POLÍTICA DE SEGURIDAD DE LA INFORMACION

1. PRELIMINAR

En la actualidad, las tecnologías de la información se enfrentan a un creciente número de amenazas, lo cual requiere de un esfuerzo constante por adaptarse y gestionar los riesgos introducidos por estas. El presente documento se encuentra enfocado a la debida observancia de la normatividad legal vigente y las buenas prácticas de protección de la información.

SOCIETÁ S.A.S, a través del presente documento, pretende establecer las directrices de seguridad o protección de la información contra cualquier amenaza que se pueda presentar durante el desarrollo de su objeto social, con el fin de garantizar el correcto uso de los documentos almacenados de manera física, electrónica o virtual, la trasmitida por correos o por medios tecnológicos, así como la divulgada de forma oral en conversaciones e interacciones con terceros, por lo tanto, mediante la presente Política de Seguridad de la Información, se disponen las medidas que permiten la protección integra, disponibilidad y confidencialidad del ciclo de vida de la información.

El amparo de la información es para SOCIETÁ S.A.S., una obligación prioritaria que exhorta a todos a velar por el acatamiento de las políticas establecidas en el presente documento.

2. OBJETIVO

Definir los parámetros que SOCIETÁ S.A.S. seguirá para la gestión de la seguridad de la información. Para tal efecto, se presentan los elementos que conforman la política, en consonancia con los principios de integridad, reserva, disponibilidad, legalidad y confiabilidad, con miras a la prevención y a la reducción de riesgos materializados, que puedan impactar la seguridad de la información.

3. ALCANCE

El alcance de la presente Política abarca toda la información de SOCIETÁ S.A.S con independencia de la forma en la que se procese, quién acceda a ella, el medio que la contenga o el lugar en el que se encuentre, ya sea que se trate de información impresa o almacenada electrónicamente.

El contenido de la presente política, es de conocimiento por parte de todos los miembros de la SOCIETÁ S.A.S., por lo cual, es aplicable desde el momento de su publicación debiendo ser cumplida y acatada por los accionistas, empleados, clientes, contratistas, usuarios, beneficiarios y terceros en general que presten sus servicios o tengan algún tipo de vinculación con SOCIETÁ S.A.S., procurando el apropiado y adecuado nivel de protección de los documentos y/o información, debiendo aportar con su participación la adopción de medidas preventivas y correctivas con el objeto de lograr la finalidad de la presente política.

La Política deberá estar disponible en las páginas web de la compañía www.societa.com.co y www.regimensimple.com de forma que sea accesible por todas las personas vinculadas de la sociedad.

4. MARCO LEGAL

- Constitución Política de Colombia 1991: Artículo 15 (Reconoce como Derecho Fundamental el Habeas Data) - Artículo 20 (Libertad de Información)

- Código Penal Colombiano (Decreto 599 de 2000), o Código de Procedimiento Penal (Ley 906 de 2004).

- Ley 527 de 1999, mediante la cual, se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación.

- Ley 1266 de 2007, a través de la cual, se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.

- Ley 1273 de 2009 - Delitos Informáticos - Protección de la información y los datos.

- Ley 1581 de 2012 - Protección de Datos personales.

- Decreto 1377 de 2013 - Reglamenta parcialmente la Ley 1581 de 2012.

- Decreto 1074 de 2015 - Por medio del cuál se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.

5. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACION

SOCIETA S.A.S., propugna adecuadamente por la seguridad de la información a través de controles e inspecciones administrativas, técnicas y jurídicas, de forma tal que se impida a cualquier persona por medio físico, virtual – electrónico, u oral, que no cuente con autorización expresa, para que pueda acceder, distribuir, compartir, conocer, publicar, exportar, operar, modificar o alterar información que se encuentre protegida bajo el principio de confidencialidad, integridad y disponibilidad, evitando incidentes y riesgos que puedan perjudicar a la empresa, trabajadores, clientes, contratistas, beneficiarios y terceros en general.

