de un adecuado y sólido ambiente de control promoviendo una cultura de Gestión del Seguridad y Riesgos.

4.2. Auditoría Interna

Es responsable por:

a. Desarrollar una evaluación independiente con base al marco de Gestión de Seguridad y Riesgos para Snider & CIA S.A.S, validando el cumplimiento de las políticas, procedimientos y controles establecidos, que intervienen en la cadena de suministro.

b. Emitir los correspondientes informes sobre sus evaluaciones a la Alta Gerencia y/o Comité de Control y Auditoría.

4.3. Auditoría Externa

Es responsable por presentar en sus informes las debilidades identificadas frente a la Gestión de Seguridad, Riesgos y Control. Podrán ser realizadas por los diferentes entes de control y empresas certificadoras, así como por la Revisoría Fiscal.

4.4. Líderes de proceso

Responsables por:

a. Aplicar el marco de Gestión de Seguridad y Riesgos de Snider & CIA S.A.S.

b. Identificar, evaluar y gestionar los riesgos a los cuales se encuentra expuesta la empresa en cada uno de sus procesos.

c. Monitorear si las actividades realizadas son acordes al nivel de tolerancia del riesgo.

d. Reportar al Comité de Gerencia mensualmente el informe de Seguridad, Riesgos y controles establecidos.

La presente política de Gestión de Seguridad y Riesgos es efectiva desde la fecha de su aprobación por la Alta Dirección.

Tipología de riesgos asociados.

Snider & CIA S.A.S, en todos sus procesos y partes interesadas, tienen la responsabilidad de identificar y clasificar los riesgos, acorde con lo establecido en el numeral 5.5.2 del procedimiento Gestión de Riesgos *P-Q-10,* y cumplir con los siguientes compromisos dada la tipología:

"*5.1.3.1 Riesgo Reputacional* *. Es deber de todos los colaboradores velar por la buena imagen de Snider & CIA S.A.S a través del cumplimiento de las disposiciones establecidas y el decidido apoyo a las autoridades competentes. Se prohíbe a todos los empleados en general realizar actividades de divulgación de información de la empresa, sin la debida autorización de la Alta Dirección; en especial aquellas relacionadas con operaciones inusuales, intentadas o sospechosas.*

Snider & CIA S.A.S, para proteger y garantizar la seguridad de la información y datos personales de los colaboradores, clientes, proveedores y demás asociados de negocio de la compañía, implementó el Programa

Integral de Gestión de Protección de Datos Personales PG-PE-03que incluye la política establecida en este aspecto, de acuerdo con el cumplimiento del derecho fundamental de habeas data en el marco de lo establecido en la ley 1581 de 2012 y sus decretos reglamentarios.

5.1.3.2 ***Riesgo de Contagio****. Para evitar el riesgo de contagio es deber de todos los funcionarios, velar por un efectivo conocimiento de las contrapartes con las que Snider & CIA S.A.S se vincula.*

5.1.3.3 ***Riesgo Legal****. Todas las actividades, operaciones, negocios o contratos realizados por Snider & CIA S.A.S deben dar cumplimiento a la legislación establecida y deberán contar con los debidos soportes, fechados y autorizados por quienes intervengan en ellos; dejando en lo posible constancia de las obligaciones que puedan derivarse de los mismos.*

5.1.3.4 ***Riesgo Operativo****. Es deber de todos los colaboradores de Snider & CIA S.A.S realizar la debida aplicación de las políticas, procedimientos y controles asignados, así como apoyar la identificación oportuna de los riesgos a los que están expuestos los diferentes procesos".*

La Alta Dirección de Snider & CIA S.A.S, asume la responsabilidad de velar por la comunicación a sus colaboradores, la publicación a sus partes interesadas, así como garantizar el cumplimiento, revisión y actualización de esta política.

Los colaboradores y demás partes interesadas son responsables de dar estricto cumplimiento a esta política. El incumplimiento de esta por parte de los colaboradores acarreará sanciones disciplinarias según lo establecido en el reglamento interno de trabajo sin perjuicio de las demás consecuencias legales a que haya lugar.

5. FIRMA

1. ALCANCE:

La política de seguridad Informática es aplicable para todos los procesos administrativos, operativos, incluyendo funcionarios, contratistas, practicantes y terceros, así como para todas las sedes de Snider & CIA SAS, que cuenten con acceso a la información y a los recursos informáticos, ya sea que accedan en forma local desde las sedes o lo hagan a través de internet por fuera de las instalaciones dando cumplimiento de lo contenido en la normatividad legal vigente y demás normas aplicables en temas de seguridad de la información, con el fin de tener un adecuado cumplimiento de sus roles asignados y cumplir con un alto nivel de protección de ciberseguridad y calidad de los mismos.

2. OBJETIVOS:

Establecer los lineamientos, normas y parámetros para garantizar el cumplimiento de los principios de confidencialidad, integridad, disponibilidad, veracidad y seguridad de la información en Snider & CIA SAS.

3. INDICADORES

- Indicador de oportunidad en la atención
- Indicador de efectividad en servicio
- Indicador de eficacia controles TI
- Indicador de requerimientos aplicativos
- Indicador de control proyectos

4. CONTENIDO

- El Jefe de Tecnología de la Información es quien gestiona y administra los recursos tecnológicos.

- Los dispositivos móviles corporativos (teléfonos inteligentes, tablets, portátiles), son herramientas de trabajo que se deben usar únicamente para el desarrollo de las funciones asignadas a su cargo.

- La asignación de usuario y contraseña de dominio, que es personal e intransferible, es administrada por Tecnología de la Información de acuerdo con lo establecido en el procedimiento "*Control al sistema de información*", la cual se debe cambiar cada 40 días para mitigar el riesgo de suplantación. Por ningún motivo los funcionarios deben usar la contraseña del correo de otro funcionario, ninguno debe dar a conocer su contraseña, a excepción de ser solicitado por el equipo de mesa de ayuda en una reparación o mantenimiento del equipo o servicio asignado y; una vez termine la labor debe generar el cambio de contraseña.

- Para la creación y actualización de contraseñas se establecen parámetros mínimos, los cuales están descritos en el procedimiento "*Control al sistema de información"*, el cambio de contraseña sólo podrá ser solicitado por el titular de la cuenta a través de la mesa de ayuda, en donde se llevará a cabo la validación de los datos personales. En caso de ser requerido el cambio de contraseña por fuerza mayor, esta solicitud debe ser realizada por el jefe directo a través de correo electrónico a la mesa de ayuda, indicando el nombre del funcionario y las razones o motivos de la solicitud.

- Se limitará la ejecución de archivos como (.exe, .vbs, .scr, .jar, etc) que no formen parte de las aplicaciones o sistemas necesarios para la correcta ejecución de las labores diarias.

- Está prohibida la instalación de software o aplicaciones por parte de los colaboradores, en los equipos entregados por Snider & CIA SAS, el proceso de tecnología de la información será el responsable de realizar a través de ticket en la mesa de ayuda, la instalación, actualización y/o eliminación de programas que se requieran para sus labores diarias o actividades propias del cargo, estos deben estar alineados a las normas de protección de derechos de autor y debe tener su respectivo licenciamiento, la instalación o uso de software no autorizado, será considerado como una violación a la presente política.

- Snider & CIA SAS, autoriza y permite la navegación en Internet con fines laborales y empresariales de acuerdo con sus funciones y roles asignados. El acceso a páginas de ocio no productivas, como los son: redes sociales, páginas de streaming de video y de audio Emisoras, Proxy, descargas P2P, torrents entre otros no está permitido.
  Excepciones a la política de restricción de navegación en Internet:

  - Departamento de Marketing & Comunicaciones: Se permite el acceso a redes sociales necesarias para el desempeño de sus funciones.

  - Capacitaciones autorizadas: Se otorgará acceso a sitios web requeridos de manera temporal para la formación profesional con previa solicitud del jefe inmediato a través de un ticket en mesa de ayuda.

  - Para cualquier excepción en la navegación de los colaboradores, el Líder de proceso correspondiente deberá solicitarla, justificando la necesidad y especificando el impacto en las funciones del colaborador. La aprobación de dicha excepción implicara su registro y actualización en la matriz de roles.

- No se permite la navegación a sitios web con contenidos contrarios a la ley, moral y buenas costumbres, o que representen algún peligro para la entidad tales como: pornografía, terrorismo, hacktivismo, segregación racial, etc. Las páginas web o sitios que al ser filtrados por las aplicaciones y/o herramientas de seguridad perimetral, sean identificados como no confiables, serán bloqueados.

- Toda la infraestructura tecnológica usada para acceder a internet es propiedad de Snider & CIA SAS, por lo anterior, se reserva el derecho a monitorear el tráfico desde y hacia internet y el acceso a la información, respetando el derecho a la privacidad y a la seguridad de los datos personales estipulados en la Ley 1581 de 2012.

- El funcionario o los funcionarios que intenten vulnerar o vulneren la seguridad de la infraestructura tecnológica de Snider & CIA SAS, podrán ser objeto de sanciones disciplinarias y judiciales si a ello hubiere lugar. Dentro de estas actividades se enmarcan algunas tales como:

  - Monitorear el tráfico de la red.

  - Evadir o instalar aplicaciones o plugins para evitar las plataformas de seguridad con el fin de obtener acceso a aplicaciones e información confidencial.

  - Intentar vulnerar medidas de ciberseguridad o validación de autenticación de usuarios en la red y/o en los sistemas de información que utiliza Snider & CIA SAS.

- Transmitir o recepcionar cualquier tipo de información y/o aplicación informática que infringa o viole los principios de la seguridad de la información como son la privacidad, confidencialidad e integridad de los datos de la entidad y de los servidores.

- Suplantación o falsificación de identidad de otro funcionario o de terceros.

- Efectuar actividades con el fin de afectar en cualquier forma los intereses, la imagen y el buen nombre de la entidad, en páginas de internet, redes sociales, blog de artículos o páginas de publicaciones con información falsa que llegue a afectar a la ciudadanía en general.

- Snider & CIA SAS, conociendo y atendiendo las necesidades de comunicación efectiva entre funcionarios, clientes y proveedores, autoriza la comunicación a través de WhatsApp web con las siguientes consideraciones:

  - Solo se puede tener activo el WhatsApp web con la línea corporativa en el equipo corporativo asignado.

  - Si un funcionario necesita utilizar su línea personal de WhatsApp para cumplir con las labores de la empresa, el líder del proceso solicitara a mesa de ayuda la matriz de roles del colaborador para su respectiva actualización.

