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 seguridad 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, Tablet, 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, 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 de otro funcionario, y de la misma manera, ninguno debe dar a conocer su contraseña, a excepción de una reparación o mantenimiento del equipo o servicio asignado y en este caso se entregará única y exclusivamente al funcionario de la mesa de ayuda de Tecnología; 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 (Facebook, YouTube, Instagram, Twitter, Emisoras, Proxy, descargas P2P, torrents entre otros) no está permitido.

- 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 seguridad 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.
    - 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.
    - 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.
- 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 institucional 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 seguridad, 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*".
    - 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 institucional 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 institucional 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 seguridad 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.
    - 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.
- El área de Tecnología de la Información establece en la consola antivirus una regla de control de dispositivos 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, 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 deben resguardar el equipo bajo llave.
- 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.
- El área de seguridad y/o el área de tecnología de la información podrán levantar o recoger los equipos que se encuentren sin guaya, dentro de las instalaciones de Snider & CIA SAS.
- 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.
- 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 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