Lo anterior, con base en la efectiva constitución de una cultura y conciencia de gestión de riesgos respecto de los accionistas, empleados, clientes, contratistas, usuarios y terceros que presten sus servicios o tengan algún tipo de vinculación con la sociedad, implementada mediante la presente Política de Seguridad de la Información.

6. PRINCIPIOS QUE INSPIRAN LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACION

La presente política responde al cumplimiento de la legislación vigente en materia de protección de datos personales en el ámbito de la Seguridad de la Información. Además, SOCIETÁ S.A.S establece los siguientes principios básicos como directrices fundamentales de seguridad de la información que han de tenerse siempre presentes en cualquier actividad relacionada con el tratamiento de información a la que tenga acceso la compañía:

I. **Alcance estratégico:** La seguridad de la información deberá contar con el compromiso y apoyo de todas las áreas de la compañía, de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas para conformar un marco de trabajo completamente coherente y eficaz.

II. **Seguridad integral**: La seguridad de la información se entenderá como un proceso integral constituido por elementos técnicos, humanos, materiales y organizativos, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información deberá considerarse como parte de la operativa habitual, estando presente y aplicándose durante todo el proceso de diseño, desarrollo y mantenimiento de los sistemas de información.

III. **Gestión de riesgos**: El análisis y gestión de riesgos será parte esencial del proceso de seguridad de la información. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que están expuestos y la eficacia y el coste de las medidas de seguridad.

IV. **Proporcionalidad:** El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

V. **Mejora continua:** Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado.

VI. **Seguridad por defecto**: Los sistemas deberán diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

Puesto que la Seguridad de la Información incumbe a todo el personal del SOCIETÁ S.A.S, esta Política deberá ser conocida, comprendida y asumida por todos sus empleados.

Para la consecución de los objetivos de esta Política, SOCIETÁ S.A.S deberá establecer una estrategia preventiva de análisis sobre los riesgos que pudieran afectarle, identificándolos, implantando controles para su mitigación y estableciendo procedimientos regulares para su reevaluación. En el transcurso de este ciclo de mejora continua, SOCIETÁ S.A.S mantendrá la definición tanto del nivel de riesgo residual aceptado (apetito al riesgo) como de sus umbrales de tolerancia.

7. POLÍTICA DE SEGURIDAD DE LAS BASES DE DATOS

La información debe estar bajo la responsabilidad de la sociedad, para evitar cualquier conflicto y reducir oportunidades de acceso, distribución, conocimiento, publicación, exportación, operación y modificación de la información por parte de personal no autorizado.

SOCIETÁ S.A.S mantendrá contacto con profesionales especializados para la protección de la información, con el fin de capacitar a su personal, compartiendo e intercambiando conocimiento óptimo, previniendo de esta manera cualquier incidente o riesgo que pueda surgir. Las labores desarrolladas por la empresa deben estar alineadas a las políticas de seguridad contenidas en el presente manual.

Frente al manejo de la información los servicios en la nube están permitidos; no obstante, se debe cumplir con los acuerdos de confidencialidad, integridad y disponibilidad vigentes. Así mismo, la información que se extraiga de las bases de datos y que pertenezcan a clientes, proveedores, contratistas, beneficiarios o terceros a través de distintos medios removibles, debe permanecer bajo custodia de la sociedad en condiciones de seguridad.

Es menester colocar de presente que la sociedad renovará o actualizará aquellos equipos (servidores, desktop o portátiles, celulares, etc.) que, por sus características técnicas, soporte, software base, han cumplido su vida útil y corresponden a un punto vulnerable de seguridad.

La sociedad ha implementado acciones para evitar la divulgación, publicidad, modificación, retiro o destrucción no autorizada de información almacenada en bases de datos o medios proporcionados por sus clientes, trabajadores, beneficiarios, contratistas y terceros, velando por la disponibilidad y confidencialidad de la información. Es por ello, que cualquier acceso a la información de manera física o virtual – electrónica, deberá ser autorizada por el Representante Legal de la sociedad.