  - WhatsApp NO es un medio de comunicación oficial de la entidad como si lo es Teams o el correo electrónico, por lo que cualquier tipo de negociación, acuerdo o envío de información y/o documentación debe formalizarse a través de los medios autorizados con el fin de mantener la confidencialidad e integridad de la información.

  - Al utilizarse el WhatsApp con una línea corporativa, se recomienda no tocar temas que no estén relacionados con el ámbito laboral (cadenas, chistes, memes, etc.), lo anterior con el ánimo de evitar confusiones y malentendidos.

  - El funcionario debe procurar tener comunicación con clientes internos, externos y proveedores, en horarios que coincidan con su jornada laboral.

  - Se prohíbe él envió de información contenida en las carpetas de Recursos Corporativos, MGI y MGI público a través de WhatsApp.

  - Cuando se compartan estados de WhatsApp, deben ser textos, imágenes y videos que sean preferiblemente realizados por el área de Marketing y Comunicaciones, y deben ser alusivos a la actividad económica de la empresa. Se prohíbe colocar temas de índole personal o temas que no hayan sido autorizados por la empresa.

- Los datos, documentos, carpetas y registros generados por los funcionarios, correspondientes a sus actividades laborales, son propiedad de la empresa, por lo tanto, cualquier divulgación o copia a entes externos sin autorización de la empresa se considera una violación a la confidencialidad de la información y una falta grave de acuerdo con el reglamento interno de trabajo.

- Cada funcionario es responsable del equipo que se le asigna y la información que este almacene. No se pueden almacenar en los equipos corporativos o en las unidades de red a las que tenga acceso, archivos de música, videos, fotos y cualquier tipo de archivo que no sea de carácter institucional.

- Está prohibido que los funcionarios realicen copias de seguridad de cualquier tipo de documentos o de información contenida en el equipo de cómputo asignado, estas copias deben ser autorizadas por su jefe inmediato, con el fin de conocer el uso y el destino de esta. La copia, daño intencional, sustracción o utilización diferente a las funciones asignadas, será considerada una falta grave de acuerdo con el reglamento interno de trabajo.

- El proceso de tecnología de la información efectuará revisiones periódicas de las aplicaciones utilizadas en cada dependencia, la ejecución de programas o aplicativos, extensiones en los navegadores, etc., no autorizados, serán considerados como una violación a la Política de Seguridad informática.
- Toda la información producto de sus labores debe almacenarse en la carpeta con nombre “OneDrive – MIEMPRESA”, en dicha carpeta se asegura la custodia, integridad y disponibilidad de la información, en caso de no tener la carpeta disponible se debe reportar inmediatamente al proceso de Tecnología de la Información a través de ticket en la mesa de ayuda.

- El uso de herramientas para almacenamiento de información en la nube como OneDrive y SharePoint debe ser exclusivo para procesos o documentos propios de sus funciones y son las únicas herramientas autorizadas para tal fin. Se prohíbe alojar información en otros gestores de almacenamiento en nube tales como: Dropbox, Google Drive, WeTransfer, etc., de requerirse acceso a alguna de estas plataformas, se debe solicitar el ingreso a través de ticket a mesa de ayuda con la respectiva autorización y justificación por parte del jefe directo.

- El uso compartido de documentos en herramientas como SharePoint y OneDrive debe realizarse únicamente entre colaboradores de la organización, utilizando exclusivamente las cuentas de correo corporativas asignadas por el personal de Tecnología de Información, si se requiere compartir información con un usuario externo y no se puede enviar a través del correo electrónico, se debe compartir a través del OneDrive enviando el respectivo link de acceso de ser posible de solo lectura y asignándole una clave de acceso que solo debe conocer el usuario o grupo de usuarios que requieran dicha información.

- Es responsabilidad del funcionario conocer la naturaleza de los documentos que se comparten a través de herramientas de almacenamiento en la Nube como OneDrive y SharePoint con otros funcionarios y usuarios externos, entendiendo el principio de confidencialidad e integridad de la información.

- Se prohíbe a los funcionarios acceder, manipular o descargar, archivos de SharePoint o OneDrive en equipos que no sean propiedad de Snider & CIA SAS. . Esta acción se considerará una falta grave y una violación a las políticas de seguridad de la información. En casos excepcionales donde sea imprescindible el uso de dispositivos personales para funciones críticas, el jefe inmediato deberá autorizar a mesa de ayuda, especificando el lugar de almacenamiento seguro y los dispositivos autorizados.

- El acceso o intento de acceso violento a información a la cual no se le ha otorgado permisos de ingreso por parte de Tecnología de la Información de acuerdo con la matriz de roles, se contempla como una violación a la confidencialidad de la información.

- El correo electrónico corporativo es una herramienta de trabajo que debe ser utilizado únicamente para envío y recepción de información de orden institucional, no puede ser utilizado para fines personales, lo anterior con el fin de facilitar las labores propias del cargo de cada funcionario; adicional es un medio formal y oficial de comunicaciones de Snider & CIA SAS.

- Las cuentas de correo electrónico serán creadas de acuerdo con el cargo asignado y deben cumplir con la siguiente nemotecnia:

  - Nombre del Cargo + @snider.com.co

  - Si se tiene alguna coincidencia con otro funcionario con el mismo cargo, se adicionará un numero consecutivo.

  - El nombre para mostrar en la cuenta de correo será el nombre completo del funcionario.

- Snider & CIA SAS, en aras de brindar un buen servicio con el correo electrónico e incrementar los niveles de ciberseguridad, se permite realizar las siguientes consideraciones:

  - Las cuentas de correo institucional son de uso personal e intransferible, por lo tanto, es responsabilidad del funcionario proteger y resguardar la contraseña y no suministrarla en ninguna circunstancia y cambiarla en los tiempos establecidos y con los parámetros indicados en el procedimiento "*Control al sistema de información*".

  - Las cuentas de correo corporativo deben utilizar MFA (doble factor de autenticación) como método para garantizar la seguridad de la información, protegiendo a los usuarios de Snider & CIA SAS. contra amenazas de ciberseguridad, como el robo de identidad y el acceso no autorizado a información confidencial.

  - Excepción para procesos automáticos

  - Existe una excepción a esta política para las cuentas de correo asignadas a procesos automáticos. Dado que estas cuentas son operadas por sistemas automatizados (robots) para enviar y recibir información, no requerirán la instalación ni utilización del MFA (doble factor de autenticación).

  - El correo electrónico no se debe utilizar para enviar videos, música, cadenas, chistes, propagandas, ofertas, negocios personales, avisos publicitarios, etc., a funcionarios internos y usuarios externos.

  - No se pueden enviar, recibir ni ejecutar a través del correo electrónico archivos adjuntos con extensiones (.jar, .exe, .tar, .bat, .msi, .zip), estas pueden contener virus o software malicioso que podrían infectar, dañar o recopilar información de los equipos o dispositivos informáticos.

  - Ningún funcionario puede compartir contactos o listas de distribución de Snider & CIA SAS con personal externo con el fin de propiciar el envío de ofertas, propagandas, negocios o material publicitario, esto genera una vulnerabilidad y/o riesgo a la seguridad de la información.

- La cuenta de correo electrónico corporativo no debe ser inscrita en páginas de publicidad, compras, deportes, apuestas, casinos, redes sociales o a otra que sea ajena a temas laborales.

- El correo electrónico corporativo es creado para el uso exclusivo de las labores propias de los funcionarios, por lo tanto, debe hacer uso de este con criterios de respeto, responsabilidad, integridad y ciberseguridad de la información, por lo anterior la información contenida es estos es propiedad de Snider & CIA SAS, y no se hace responsable de datos o información personal que los funcionarios almacenen en las cuentas institucionales.

- El correo electrónico institucional no se debe utilizar para el envío de correos con mensajes que quebranten las normas legales, la intimidad o el buen nombre de las personas, la moral, el orden público, que contengan contenido irrespetuoso, difamatorio, racista, discriminatorio, acoso; así como videos o imágenes con información ilegal, extorsiva o material sexual.

- Todo mensaje sospechoso o de procedencia desconocida, SPAM, debe ser ignorado y eliminado inmediatamente, en caso de abrirlo por error, se debe reportar inmediatamente a la mesa de ayuda, con el fin de evitar posibles infecciones por virus o códigos maliciosos.

- Los buzones de correo electrónico cuentan con una capacidad de almacenamiento de 50 Gb para licenciamiento básico y estándar y de 100 Gb para licencias E3, una vez se llegue a su máxima capacidad se debe informar a la mesa de ayuda para proceder con el respectivo backup.

- El tamaño de los archivos adjuntos en el correo electrónico no debe superar las 30 Mb, si requiere el envío de un archivo de mayor tamaño, puede ser compartido a través del OneDrive, de ser necesario puede solicitar apoyo a través de la mesa de ayuda.

- Como política de ciberseguridad, se prohíbe el envío de información de la entidad desde o con destino a cuentas de correo o sistemas de almacenamiento personal de los funcionarios.

- El área de Tecnología de la Información a través de la consola de informes de seguimiento de office365, verificara aleatoriamente el flujo de los correos salientes con el fin de controlar y evitar pérdidas y fuga de información.

- El área de Tecnología de la información a través de la consola antivirus y del firewall perimetral restringe el acceso a plataformas de correo tales como: Gmail, Hotmail y Yahoo, con el fin de evitar pérdidas y fugas de información corporativa, de requerirse acceso, se debe solicitar el ingreso a través de ticket a mesa de ayuda con la respectiva autorización y justificación por parte del jefe directo.

- El envío de correos masivos con temas informativos, comunicados, temas de interés general o de información importante de carácter institucional solo podrán ser enviados por los lideres de proceso y/o por el área de marketing y comunicaciones.

- Los sistemas de información establecidos para el manejo, recepción y envío de información son los definidos en el procedimiento *"Control al sistema de información"*.

- El uso de medios externos como lo son: USB, Memorias SD, Cámaras Fotográficas, celulares está habilitado por GPO de directorio activo y por consola de antivirus en modo de solo lectura para todos los funcionarios (Solo se puede descargar información desde estos dispositivos hacia el equipo corporativo), la copia de información desde el equipo corporativo hacia estos dispositivos no está permitida.

  Nota: de ser necesario la habilitación de los puertos para el cumplimiento de una función debe ser solicitado con justificación por el jefe directo a mesa de ayuda.

- El área de Tecnología de la Información establece en la consola antivirus una regla de control de dispositivos y ciberseguridad, para evitar la extracción de información a través de dispositivos de almacenamiento extraíbles. Si un funcionario intentase copiar información, en la consola quedará consignado el reporte con los siguientes datos:

  - Fecha y hora
  - Usuario
  - Dispositivo o nombre el equipo
  - Acción Realizada
  - Tipo de Dispositivo o fabricante

- Los daños físicos ocasionados a recursos de tecnología, bien sea por uso inadecuado o abuso. En tales casos, el costo de la reparación o remplazo del equipo deben ser directamente asumidos por el funcionario que tenga el equipo o activo asignado.

- Está prohibido el consumo de alimentos y bebidas en los puestos de trabajo, ya que esto puede ocasionar daños a los recursos tecnológicos asignados.

- Todos los funcionarios que cuenten con equipos de cómputo portátiles y que estén dentro de las instalaciones de Snider & CIA SAS, deben tener instalada su respectiva guaya de seguridad con el fin de evitar pérdidas o robo, en caso de no tenerla deben solicitarla al área de Tecnología de la Información y mientras se asigna, al terminar su jornada laboral o retirarse de su puesto de trabajo deben resguardar el equipo bajo llave o dejarlo en custodia del área de tecnología de la información o seguridad.

- Para los funcionarios que trabajen bajo la modalidad de teletrabajo, trabajo en casa o en modalidad hibrida, se les proporcionará una guaya. A pesar de que su lugar de trabajo principal sea su hogar, se comprometen a utilizar la guaya de seguridad en todas las ocasiones en que deban trabajar en las instalaciones de Snider & CIA SAS. La clave de la guaya de seguridad está compuesta por 4 dígitos numéricos y es asignada por el área de tecnología de la información, y se deben tener las siguientes consideraciones:

  - La clave es personal e intransferible.

  - La clave asignada en ninguna circunstancia debe ser cambiada por el funcionario, ya que el área de Tecnología lleva un control de estas.

En caso de encontrarse un equipo sin guaya:

- El área de seguridad y/o el área de tecnología de la información podrán levantar o recoger los equipos que se encuentren desatendidos, dentro de las instalaciones de Snider & CIA SAS.

- Se enviará correo electrónico como llamado de atención a la persona responsable del equipo y su líder de área.

- En caso de que se repita la situación, se procederá a reportar ante capital humano por incumplimiento de la política.

- En ninguna circunstancia los equipos de cómputo pueden ser dejados desatendidos en lugares públicos o a la vista.

- En caso de robo o pérdida del equipo o activo, deberá presentarse denuncia a las autoridades competentes de manera inmediata y el suceso debe ser reportado posteriormente a su jefe inmediato, al área de Tecnología de la Información y al área de gestión de seguridad. El valor de reposición de este debe ser asumido por el funcionario que tenga asignado el activo.

- El acceso remoto a la información y a las aplicaciones informáticas fuera de la sede principal y de las sucursales, se debe hacer a través de una conexión VPN, la cual es instalada y suministrada por el área de tecnología de la información. Esta VPN solo está autorizada en equipos corporativos.

- Evitar hacer uso de redes inalámbricas publicas abiertas (Wifi públicas), para transmitir información institucional

- No se permite el acceso o conexiones a través de aplicaciones de escritorio remoto tales como Anydesk, TeamViewer, VNC, debido a que estas no están licenciadas por Snider & CIA SAS, la herramienta autorizada para tal fin es Logmein.

- Excepción para el uso de Anydesk en casos excepcionales:

  En situaciones excepcionales en las que mesa de ayuda no pueda acceder a un equipo mediante Logmein para brindar soporte, se permite la instalación de Anydesk. Sin embargo, esta excepción debe cumplir con las siguientes condiciones:

  - Solo se debe instalar Anydesk cuando no sea posible acceder al equipo del usuario a través de Logmein debido a problemas técnicos o limitaciones.

  - Anydesk solo debe instalarse de manera temporal por mesa de ayuda y exclusivamente para resolver el problema específico del usuario.

  - Una vez finalizado el proceso de soporte, mesa de ayuda de programar la desinstalación inmediata de Anydesk en el equipo del usuario.

- A través del directorio activo está habilitado por GPO el bloqueo de pantalla el cual se activa a los 5 minutos de inactividad en el equipo, adicional los funcionarios deben bloquear la pantalla cuando por cualquier motivo deba dejar su puesto de trabajo, también lo pueden hacer combinando las teclas del símbolo de Windows + L.

- Los funcionarios de los sistemas de información deben cerrar las aplicaciones y sesiones de red cuando no se estén usando, termine su jornada laboral o se retire de su puesto de trabajo.

- Los funcionarios deben apagar y desconectar su equipo de cómputo al finalizar jornada laboral. Esta medida excluye a los funcionarios cuyas labores requieren mantener el equipo encendido. Esta acción contribuye a Snider & CIA SAS reduciendo la huella de carbono.

- Los funcionarios al terminar su jornada laboral deben dejar los escritorios y/o puestos de trabajo libres de documentos físicos que contengan información confidencial o reservada, estos deben estar bajo llave en un lugar seguro.

Los escritorios y/o puestos de trabajo deben permanecer limpios y ordenados, las impresoras y los escáner deben permanecer libres de documentos.

5. RESPONSABILIDADES.

La Alta Dirección de la SNIDER & CIA S.A.S, asume la responsabilidad de velar por la comunicación a sus funcionarios, la publicación a sus partes interesadas, así como garantizar el cumplimiento, revisión y actualización de esta política.

Los funcionarios y demás partes interesadas son responsables de dar estricto cumplimiento a esta política. El incumplimiento de esta por parte de los funcionarios acarreará sanciones disciplinarias según lo establecido en el reglamento interno de trabajo sin perjuicio de las demás consecuencias legales a que haya lugar.

6. FIRMA

1. ALCANCE

La presente política se establece en cumplimiento de lo contenido en la normatividad legal vigente (Resolución 0312 de 2019) y demás normas aplicables en temas de Seguridad y Salud en el Trabajo. Aplica para **Snider & CIA. S.A.S**

2. OBJETIVOS

- Proporcionar a los trabajadores el conocimiento y recursos necesarios para desempeñar su trabajo en forma eficiente y segura, cumpliendo con estándares de Seguridad y Salud en el Trabajo.

- Cumplir con las actividades propuestas dentro del plan de trabajo establecido al inicio de cada periodo, buscando mitigar peligros a través de la identificación de los riesgos asociados a su operación y la prevención y promoción de la salud del colaborador.

3. INDICADORES

- Indicador general de ausentismo por causa médica
- Indicador de frecuencia de accidentalidad
- Indicador de severidad de accidentalidad
- Indicador de proporción de accidentes mortales
- Indicador de incidencia de Enfermedad Laboral
- Indicador de prevalencia de Enfermedad Laboral
- Indicador de ejecución del Plan de Trabajo Anual

4. CONTENIDO

Snider & CIA. S.A.S es una empresa que presta el servicio de almacenamiento de mercancías bajo el control aduanero, mercancías nacionales y nacionalizadas, y administración de inventarios. Mediante la presente política define su Sistema de Gestión de Seguridad y Salud en el Trabajo, orientado al cuidado individual y colectivo.

La organización está comprometida en fomentar comportamientos socialmente responsables mediante mecanismos que permitan la participación de sus colaboradores de manera presencial y remota, vinculando también a sus contratistas, visitantes y proveedores; dando cumplimiento a la legislación vigente en Seguridad y Salud en el Trabajo, destinando los recursos económicos, humanos y tecnológicos necesarios para garantizar un ambiente de trabajo sano y seguro.

La consulta y participación activa de los trabajadores y todas las partes interesadas en la gestión de la prevención de riesgos laborales, es fundamental para el establecimiento de una cultura preventiva.

Como parte fundamental de su sistema de gestión, la organización busca mitigar la ocurrencia de incidentes y accidentes de trabajo, enfermedades laborales, enfermedades de salud pública o emergencias sanitarias a través de la identificación de los riesgos y la eliminación de peligros que puedan atentar contra la salud e integridad física de los mismos; mediante la planeación, seguimiento y monitoreo del plan de trabajo que conlleva a la mejora continua del sistema.

Para el cumplimiento y logro de los objetivos propuestos **SNIDER & CIA. SAS** se compromete a:

- Identificar los peligros, evaluar y valorar los riesgos, además de establecer los controles necesarios
- Cumplir con la legislación vigente y otros requisitos aplicables en Seguridad y Salud en el Trabajo
- Establecer objetivos y metas con base en los riesgos prioritarios, para el buen desempeño y mejora continua del sistema de gestión en Seguridad y Salud en el Trabajo

5. RESPONSABILIDADES

La Alta Dirección de **SNIDER & CIA. SAS**, asume la responsabilidad de velar por la comunicación a sus colaboradores, la publicación a sus partes interesadas, así como garantizar el cumplimiento, revisión y actualización de esta política.

Los colaboradores y demás partes interesadas son responsables de dar estricto cumplimiento a esta política. El incumplimiento de esta por parte de los colaboradores, acarreará sanciones disciplinarias según lo establecido en el reglamento interno de trabajo sin perjuicio de las demás consecuencias legales a que haya lugar.

6. FIRMA

1. ALCANCE:

SNIDER & CIA S.A.S, especializada en almacenamiento de mercancías bajo control aduanero, mercancías nacionales, administración de inventarios, usuario comercial en zona franca, su Alta Dirección, Líderes de Proceso y Colaboradores se comprometen en apoyar e implementar medidas de control para la prevención, mitigación, corrección y/o compensación frente a sus impactos y riesgos ambientales significativos, así como, el cumplimiento de la normatividad ambiental y otros requisitos, la asignación de los recursos necesarios y el fortalecimiento de una cultura sostenible, con el fin de prevenir la contaminación generada por la prestación de sus servicios y la protección del medio ambiente para las generaciones futuras, integrando la responsabilidad social como mecanismo de prevención y control para evitar el abuso laboral, discriminación, trabajo forzoso, trabajo infantil y otras violaciones a los derechos humanos, mejorando continuamente el desempeño sostenible y demostrando un equilibrio entre los pilares económico, social y ambiental.

SNIDER & CIA S.A.S, en cumplimiento de la Norma Técnica ISO 14001:2015 establece, implementa y mantiene su política de Sostenibilidad Ambiental.