Se realizan procedimientos de mantenimiento en los equipos que poseen información sujeta a protección, de modo que, las bases de datos se encuentren habilitadas y en constante revisión para prevenir cualquier filtración o eliminación que pueda conducir a una posible trasgresión de la presente política de seguridad en la información.

Bajo ninguna eventualidad o solicitud, SOCIETÁ S.A.S., entregará copia de las bases de datos y servidores en dispositivos como discos duros externos, USB, CD, DVD. Salvo previo requerimiento de autoridad judicial, administrativa o entidad del Estado colombiano que así lo solicite, conforme a las causales establecidas en la legislación vigente.

8. PROTECCION DE DATOS Y PRIVACIDAD

Se implementarán los términos, circunstancias y finalidades para las cuales la sociedad, como garante de los datos personales obtenidos mediante los distintos canales de atención, tratará la información de todas las personas que, en algún instante, por cuestiones del objeto social que desarrolla la sociedad, hayan suministrado datos personales.

En caso de comisionar a un tercero el tratamiento de datos personales, SOCIETÁ S.A.S., requerirá al tercero la ejecución de los lineamientos y procedimientos necesarios para la protección y seguridad de los datos personales. Así mismo, tendrá como objetivo la protección de la privacidad de la información personal de sus trabajadores, accionistas, contratistas y terceros en general estableciendo los controles necesarios para preservarla, velando porque dicha información sea utilizada únicamente conforme a las funciones propias de la empresa, y esta no sea revelada, publicada o entregada a funcionarios o terceras partes sin autorización para ello.

Normas generales de privacidad y protección de datos personales en SOCIETÁ S.A.S.:

- Para el tratamiento de datos personales de beneficiarios, trabajadores, clientes, contratistas u otros terceros, se debe obtener la pertinente autorización con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la sociedad.

- La sociedad debe asegurar que únicamente aquellas personas que tengan una necesidad legítima de acuerdo con sus funciones o servicios que presten para la compañía puedan tener acceso a dichos datos.

- Los trabajadores y demás personas que puedan tener acceso legitimo a los datos administrados por la sociedad deben guardar discreción oportuna y reserva absoluta con respecto a la información de SOCIETÁ S.A.S., o de sus clientes, proveedores, contratistas, beneficiarios o terceros de los cuales tengan conocimiento en el ejercicio de sus cargos.

9. POLÍTICA DE SEGURIDAD DE INTERNET

El Internet es un instrumento de trabajo que permite navegar en áreas relacionadas o no con las labores diarias de la empresa, por lo cual, el uso adecuado de este recurso se inspecciona, coteja y monitorea, considerando para todos los casos a partir de las siguientes políticas:

- No está permitido generar, reunir, reproducir, propagar, publicar, ejecutar, escribir o intentar introducir cualquier código de programación diseñado para auto replicarse, perjudicar o dañar el desempeño de cualquier equipo o red de la sociedad.

- SOCIETÁ S.A.S., implementa herramientas para impedir la descarga de software no autorizado y/o malicioso en los equipos de la sociedad, así mismo, controla el acceso a la

información comprendida en portales de almacenamiento dispuestos en internet para prevenir la fuga de información.

- La Entidad permite el acceso a servicio de internet, estableciendo lineamientos que certifiquen la navegación segura y el uso conveniente de la red por parte de los usuarios finales, evitando errores, pérdidas, alteraciones, filtraciones, modificaciones no autorizadas o uso inoportuno de la información en las aplicaciones de la web.