2. OBJETIVOS:

Para el cumplimiento y logro del Sistema de Gestión Ambiental, **SNIDER & CIA S.A.S** tiene como objetivos:

- Verificar el desempeño ambiental derivado del establecimiento de medidas de control para impactos y riesgos ambientales significativos generando planes de acción para una mejora continua.
- Asignar recursos financieros, humanos, tecnológicos y de infraestructura necesarios para el mantenimiento y mejora del Sistema de Gestión Ambiental.
- Cumplir con la normativa ambiental y otros requisitos aplicables a la organización.
- Fomentar y fortalecer la cultura sostenible en los colaboradores de la organización
- Implementar un programa de Responsabilidad Social Empresarial que fomente la inclusión, trabajo con distintas comunidades y enmarcado en la agenda de Desarrollo Sostenible global.

3. INDICADORES

- Consumo Agua
- Consumo de Energía
- Generación de Residuos Aprovechables
- Huella de Carbono
- Cumplimiento Programa de Capacitaciones
- Cumplimiento Legal
- Desempeño Ambiental
- Desempeño RSE

4. RESPONSABILIDADES.

La Alta Dirección de **SNIDER & CIA S.A.S** asume la responsabilidad de velar por la comunicación a sus colaboradores, la publicación a sus partes interesadas, así como garantizar su cumplimiento, revisión y actualización de esta política.

Los colaboradores y demás partes interesadas son responsables de dar estricto cumplimiento a esta política. El incumplimiento de esta por parte de los colaboradores acarreará sanciones disciplinarias según lo establecido en el reglamento interno de trabajo sin perjuicio de las demás consecuencias legales a que haya lugar.

5. FIRMA

POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES SNIDER & CÍA. S.A.S

1. ALCANCE Y OBLIGACIONES:

Esta política aplica para todos los titulares de información personal que sea utilizada y/o se encuentre en las bases de datos de **EL RESPONSABLE,** quien actúa en calidad de responsable del tratamiento de los datos personales.

Esta política es de obligatorio cumplimiento para **EL RESPONSABLE**, en calidad de responsable, así como todos los terceros que obran en nombre de **EL RESPONSABLE,** o que, sin actuar en nombre de **EL RESPONSABLE,** utilicen datos personales a su nombre como encargados.

Tanto el responsable como encargados, inclúyase, empleados y terceros que traten datos a nombre de **EL RESPONSABLE,** deben conocer y practicar esta política en el cumplimiento de las funciones y/o actividades aún después de terminados los vínculos legales, comerciales, laborales o de cualquier índole. De igual manera, se comprometen a guardar estricta confidencialidad en relación con los datos tratados.

2. OBJETIVO GENERAL DE LA POLÍTICA.

El objetivo general de la presente Política es establecer los lineamientos para garantizar el adecuado cumplimiento de lo dispuesto en la Ley 1581 de 2012 y en el Decreto 1074 de 2015, para desarrollar de manera suficiente el derecho constitucional al Hábeas Data que tienen todas las personas naturales respecto de las cuales **EL RESPONSABLE** de los datos personales, haya recogido, administre o conserve información de carácter personal.

2.1. OBJETIVOS ESPECÍFICOS DE LA POLÍTICA

Adoptar los lineamientos generales para el tratamiento de los datos personales administrados por **EL RESPONSABLE,** en cumplimiento de la normatividad vigente sobre la materia.

Establecer el tratamiento al cual son sometidos los datos personales por **EL RESPONSABLE,** y su finalidad.

Definir los procedimientos generales para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar, suprimir información y revocar la autorización de tratamiento de datos personales en los casos que la ley lo permita.

Establecer los criterios que permitan clasificar a **EL RESPONSABLE,** la información de carácter personal y al mismo tiempo respetar los derechos fundamentales a la intimidad, hábeas data y protección de datos de los ciudadanos.

3. INDICADORES

- Control de Solicitudes

4. CONTENIDO

AUTORIZACIÓN DE LA POLÍTICA DE TRATAMIENTO

De acuerdo con el artículo 9 de la Ley 1581 de 2012, para el tratamiento de datos personales se requiere la autorización previa e informada del Titular. Mediante la aceptación de la presente política, todo Titular que facilite información relativa a sus datos personales está consintiendo el tratamiento de sus datos por parte de **EL RESPONSABLE**, en los términos y condiciones recogidos en la misma.

INFORMACIÓN DEL RESPONSABLE DEL TRATAMIENTO DE INFORMACIÓN PERSONAL.

El responsable del tratamiento de las bases de datos objeto de esta política es **EL RESPONSABLE,** cuyos datos de contacto son los siguientes:

- **Razón social:** SNIDER & CÍA. S.A.S
- **NIT:** 860.517.479-4
- **Domicilio:** Avenida el Dorado # 96 a - 47
- **Email Principal:** info@snider.com.co
- **Teléfono:** 601 5551795
- **Página WEB:** www.snider.com.co

TRATAMIENTO AL CUAL SERÁN SOMETIDOS LOS DATOS PERSONALES Y SU FINALIDAD.
EL RESPONSABLE, en el desarrollo de su actividad, lleva a cabo el tratamiento de datos personales relativos a personas naturales que están contenidos y son tratados en bases de datos destinadas a finalidades legítimas, cumpliendo con la Constitución y la Ley.
Los datos personales serán sometidos a procedimientos de recolección, uso, almacenamiento, circulación y supresión; Para las siguientes finalidades según el tipo de titular.
La siguiente tabla (Tabla I) presenta las distintas bases de datos que maneja **EL RESPONSABLE,** y las finalidades asignadas a cada una de ellas.

Tabla I. Bases de datos y finalidades

Base de datos	Finalidad Legitima	Finalidad descrita por la Superintendencia de industria y comercio
EMPLEADOS	Efectuar las gestiones pertinentes para el desarrollo del objeto social de **EL RESPONSABLE**, en lo que tiene que ver con el cumplimiento del objeto del contrato celebrado con el Titular de la información. Registrar datos personales y de carácter sensible a fin de mantener una relación contractual (Gestión de empleo, Nómina, Aportes a seguridad social del titular y de sus beneficiarios). Desarrollar procesos de gestión y recursos humanos, controlando las etapas de convocatoria, selección, promoción, novedades de personal y actualización de nómina. Realizar seguimiento a su historial laboral desde el ingreso hasta la desvinculación. Desarrollar el Sistema de Seguridad y Salud en el trabajo. Mantener los soportes históricos de los pagos de seguridad social y del desempeño propio de sus labores y soporte de capacitaciones Uso de datos biométricos para el acceso a las instalaciones de **EL RESPONSABLE**, el control de horario y video vigilancia para la seguridad. Realizar invitaciones a eventos, ofrecer nuevos productos y servicios. Enviar mensajes con contenidos institucionales, notificaciones, información relativa de **EL RESPONSABLE**, a través de correo electrónico y/o mensajes al teléfono móvil (SMS y/o aplicaciones). Gestionar trámites (solicitudes, quejas, reclamos).	-Finalidades varias – Custodia y gestión de información y bases de datos. -Gestión contable, fiscal y administrativa - Verificación de datos y referencias. -Recursos humanos - Gestión de personal -Seguridad - Seguridad y control de accesos -SST -Publicidad y prospección comercial - Publicidad propia

	Ofrecer programas de bienestar corporativo y planificar actividades empresariales, para el titular y sus beneficiarios (hijos, cónyuge, compañero permanente). Suministrar información de contacto a la fuerza comercial y/o red de distribución, telemercadeo, investigación de mercados y cualquier tercero con el cual **EL RESPONSABLE** tenga un vínculo contractual para el desarrollo de actividades de ese tipo (investigación de mercados y telemercadeo, etc.) para la ejecución de estas. Registrar datos personales y de carácter sensible en este caso datos biométricos (foto), para publicidad impresa y digital de uso exclusivo de **EL RESPONSABLE**. Registrar datos personales y de carácter sensible en este caso la huella dactilar, a fin de autorizar la consulta de antecedentes y realizar pruebas de alcohol y drogas. Suministrar la información a terceros con los cuales **EL RESPONSABLE**, tenga relación contractual y que sea necesario entregársela para el cumplimiento del objeto contratado. Realizar consultas y verificación en listas restrictivas y vinculantes en relación con el LAFT-FPADM Realizar consultas y verificación en centrales de riesgo	
PROVEEDORES Y CONTRATISTAS	Efectuar las gestiones pertinentes para el desarrollo del objeto social de **EL RESPONSABLE**, en lo que tiene que ver con el cumplimiento del objeto del contrato y/o relación comercial celebrado con el Titular de la información. Registrar datos personales y de carácter sensible a fin de mantener una relación contractual y/o relación comercial (Gestión de Proveedores y Contratistas). Dar trámite a la información financiera y contable. Desarrollar el Sistema de Seguridad y Salud en el trabajo. Uso de datos biométricos para el acceso a las instalaciones de **EL RESPONSABLE**, el control de horario y video vigilancia para la seguridad. Realizar invitaciones a eventos, ofrecer nuevos productos y servicios. Enviar mensajes con contenidos institucionales, notificaciones, información relativa de **EL RESPONSABLE**, a través de correo electrónico y/o mensajes al teléfono móvil (SMS y/o aplicaciones). Gestionar trámites (solicitudes, quejas, reclamos). Suministrar información de contacto a la fuerza comercial y/o red de distribución, telemercadeo, investigación de mercados y cualquier tercero con el cual **EL RESPONSABLE** tenga un vínculo contractual para el desarrollo de actividades de ese tipo (investigación de mercados y telemercadeo, etc.) para la ejecución de estas. Transmitir los datos personales fuera del país a terceros con los cuales **EL RESPONSABLE**, haya suscrito un contrato de procesamiento de datos y sea necesario entregársela para el cumplimiento del objeto contractual.	-Finalidades varias – Custodia y gestión de información y bases de datos -Gestión contable, fiscal y administrativa - Gestión proveedores -Gestión técnica y administrativa – Desarrollo operativo -Envió de comunicaciones

	Suministrar la información a terceros con los cuales **EL RESPONSABLE**, tenga relación contractual y que sea necesario entregársela para el cumplimiento del objeto contratado. Realizar consultas y verificación en listas restrictivas y vinculantes en relación con el LAFT-FPADM Realizar consultas y verificación en centrales de riesgo.	
VISITANTES	Efectuar las gestiones pertinentes para el desarrollo del objeto social de **EL RESPONSABLE**, en lo que tiene que ver con la atención al Titular de la información. Registrar datos personales y de carácter sensible a fin de mantener una relación contractual (Gestión de Visitantes). Desarrollar el Sistema de Seguridad y Salud en el trabajo. Uso de datos biométricos para el acceso a las instalaciones de **EL RESPONSABLE**, el control de Ingresos y salidas y video vigilancia para la seguridad. Gestionar trámites (solicitudes, quejas, reclamos).	-Finalidades varias – Custodia y gestión de información y bases de datos -Gestión técnica y administrativa – Desarrollo operativo -Envió de comunicaciones
BIOMÉTRICA	Registrar imágenes de video por seguridad de las instalaciones, residentes y visitantes. Registrar acceso a las instalaciones y su permanencia.	-Seguridad - Seguridad y control de acceso a edificios
CLIENTES	Efectuar las gestiones pertinentes para el desarrollo del objeto social de **EL RESPONSABLE**, en lo que tiene que ver con el cumplimiento del objeto de la relación contractual y/o comercial celebrado con el Titular de la información. Registrar datos personales y de carácter sensible a fin de mantener una relación contractual y/o comercial (Gestión de Clientes). Dar trámite a la información financiera y contable. Bajo la responsabilidad del titular autoriza a **EL RESPONSABLE**, Transferir los datos personales fuera del país a los AGENTES INTERNACIONALES para el cumplimiento del objeto contractual y/o comercial. Así mismo da la autorización al tercero para el tratamiento de la información. Uso de datos biométricos para el acceso a las instalaciones de **EL RESPONSABLE**, el control de horario y video vigilancia para la seguridad. Realizar invitaciones a eventos, ofrecer nuevos productos y servicios. Enviar mensajes con contenidos institucionales, notificaciones, información relativa de **EL RESPONSABLE**, a través de correo electrónico y/o mensajes al teléfono móvil (SMS y/o aplicaciones). Gestionar trámites (solicitudes, quejas, reclamos). Suministrar información de contacto a la fuerza comercial y/o red de distribución, telemercadeo, investigación de mercados y cualquier tercero con el cual **EL RESPONSABLE** tenga un vínculo contractual para el desarrollo de actividades de ese tipo (investigación de mercados y telemercadeo, etc.) para la ejecución de estas.	-Gestión técnica y administrativa – Desarrollo operativo -Envió de comunicaciones -Gestión contable, fiscal y administrativa -Gestión económica y contable.

	Transmitir los datos personales fuera del país a terceros con los cuales **EL RESPONSABLE**, haya suscrito un contrato de procesamiento de datos y sea necesario entregársela para el cumplimiento del objeto contractual. Suministrar la información a terceros con los cuales **EL RESPONSABLE**, tenga relación contractual y que sea necesario entregársela para el cumplimiento del objeto contratado. Dar trámite a los requerimientos de los organismos de control y vigilancia. Realizar consultas y verificación en listas restrictivas y vinculantes en relación con el LAFT-FPADM Realizar consultas y verificación en centrales de riesgo.	
SOCIOS	Registrar datos personales y de carácter sensible a fin de mantener una relación contractual (Gestión de Socios). Tramitar de manera la información financiera y contable. Uso de datos biométricos para el acceso a las instalaciones de **EL RESPONSABLE**, el control de Ingresos y salidas y video vigilancia para la seguridad. Realizar invitaciones a eventos, ofrecer nuevos productos y servicios. Enviar mensajes con contenidos institucionales, notificaciones, información relativa de **EL RESPONSABLE**, a través de correo electrónico y/o mensajes al teléfono móvil (SMS y/o aplicaciones). Gestionar trámites (solicitudes, quejas, reclamos). Suministrar información de contacto a la fuerza comercial y/o red de distribución, telemercadeo, investigación de mercados y cualquier tercero con el cual **EL RESPONSABLE** tenga un vínculo contractual para el desarrollo de actividades de ese tipo (investigación de mercados y telemercadeo, etc.) para la ejecución de estas. Dar trámite a los requerimientos de los organismos de control y vigilancia. Realizar consultas y verificación en listas restrictivas y vinculantes en relación con el LAFT Realizar consultas y verificación en centrales de riesgo.	-Finalidades varias - Fines históricos, científicos o estadísticos -Finalidades varias - Procedimientos administrativos -Gestión Técnica y Administrativa - Envío de comunicaciones

La siguiente tabla (Tabla II) presenta la descripción del procedimiento de ciclo de vida del dato, de las bases de datos que maneja LA ORGANIZACIÓN, y las finalidades asignadas a cada una de ellas.

Tabla II. Procedimiento de ciclo de vida del dato

Base De Datos	Recolección	Uso	Almacenamiento	Circulación	Eliminación
EMPLEADOS	-Solicitud de documentos físicos o electrónicos. Solicitud de información personal. -Registro biométrico (CCTV, fotografías y video corporativos)	Pagos de nómina, gestión laboral, sistema de gestión de seguridad y salud en el trabajo, afiliaciones. Enviar mensajes con contenidos institucionales, notificaciones, información relativa de **EL RESPONSABLE.**	Física y electrónica	Se realiza circulación, con las empresas de **LA ORGANIZACIÓN,** solo se circula a las autoridades competentes por solicitud en términos fiscales.	Se almacenan de forma indefinida.
PROVEEDORES Y CONTRATISTAS	-La información se recolecta por referenciación, por búsqueda en internet o por propuestas presentadas por el proveedor. -Solicitud de documentos físicos o electrónicos.	Gestión de pagos, gestión administrativa y contractual, evaluación de proveedores, gestión del producto o servicio	Almacenamiento físico, registro electrónico.	Se realiza circulación, con las empresas de **LA ORGANIZACIÓN,** solo se circula a las autoridades competentes por solicitud en términos fiscales.	No se realiza eliminación.
VISITANTES	La información se recolecta en la portería al momento de ingresar, se solicitan los siguientes datos: nombre, No de documento, ARL, EPS, persona a visitar, número de teléfono en caso de alguna emergencia, datos del vehículo o equipo portátil y número de ficha si el	Control de visitantes a las instalaciones	Registro electrónico	Se realiza circulación, con las empresas de **LA ORGANIZACIÓN,** solo se circula a las autoridades competentes por solicitud en términos fiscales.	Se almacenan de forma indefinida

	computador es de alguna de las empresas de la Organización				
BIOMÉTRICA	-La información se recolecta por medio de cámaras de videovigilancia ubicadas en las instalaciones	La información se utiliza para seguridad y registro de accesos	La información se almacena en un DVR ubicado en las instalaciones	Se realiza circulación, con las empresas de **LA ORGANIZACIÓN,** solo se circula a las autoridades competentes por solicitud en términos fiscales.	Tiene una capacidad de almacenamiento de aproximadamente 20 días.
CLIENTES	-La información se recolecta a través de llamadas telefónicas, correos electrónicos. - Solicitud de documentos físicos o electrónicos. -Radicación de documentos físicos y electrónicos por parte del titular de la información.	-Registra datos personales y de carácter sensible a fin de mantener una relación contractual. -Recopilación de información para establecer comunicaciones en el desarrollo de la relación contractual. -Dar trámite a los requerimientos de los organismos de control y vigilancia, -Recepción y administración de la información y documentación necesaria para el buen desarrollo de las funciones de **EL RESPONSABLE.** -Ingreso, registro, control y trazabilidad de peticiones, quejas, reclamos o sugerencias. -Histórico para investigación, estudios especializados y/o planteamientos en políticas públicas.	Almacenamiento físico, registro electrónico.	Se realiza circulación, con las empresas de **LA ORGANIZACIÓN,** solo se circula a las autoridades competentes por solicitud en términos fiscales.	Se almacenan de forma indefinida.

		Manejo adecuado de la información financiera y contable.			
SOCIOS	-Solicitud de documentos físicos o electrónicos. Solicitud de información personal. -Registro biométrico (CCTV, fotografías y video corporativos)	-Registros históricos y administrativos -Gestión gerencial y administrativa -Enviar mensajes con contenidos institucionales, notificaciones, información relativa de **EL RESPONSABLE**, a través de correo electrónico y/o mensajes al teléfono móvil. -Participar en la publicidad relativa a **EL RESPONSABLE.** -Manejo adecuado de la información financiera y contable.	Almacenamiento físico, registro electrónico.	Se realiza circulación, con las empresas de **LA ORGANIZACIÓN,** solo se circula a las autoridades competentes por solicitud en términos fiscales.	Se almacenan de forma indefinida

CATEGORÍAS ESPECIALES DE DATOS

La Ley estatutaria de Protección de Datos Personales (LEPD) considera dentro de la categoría de datos especiales, los datos sensibles y los relativos a las niñas, niños y adolescentes, Artículos 5° y 7° respectivamente.

Datos sensibles

En la categoría de datos sensibles, **EL RESPONSABLE** realiza tratamiento de información relativa a la salud y biométrica

La LEPD prohíbe el tratamiento de datos sensibles, excepto cuando:

a. El titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.

b. El tratamiento sea necesario para salvaguardar el interés vital del titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.

c. El tratamiento sea efectuado en el curso de las actividades legítimas de **EL RESPONSABLE**

d. El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

e. El tratamiento tenga una finalidad histórica, estadística o científica. En este evento se adoptan las medidas conducentes a la supresión de identidad de los titulares.

Por disposición del decreto 1377 de 2013 se informa al titular que:

a. Por tratarse de datos sensibles no está obligado a autorizar su tratamiento.

b. El tratamiento de los datos relativos a salud, son tratados de acuerdo con las finalidades definidas.

c. Ninguna actividad podrá condicionarse a que el titular suministre datos personales sensibles.

DERECHOS DE LOS TITULARES.

De acuerdo con lo previsto en el artículo 8 de la LEPD y los artículos 21 y 22 del Decreto 1377 de 2013, los Titulares de los datos pueden ejercer una serie de derechos con relación al tratamiento de sus datos personales. Estos derechos podrán ejercerse por las siguientes personas.

- Por el Titular, quién deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.
- Por sus causahabientes, quienes deberán acreditar tal calidad.
- Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.
- Por estipulación a favor de otro y para otro.

De conformidad con lo establecido en el artículo 8 de la Ley 1581 de 2012 y el decreto 1377 de 2013, el titular de los datos personales tiene los siguientes derechos frente a **EL RESPONSABLE.**

- Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado;
- Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley;
- Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que les ha dado a sus datos personales;
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen;
- Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución;
- Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

Derechos de los niños, niñas y adolescentes
En el tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.
Queda proscrito el tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública.
Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto al tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás.