- Se prohíbe la navegación, publicación, envío o adquisición en sitios de contenido sexualmente explícito, discriminatorio, que implique un delito informático o cualquier otro uso que se considere fuera de los límites permitidos, al igual que, cualquier publicación o envío de información confidencial sin la aplicación y autorización previa, cumpliendo con los controles establecidos dentro de la presente política con el fin de salvaguardar la información. Así mismo, se impide la utilización de otros servicios dispuestos a través de Internet que permitan establecer conexiones o intercambios no autorizados por el Representante Legal de SOCIETÁ S.A.S

- Así mismo, se puede inspeccionar, registrar y comunicar las actividades ejecutadas durante la navegación. El uso de Internet no considerado dentro de las restricciones anteriores es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información.

10. POLÍTICA DE SEGURIDAD EN LA NUBE O CLOUD

Dependiendo del modelo de servicio en la nube, se deberán aplicar diferentes medidas de seguridad, tales como:

i. **Infraestructura:** en primer lugar, se deberá asegurar que el Proveedor monitoriza el entorno para detectar cambios no autorizados. Además, se deberán establecer fuertes niveles de autenticación y control de acceso para los administradores y las operaciones que estos realicen. Por último, las instalaciones y/o configuraciones de los elementos comunes deberán estar registrados y conectados con el objetivo de obtener la trazabilidad adecuada.

ii. **Plataforma:** de forma adicional a las medidas indicadas en el modelo de servicio de Infraestructura, el Proveedor del servicio deberá proporcionar mecanismos de seguridad correspondientes al ciclo de vida del software seguro.

11. POLÍTICA DE SEGURIDAD EN EL ACCESO FÍSICO DE LA INFORMACION Y A TRAVÉS DE LA RED

SOCIETÁ S.A.S., mediante el presente numeral define las reglas para asegurar un acceso controlado, lógico, físico y de red, de toda la información sujeta a protección, para lo cual, se implementan los siguientes enunciados:

- El acceso, ingreso, conocimiento y manipulación de carpetas físicas o documentos de información se encuentran bajo la custodia del representante legal, en caso de que se requiera manipular o tener acceso a la información se deberá obtener autorización expresa de este.

- El control de acceso a la Información y documental física y/o virtual dispuesta en la red o en archivo, se realiza aplicando el principio de privilegio obligatorio para la realización de actividades asignadas siempre y cuando se presente autorización por parte del Representante Legal de la empresa. De igual manera, dicho permiso se realiza de acuerdo con los niveles de calificación de la información y perfil del trabajador asignado.

12. POLÍTICA DE USO DE REDES SOCIALES Y MENSAJERÍA

Para asegurar una apropiada protección de la información de todos sus clientes, contratistas, trabajadores, beneficiarios y terceros, en el uso del servicio de mensajería instantánea y de las redes sociales, se implementan las siguientes reglas a seguir:

- La información que sea transmitida o divulgada por cualquier medio de la web, con ocasión del actuar de un trabajador, contratista o colaborador de la sociedad, que sea creado a nombre personal en redes sociales como: Facebook, Twitter, LinkedIn, blogs, YouTube, Instagram, etc., se considera fuera del alcance de la sociedad, y por lo tanto, su integridad, confiabilidad y disponibilidad, junto con los daños y perjuicios que ello pueda llegar a generar, serán de completa responsabilidad de la persona que las haya producido.

- Toda la información publicada en las redes sociales que sea originada por SOCIETÁ S.A.S., debe ser autorizada por el Representante Legal. No se debe utilizar el nombre de empresas, trabajadores, clientes, beneficiarios, contratistas y terceros en las redes sociales, sin su autorización expresa.

- Se tiene prohibida la vinculación de cuentas de correo electrónico personales o comerciales, a las redes sociales que se creen bajo el nombre de la empresa o que posea algún seudónimo de esta.

- No se recomienda la administración de las redes sociales o correos electrónicos de la sociedad en dispositivos móviles personales.