TRATAMIENTO DE DATOS SENSIBLES
EL RESPONSABLE, no recolectará ni tratará datos personales ligados a ideologías políticas, afiliación sindical, creencias religiosas, vida sexual u origen étnico. Los casos en que sean necesarios datos biométricos, de salud o de menores de edad solo se utilizarán con autorización expresa del titular o de su responsable.
La información personal de carácter sensible que se pueda obtener de un proceso interno, selección de personal o de ejecución de contratos será protegida a través de las medidas de seguridad apropiadas.
EL RESPONSABLE, prohíbe el acceso, uso, gestión, cesión, comunicación, almacenamiento y cualquiera otro tratamiento de datos personales de carácter sensible sin autorización del titular del dato personal.
El incumplimiento de esta prohibición por parte de los empleados o proveedores y/o terceros será considerado como falta grave, que podrá dar lugar a la terminación de la relación laboral, contractual o comercial.
Los datos sensibles que se identifiquen serán informados al titular a más tardar al momento de la recolección, una vez se cumpla con sus finalidades y con los tiempos estipulados por la ley se procederá a eliminarlos de manera segura.

ATENCIÓN DE PETICIONES, CONSULTAS Y RECLAMOS.
La persona o área responsable de la atención de consultas y reclamos, ante la cual el titular de la información puede ejercer los derechos a conocer, actualizar, rectificar, suprimir el dato y/o revocar la autorización de tratamiento de datos personales, es **EL OFICIAL DE PROTECCIÓN DE DATOS** de **EL RESPONSABLE** con los siguientes canales de atención.

- **Persona o área responsable:** OFICIAL DE PROTECCIÓN DE DATOS
- **Email:** protecciondedatos@snider.com.co

Así mismo, usted podrá realizar las solicitudes o consultar nuestra Política de Protección de Datos Personales por escrito en el domicilio de **EL RESPONSABLE,** en el horario de 8:00 AM A 5:00 PM de lunes a viernes, o ingresando a la página web de **EL RESPONSABLE.**

EJERCICIO Y PROCEDIMIENTO PARA EJERCER LOS DERECHOS AL HABEAS DATA (CONSULTA, RECLAMO Y REVOCATORIA DE AUTORIZACIÓN).
En cumplimiento de las normas sobre protección de datos personales***,*** **EL RESPONSABLE,** presenta el procedimiento para ejercer los derechos al habeas data.

Consulta: **EL RESPONSABLE,** garantiza el derecho de consulta, suministrando a las personas que actúen en ejercicio de este derecho, toda la información contenida en el registro individual o que esté vinculada con la identificación del titular.
Para la atención de solicitudes de consulta de datos personales **EL RESPONSABLE,** garantiza que existen medios de comunicaciones electrónicas y asistidas de manera telefónica.
En cualquier caso, independientemente del mecanismo implementado para la atención de solicitudes de consulta, las mismas serán atendidas en un término máximo de diez (10) días hábiles contados a partir de la fecha de su recibo y plena identificación para la cual se le solicitarán los soportes pertinentes dependiendo del tipo de consulta.

Cuando no sea posible atender la consulta dentro de dicho término, se informará al interesado antes del vencimiento de los 10 días hábiles, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer plazo.

Reclamos **EL RESPONSABLE**, garantiza el derecho de reclamo de los titulares incluidos en las bases de datos para la corrección, actualización, supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la Ley 1581 de 2012 y demás normas aplicables. El reclamo será tramitado bajo las siguientes reglas:
Si el reclamo recibido por los canales de atención establecidos no cuenta con información completa que permita darle trámite, esto es, con la identificación del titular con los debidos soportes, la descripción de los hechos que dan lugar al reclamo y la dirección, si el reclamo está incompleto se requerirá al interesado dentro de los cinco (5) días siguientes a su recepción para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.
Una vez radicado el reclamo el término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atenderlo dentro de dicho término se informará al interesado antes del vencimiento del referido plazo los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

Implementación de procedimientos para garantizar el derecho a presentar reclamos.
La solicitud de rectificación, actualización o supresión debe ser presentada a través de los medios habilitados por **EL RESPONSABLE,** debe contener, como mínimo, la siguiente información:
El nombre, domicilio del titular y medio de contacto para recibir la respuesta como teléfono, correo electrónico, dirección de residencia.
Los documentos que acrediten la identidad del titular, de su causahabiente o la de representación.
La descripción clara y precisa de los datos personales respecto de los cuales el titular busca ejercer alguno de los derechos.
En caso dado otros elementos o documentos que faciliten la localización de los datos personales.
Para rectificación y actualización de datos **EL RESPONSABLE,** tiene la obligación de rectificar y actualizar la información del titular que ser incompleta o inexacta, de conformidad con el procedimiento y los términos arriba señalados.
Para supresión de datos el titular tiene derecho en todo momento, a solicitar a **EL RESPONSABLE,** la supresión (eliminación) de los datos personales cuando:
Considere que los mismos no están siendo tratados conforme a los principios, deberes y obligaciones previstas en la Ley 1581 de 2012.
Hayan dejado de ser necesarios o pertinentes para la finalidad para la cual fueron recolectados.
Se haya superado el periodo necesario para el cumplimiento de los fines para los que fueron recolectados.
Esta supresión implica la eliminación total o parcial de la información personal de acuerdo con lo solicitado por el titular en los registros, archivos, bases de datos o tratamientos realizados por **EL RESPONSABLE,** es importante tener en cuenta que el derecho de cancelación no es absoluto y el responsable puede negar el ejercicio de este cuando:
La solicitud de supresión de la información no procederá cuando el titular tenga un deber legal o contractual de permanecer en la base de datos.
La eliminación de datos obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos, la actualización de sanciones administrativas o los requisitos establecidos por los reglamentos de certificación de producto.
Los datos necesarios para proteger los intereses jurídicamente tutelados del titular; para realizar una acción en función del interés público o para cumplir con una obligación legalmente adquirida por el titular.

En caso de resultar procedente la cancelación de los datos personales **EL RESPONSABLE,** debe realizar operativamente la supresión de tal manera que la eliminación no permita la recuperación de la información.

Revocatoria de autorización.
Los titulares de los datos personales pueden revocar la autorización para el tratamiento de los datos personales en cualquier momento, siempre y cuando no lo impida una disposición legal o contractual.

Se tendrán dos modalidades en las que la revocación del consentimiento puede darse. La primera, sobre la totalidad de las finalidades consentidas, esto es, **EL RESPONSABLE,** deba dejar de tratar por completo los datos del titular; La segunda, puede sobre algunos tipos de tratamiento determinados, como por ejemplo para estudios de mercado. Por lo anterior, será necesario que el titular al momento de presentar la solicitud de revocatoria de consentimiento a **EL RESPONSABLE**, para que indique en ésta si la revocación que pretende realizar es total o parcial. En la revocatoria parcial deberá indicar con cuál tratamiento el titular no está conforme.
Habrá casos en que el consentimiento, por su carácter necesario en la relación entre **EL TITULAR DE LOS DATOS** y **EL RESPONSABLE** y por disposición legal no podrá ser revocado.

VIGENCIA

La presente Política para el Tratamiento de Datos Personales rige a partir del 4 de septiembre de 2023. Las bases de datos en las que se registrarán los datos personales tendrán una vigencia igual al tiempo en que se mantenga y utilice la información para las finalidades descritas en esta política.
Una vez se cumpla(n) esa(s) finalidad(es) y siempre que no exista un deber legal o contractual de conservar su información, sus datos serán eliminados de nuestras bases de datos.

5. RESPONSABILIDADES.

La Alta Dirección de SNIDER & CIA S.A.S, asume la responsabilidad de velar por la comunicación a sus colaboradores, la publicación a sus partes interesadas, así como garantizar el cumplimiento, revisión y actualización de esta política.

Los colaboradores y demás partes interesadas son responsables de dar estricto cumplimiento a esta política. El incumplimiento de esta por parte de los colaboradores acarreará sanciones disciplinarias según lo establecido en el reglamento interno de trabajo sin perjuicio de las demás consecuencias legales a que haya lugar.

6. FIRMA

1. ALCANCE:

La presente política se establece en cumplimiento de las leyes antisoborno y anticorrupción vigentes y es de aplicación obligatoria para todos los colaboradores y partes intersadas que interactúan con SNIDER & CIA SAS en el ejercicio de su actividad económica. Todas las actuaciones que se surtan durante el desarrollo del objeto social deben respetar los valores corporativos de SNIDER & CIA SAS y cumplir con los más altos estándares de comportamiento, incluyendo la honestidad y la imparcialidad.

La alta dirección de SNIDER & CIA SAS será responsable de vigilar el cumplimiento de esta política y asegurar que los empleados sean conscientes de esta política y la necesidad de cumplirla.

Los Gerentes de SNIDER & CIA SAS tienen *obligaciones* específicas con respecto a la aplicación de la debida diligencia y la supervisión de terceros conforme a lo dispuesto en esta política.

2. OBJETIVOS:

Definir los lineamientos para que las negociaciones e interacion con terceros y con las entidades publicas, se lleven a cabo con el máximo nivel de integridad requerido para todos los negocios y el cumplimiento de todas las leyes y regulaciones pertinentes. Esta política declara que las prácticas corruptas ante entidades públicas o privadas no son aceptadas, permitidas ni promovidas en SNIDER & CIA SAS.

3. INDICADORES:

- Control de Novedades

4. CONTENIDO

SNIDER & CIA SAS exige el cumplimiento de toda la normatividad de anticorrupción y antisoborno aplicable y vigente en el ejercicio de su actividad. La Empresa aplica los valores de integridad y transparencia promoviéndolos y estableciéndolos como parte de su cultura organizacional, y aplica *"tolerancia cero"* a todo tipo de actividades de corrupción de cualquier naturaleza, ya sea cometida por empleados o por un tercero que actúe en nombre y/o representación de la misma, implementando para ello todo tipo de medidas necesarias para la prevención y mitigación de los factores de riesgo asociados a la corrupción y soborno que se puedan materializar.

SNIDER & CIA SAS ha adoptado el documento de referencia de la Convención de las Naciones Unidas contra la Corrupción (Resolución 58/4 de la Asamblea General del 31 de octubre de 2003); corroborando que la compañía está decidida a evitar la corrupción y a luchar contra ella. En concordancia con lo anteriormente citado, SNIDER & CIA SAS siempre actuará de manera honesta, responsable, transparecente y respetuosa de cara al estado social de derecho.

4.1. Definiciones

Las siguientes definiciones sirven como una guía para algunas de las palabras o frases utilizadas en esta política; sin perjuicio de la definición legal y/o literal que cada una tenga.

- **Corrupción:** conductas encaminadas a que una Empresa se beneficie, o busque un beneficio o interés, o sea usada como medio en, la comisión de delitos contra la administración pública o el patrimonio público o en la comisión de conductas de Soborno Transnacional o Nacional.

- **Soborno:** Se refiere al acto de entregar o prometer indebidamente dinero u otra utilidad a alguien, con el ánimo de obtener un beneficio. Empleados, contratistas y/o asociados de negocio de SNIDER & CIA SAS no deberán hacer, ofrecer para hacer o autorizar cualquier pago indebido; o proporcionar cualquier cosa de valor a cualquier individuo, o a petición de cualquier persona, con el propósito de influir, incluir o recompensar cualquier acto, omisión o decisión para asegurar una ventaja indebida, obtener o retener un negocio.
  En esencia, SNIDER & CIA SAS prohíbe los pagos *quid pro quo* por lo que el pago se realice con la expectativa de recibir a cambio un beneficio o ventaja indebida.
- **Oficial de Asuntos Exteriores:** Cualquier funcionario o empleado de un gobierno o de cualquiera de sus organismos o de una corporación del gobierno, o cualquier persona que actué en calidad oficial para cualquiera de dichas entidades e incluye familiares de dicha persona.
- **Gobierno:** Una agencia, subdivisión u otro organismo de cualquier gobierno nacional, estatal o local, incluyendo hospitales u otros centros de salud que son de propiedad u operados por un gobierno, y que incluye las agencias reguladoras o negocios controlados por el gobierno, corporaciones, empresas o sociedades.
- **Conocer:** Se refiere al acto de tener información sobre algo o alguien. Una compañía o persona tiene conocimiento de la conducta prohibida si la empresa o persona es:
  - (a) Conscientes de que tal persona está participando en dicha conducta, que existe tal circunstancia, o que tal resultado es sustancialmente seguro que ocurra o
  - (b) Tiene la firme creencia de que la existencia de las circunstancias o que tal resultado es sustancialmente seguro que ocurra. Una empresa o persona también se considera que tiene conocimiento de una circunstancia particular, si la empresa es *"consciente de una alta probabilidad de la existencia de tal circunstancia, a menos que la persona realmente cree que tal circunstancia no existe."*
- **Dinero o "cualquier cosa de valor":** Este término incluye, pero no se limita a, dinero en efectivo o equivalentes de efectivo, regalos, servicios, ofertas de empleo, prestamos, gastos de viaje, entretenimiento, contribuciones políticas, donaciones de caridad, subsidios, el patrocinio, honorarios o la prestación de cualquier otro activo, incluso si un valor nominal.
- **Pago:** Este término se refiere e incluye cualquier oferta directa o indirecta para pagar, se compromete a pagar, autorizaciones de pagos o de cualquier cosa de valor.
- **Tercero:** Se refiere a personal ajeno de SNIDER & CIA SAS. Leyes contra la corrupción no siempre de diferencian entre la conducta de la empresa y la conducta de un tercero que actúe en nombre y representación de la empresa. Por lo tanto, es obligación de SNIDER & CIA SAS "*conocer de sus negocios* "; y debe asegurarse que los terceros con y por medio de los cuales lleva a cabo negocios, reconocen y aceptan cumplir con los principios de esta política.

4.2. Para luchar contra la corrupción y el soborno nuestra compañía se compromete a:

- Educar a nuestros empleados sobre la responsabilidad de la compañía para erradicar la corrupción. La justicia e imparcialidad para todos es fundamental para la estabilidad y el crecimiento de un país.
  También ayuda a combatir eficazmente la delincuencia. Esta educación será proporcionada dentro de la compañía y los facilitadores serán los directos y supervisores de la compañía.

- Educar a los empleados acerca de los que significa el comportamiento ético, lo que significa la corrupción y como luchar contra ella, y animarlos a exigir el respeto de sus derechos. Enseñar que esperan vivir en un país sin corrupción es una de las mejores herramientas para asegurar un futuro.

Esta educación será proporcionada dentro de las instalaciones de la compañía y los facilitadores serán los gerentes y supervisores de la compañía.

- Informar de los casos de corrupción. La creación de un entorno en el que el Estado de Derecho prevalece. Cada denuncia de corrupción o soborno se grabará en el control de las no conformidades, y serán tratados de acuerdo con el procedimiento de acciones correctivas de la Compañía.

- Negarse a participar en actividades que no son legales ni transparentes. Aquellos responsables de cada proceso se responsabilizarán de asegurar que la compañía no participe en actividades de esta naturaleza.

- Promover la estabilidad económica asumiendo una actitud de "tolerancia cero" hacia la corrupción. Una comunidad de negocios transparente es la piedra angular de cualquier democracia sólida.
  Si se demuestra que un empleado de la organización ha cometido delitos de corrupción y de soborno se emitirá una no conformidad y se le aplicarán las sanciones disciplinarias correspondientes. En el caso de los terceros, se adeoptarán las medidas comeciales sancionatorias y las penales cuando a ello hubiere lugar.

4.3. Requerimientos para Asociados de Negocio

Contratistas, consultores o proveedores que son nuestros asociados, o que trabajan en nuestro nombre, a través de prestación de servicios, procesos o cualquier actividad comercial, estarán obligados a actuar de manera coherente con esta política cuando actúen en nuestro nombre.

Los contratistas independientes, consultores o proveedores serán informados de esta política que se aplica a nuestros colaboradores en sus relaciones con estos.

4.4. Actividad permitida

Los pagos que se realicen a entidades gubernamentales nacionales, locales o internacionales, se adelantarán bajo los parámetros legales; no se deben utilizar intermediarios o terceras personas para que ellos realicen pagos inapropiados. Los pagos de facilitación (pagos dados a un funcionario o persona de negocios para agilizar un trámite), están prohibidos. Dichos pagos no deben hacerse a funcionarios públicos, ni siquiera si son una práctica común en un país determinado.

En el establecimiento de las relaciones comerciales con terceros, se brindará obsequios de material publicitario no ostentoso, así como invitaciones que no generen gastos excesivos, sólo para efectos de recordación.

4.5. Resolución 58/4 de la Asamblea General en octubre 31 de 2003 (ONU)

SNIDER & CIA SAS ratifica y promulga a la Convención de las Naciones Unidas contra la corrupción. La principal razón de esta decisión es que los países que erradican con éxito la corrupción son mucho más legítimos para sus ciudadanos y crean estabilidad y confianza, y nuestra compañía quiere ser parte de esa generación de confianza y estabilidad de sus partes interesadas.

4.6. Canales de denuncia

SNIDER & CIA SAS cuenta con los siguientes canales de denuncia que permiten que cualquier persona interna o externa informe de manera confidencial y segura acerca de actividades sospechosas relacionadas con el Soborno Nacional y/o Transnacional y cualquier otra práctica corrupta:

Correo electrónico: etica@snider.com.co
Formulario en la página web www.snider.com.co y en la Intranet de Aquí trabajo.

5. RESPONSABILIDADES.

La Alta Dirección de SNIDER & CIA S.A.S, asume la responsabilidad de velar por la comunicación a sus colaboradores, la publicación a sus partes interesadas, así como garantizar el cumplimiento, revisión y actualización de esta política.

Los colaboradores y demás partes interesadas son responsables de dar estricto cumplimiento a esta política. El incumplimiento de esta por parte de los colaboradores, acarreará sanciones disciplinarias según lo establecido en el reglamento interno de trabajo sin perjudicio de las demás consecuencias legales a que haya lugar.

6. FIRMA

1. ALCANCE

La presente política corresponde al cumplimiento de lo establecido en la Resolución 0312 de 2019 y las demás normas vigentes en materia de Seguridad y Salud en el Trabajo. Aplica para **SNIDER & CIA. S.A.S.**

2. OBJETIVO

Establecer el procedimiento para determinar el incumplimiento del colaborador. El contenido de la política es de estricto cumplimiento y cualquier violación de esta será considerada falta grave. Se hace expreso que lo anterior obedece a razones ocupacionales y de servicio al cliente, razones objetivas que son aceptadas por todo trabajador al vincularse laboralmente con la compañía, razón por la cual su incumplimiento además de constituir un acto de grave indisciplina supone objetivamente un riesgo a la seguridad de los trabajadores, así como afecta la imagen de la compañía frente a sus clientes

3. INDICADORES

- Cobertura en el programa de capacitación

4. CONTENIDO

MARCO LEGAL

- **LEY 9 DE 1979: Artículo 84** Todos los empleadores están obligados a adoptar medidas efectivas para proteger y promover la salud de los colaboradores, logrando de esta forma evitar accidentes y enfermedades en los lugares de trabajo.
- **RESOLUCIÓN 1075 DE 1992 - DECRETO 1108 DE 1994:** Los empleadores se encuentran obligados a incluir dentro de las actividades del subprograma de medicina preventiva establecido por la Resolución 1016 de 1989, campañas específicas tendientes a fomentar la prevención del consumo de sustancias psicoactivas (la farmacodependencia, el alcoholismo y el tabaquismo), dirigidas a sus colaboradores.
- **RESOLUCIÓN 000414 DE 2002:** En virtud de la cual se fijan los parámetros científicos y técnicos relacionados con el examen de embriaguez y alcoholemia.
- **RESOLUCIÓN 1956 DE 2008:** Adopta medidas en relación con el consumo de cigarrillo o del tabaco, establece en el artículo 1º que por lugar de trabajo debe entenderse las zonas o áreas utilizadas por las personas durante su empleo o trabajo incluyendo todos los lugares conexos o anexos y vehículo que los colaboradores utilizan en el desempeño de su labor.
- **LEY 1385 DE 2010:** Promueve la prevención del consumo de alcohol de las mujeres en estado de embarazo, con acciones afirmativas de prevención y educación, establece acciones para prevenir el síndrome de alcoholismo fetal en los bebés por el consumo de alcohol de la madre durante la gestación y se dictan otras disposiciones.
- **DECRETO 120 DE 2010:** Mediante el cual se protege al menor de edad y a la comunidad en general de los efectos nocivos del consumo de bebidas alcohólicas y establece medidas tendientes a la reducción del daño y la minimización del riesgo de accidentalidad, violencia cotidiana y criminalidad asociada al consumo inmoderado de alcohol.
- **CIRCULAR 0038 DE 2010:** Expresa las determinaciones e instrucciones pertinentes para que las empresas mantengan espacios libres de humo y de sustancias psicoactivas, las cuales son de obligatorio cumplimiento en los lugares de trabajo anexos y conexos a la organización y recuerda a los empleadores su obligación de cumplir con la ejecución de la Resolución 1016 de 1989, Resolución

1075 de 1992, Resolución 1956 de 2008, incluyendo dentro de las actividades del Subprograma de Medicina Preventiva, campañas específicas de prevención y control de la farmacodependencia, el alcoholismo y el tabaquismo, dirigidas a sus colaboradores.

- **LEY 1566 DE 2012:** Por la cual se dictan normas para garantizar la atención integral a personas que consumen sustancias psicoactivas y se crea el premio nacional "*entidad comprometida con la prevención del consumo, abuso y adicción a sustancias"* psicoactivas.
- **LEY 1548 DE 2012:** Por la cual se modifica la ley 769 de 2002 y la ley 1383 de 2010 en temas de embriaguez y reincidencia y se dictan otras disposiciones".
- **LEY 1696 DE 2013**: por medio de la cual se dictan disposiciones penales y administrativas para sancionar la conducción bajo el influjo del alcohol u otras sustancias psicoactivas
- **RESOLUCION 181 DE 2015:** Por la cual se adopta la Guía para la Medición Indirecta de Alcoholemia a través de Aire Espirado.
- **RESOLUCIÓN 1844 DE 2015**: Por el cual se regula el procedimiento para realizar las pruebas de las pruebas de alcoholemia.

CÓDIGO SUSTANTIVO DEL TRABAJO:

- ***"ARTÍCULO 49.*** *Toda persona tiene el deber de procurar el cuidado integral de su salud y la de su comunidad."*
- ***"ARTÍCULO 60.*** *PROHIBICIONES A LOS COLABORADORES. Se prohíbe a los colaboradores: Presentarse al trabajo en estado de embriaguez o bajo la influencia de narcóticos o drogas enervantes."*
- ***"ARTÍCULO 62****. TERMINACIÓN DEL CONTRATO POR JUSTA CAUSA."*

"A) Por parte del empleador

11. Todo vicio del colaborador que perturbe la disciplina del establecimiento."

CÓDIGO DE PROCESAL DEL TRABAJO

"ARTÍCULO 51. MEDIOS DE PRUEBA: El Juez tiene libertad probatoria y por lo tanto formará libremente su convencimiento, (visto de la alternativa judicial)

- ***"SENTENCIA C-221 de 1994****. Despenalización del consumo de la dosis personal."*
- ***"SENTENCIA No 22779 del 22 de septiembre de 2009****: El incumplimiento de las prohibiciones especiales del colaborador pueden dar por terminado en contrato de trabajo por justa causa."*
- *"Resolución 000181 -27/feb/2015 por la cual se adopta la 'Guía para la Medición Indirecta de Alcoholemia a Través de Aire Espirado'"*
- ***"SENTENCIA No 38381 del 18 de junio de 2014****, Sala Laboral de la Corte Suprema de Justicia. Legitima la facultad de los empleadores para realizar pruebas de alcoholimetría y advierte que es falta grave el que el colaborador se niegue a su práctica."*
- ***"CONCEPTO 202494 de Julio 18 de 2005*** *Ministerio de Protección Social: Por medio del cual, se establece la posibilidad de que el empleador practique pruebas de alcoholemia y narcóticas".*

5. RESPONSABILIDADES.

La Alta Dirección de **SNIDER & CIA. S.A.S** se compromete a promover estilos de vida saludable entre los colaboradores, realizando actividades preventivas en cuanto al consumo, abuso y adicción de bebidas alcohólicas

y sustancias psicoactivas, fortaleciendo valores y hábitos saludables a todos los colaboradores directos, visitantes, terceros, etc., conforme lo dispuesto en la presente política.

La Alta Dirección de la **SNIDER & CIA. S.A.S**, asume la responsabilidad de velar por la comunicación a sus colaboradores, la publicación a sus partes interesadas, así como garantizar el cumplimiento, revisión y actualización de esta política.

Los colaboradores y demás partes interesadas son responsables de dar estricto cumplimiento a esta política. El incumplimiento de esta por parte de los colaboradores acarreará sanciones disciplinarias según lo indicado anteriormente, sin perjuicio de las demás consecuencias legales a que haya lugar

6. FIRMA

1. SCOPE:

SNIDER & CIA S.A.S., specialized in storage of goods under customs control, national merchandise, inventory management and commercial user in free zone, its Senior Management, Process Leaders and Collaborators are committed to support and implement control measures for the prevention, mitigation, correction and/or compensation against their significant environmental impacts and risks, as well as compliance with environmental regulations and other requirements, the allocation of the necessary resources and the strengthening of a sustainable culture, in order prevent pollution generated by the provision of its services and the protection of the environment for future generations, integrating social responsibility as a prevention and control mechanism to avoid labor abuse, discrimination, forced labor, child labor and other human rights violations, continuously improving sustainable performance and demonstrating a balance between the economic, social and environmental pillars.

SNIDER & CIA S.A.S., in fulfillment of the Technical Norm ISO 14001:2015 establishes, implements and maintains its policy of Environmental Sustainability.

2. OBJECTIVES:

For the fulfillment and achievement of the Environmental Management System **SNIDER & CIA S.A.S.** has the following objectives

- Implement control measures to prevent, mitigate, correct and/or compensate significant environmental impacts and risks.
- Allocate financial, human, technological and infrastructure resources necessary for the maintenance of the Environmental Management System.
- Comply with environmental regulations and other requirements applicable to the organization.
- Strengthen the sustainable culture in the organization's collaborators.
- Implement a Corporate Social Responsibility program that promotes inclusion, works with different communities and is framed within the global Sustainable Development agenda.

3. INDICATORS

- Water Consumption
- Energy Consumption
- Generation of Usable Waste
- Carbon Footprint
- Compliance Training Program
- Legal Compliance
- Environmental Performance
- CSR Performance

4. RESPONSIBILITY

The Senior Management of **SNIDER & CIA S.A.S.,** assumes the responsibility of ensuring the dissemination, compliance, revision and updating of this policy whenever necessary.

Collaborators and other stakeholders are responsible for strict compliance with this policy. Failure by the employees to comply with it shall result in disciplinary measures in accordance with the rules of procedure, without prejudice to any other legal consequences.

5. FIRM

1. ALCANCE:

Para todos los colaboradores de AVIOMAR S.A.S Expresos Aéreos y Marítimos, Agencia de Aduanas COLVAN S.A.S Nivel I y SNIDER & CIA S.A.S, cuyo cargo demande el uso de un dispositivo móvil. La organización se compromete a establecer buenas prácticas para la entrega, uso y oportuna reposición de los equipos móviles.

2. OBJETIVOS:

Definir las condiciones para la entrega, el uso, reposición y devolución de dispositivos móviles en la Organización, los cuales serán asignados a los cargos que así lo requieren, de acuerdo con la solicitud del jefe inmediato y/o visto bueno de gerencia.

3. INDICADORES

- Cumplimiento del cronograma de reposición.
- Reporte de novedades en el ERP relacionados con el desempeño de los dispositivos móviles.

4. CONTENIDO

Condiciones generales

El dispositivo móvil constituye una herramienta de trabajo y se utilizará para el intercambio de mensajes, correos electrónicos y llamadas a clientes internos o externos.

Cada dispositivo móvil se entrega con su respectiva tarjeta Simcard, cuyo plan será asumido 100% por la Organización, el cual incluye voz y datos

El uso del dispositivo móvil es para fines netamente laborales, por lo que se recomienda la NO utilización para navegar en redes sociales, (salvo los cargos que tengan expresamente asignada esta actividad) descargar juegos, aplicaciones de uso personal que puedan limitar el acceso a la línea a clientes internos y externos durante la jornada laboral.

El uso adecuado y responsabilidad del dispositivo móvil estará a cargo del colaborador al que le fue asignado, por lo tanto, no está permitido el préstamo de los dispositivos móviles a compañeros de trabajo, ni cualquier otra persona En caso de robo, pérdida o daño del equipo, el colaborador será quien asuma los costos que correspondan.

Proceso de reposición de dispositivos móviles

Se hará la reposición cada 2 años, contados desde el momento de la adquisición de este.

Las especificaciones técnicas de los equipos móviles estarán sujetas a la asignación presupuestal y a las necesidades de la Organización en el momento de la reposición.

Nota: El colaborador al cual se le realice reposición de equipo debe retornar al área administrativa su equipo móvil anterior. La reposición aplicará únicamente a los equipos que ya no tengan normal funcionamiento por causas propias al uso y desgaste, los colaboradores que entreguen equipos que presenten roturas en la pantalla o daños en el display y aun cumpliendo con el tiempo requerido para la reposición, deberán asumir los costos de reposición, dado que estos daños corresponden a una inadecuada manipulación del equipo.

Los colaboradores que se retiren de la Organización por cualquier motivo deberán entregar su dispositivo móvil, Simcard y accesorios al área administrativa.

Seguridad de la información

Está estrictamente prohibido el uso de cámaras o grabadoras móviles para grabar información confidencial relacionada con la Organización.

Está estrictamente prohibido Cargar cualquier material ilegal u obsceno con el uso de la intranet de la compañía.

El equipo móvil no se puede usar en ningún momento para enviar / recibir material ilícito, para acosar a otros, para almacenar información confidencial perteneciente a otra compañía y en general para las actuaciones que atenten contra la legalidad, ética y buenas costumbres sociales.

El equipo móvil debe estar protegido con contraseña, para evitar el acceso de terceros y/o violación de la seguridad de la información allí contenida.

Pérdida o daño de teléfonos móviles

La Organización no se responsabiliza por la pérdida o daño del equipo móvil. Es responsabilidad exclusiva del colaborador mantener el dispositivo en un lugar seguro y en condiciones óptimas. El equipo móvil está bajo la responsabilidad y el riesgo del colaborador que lo tiene asignado.

Los dispositivos móviles proporcionados por la Organización, en caso de robo deben ser reportados dentro de las 24 horas siguientes al jefe inmediato y al área de Gestión Administrativa con el respectivo denuncio ante las autoridades competentes y deberá con sus propios recursos realizar la reposición de este y adicionalmente asumir el costo de reposición de la tarjeta Simcard asignada.

5. RESPONSABILIDADES.

La Alta Dirección de AVIOMAR S.A.S Expresos Aéreos y Marítimos, Agencia de Aduanas COLVAN S.A.S Nivel I y SNIDER & CIA S.A.S, asume la responsabilidad de velar por la comunicación a sus colaboradores, así como garantizar el cumplimiento, revisión y actualización de esta política.

Los colaboradores son responsables de dar estricto cumplimiento a esta política. El incumplimiento de esta por parte de los colaboradores acarreará sanciones disciplinarias según lo establecido en el reglamento interno de trabajo sin perjuicio de las demás consecuencias legales a que haya lugar.

6. FIRMA