13. CONTROL DE ACCESO A LA INFORMACION

13.1 Requisitos de negocio para el control de acceso

Todos los sistemas de información de SOCIETÁ S.A.S deberán contar con un sistema de control de acceso a los mismos. Así mismo, el control de acceso se enfoca en asegurar el acceso de los usuarios y prevenir el acceso no autorizado a los sistemas de información, incluyendo medidas como la protección mediante contraseñas.

El control de acceso se entenderá desde la perspectiva tanto lógica (enfocado a sistemas de la información) como física. SOCIETÁ S.A.S deberá asumir una serie de requisitos para el control de acceso, que serán, al menos, los siguientes:

• Los usuarios deberán ser únicos y no podrán ser compartidos.

• Se prohibirá el uso de usuarios genéricos. En su defecto, se utilizarán cuentas de usuario asociadas a la identidad nominal de la persona asociada.

13.2 Derechos de acceso

SOCIETÁ S.A.S establece controles de acceso que garantizan que a los usuarios sólo se les otorguen privilegios y derechos necesarios para desempeñar su función.

Los derechos de acceso deberán ser establecidos en función de:

• Control de acceso basado en roles: deberán establecerse perfiles o roles de acceso por aplicación y/o sistemas para poder asignar los mismos a los diferentes usuarios.

• Necesidad de saber: Solo se permitirá el acceso a un recurso cuando exista una necesidad legítima para el desarrollo de la actividad.

• Privilegios mínimos: los permisos otorgados a los usuarios deberán ser los mínimos.

• Segregación de funciones: deberá asegurarse una correcta segregación de funciones para desarrollar y asignar derechos de acceso.

13.3. Control de acceso lógico

Asimismo, ningún usuario deberá poder acceder por sí mismo a un sistema de información controlado sin la aprobación del responsable del propio usuario (o de la persona designada).

14. TRABAJADORES

La sociedad realiza labores para asegurar que sus trabajadores, comprendan y aprehendan sus responsabilidades respecto de los roles asignados, con el fin de reducir el riesgo de hurto, modificación, alteración, acceso no autorizado, fraude, filtraciones o uso inadecuado de la información y de las instalaciones, por lo tanto, se deberán cumplir las siguientes prerrogativas:

Los trabajadores deben dar aprobación a SOCIETÁ S.A.S., para el tratamiento de sus datos personales de acuerdo con la Ley 1581 de 2012, mediante la cual, se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales, encontrándose reflejada en las cláusulas de los contratos firmados.

Se deberá capacitar y sensibilizar a los trabajadores durante la inducción respecto de las políticas de seguridad de la información y política de tratamiento de datos.

Los trabajadores deberán acatar y cumplir de manera férrea las políticas de Seguridad de la Información, contempladas en la presente directiva.

De igual manera, se debe velar por el cumplimiento de la política de seguridad de la información dentro del entorno laboral.

Se debe retirar de manera inmediata cualquier documento enviado a las impresoras que contenga información privada, secreta, sensible o confidencial de algún cliente, proveedor, beneficiario, contratista, trabajador o tercero.

En los puestos de trabajo de los empleados no se deben tener documentos clasificados como privado, sensible, confidencial o secreto.

Los trabajadores de SOCIETÁ S.A.S., son responsables de la debida observancia de esta política de seguridad de acuerdo con el alcance que se define en este documento.

Los documentos electrónicos o físicos que contienen información sensible, secreta, privada o confidencial se guardan en condiciones de seguridad y con acceso restringido, que únicamente estará autorizado por el Representante Legal de la empresa.

Utilizar los sistemas de información, software, carpetas, documentos, equipos (dispositivos móviles, redes, portátiles, impresoras, Internet, equipos de escritorio, herramientas de acceso remoto, aplicaciones, correos electrónicos, teléfonos y faxes, etc.) y el acceso a la red únicamente para los propósitos que lo vinculan.

15. POLÍTICA DE SEGURIDAD EN USO COMPARTIDO DE REDES O CARPETAS VIRTUALES

El uso compartido de redes o carpetas virtuales se encuentran definidas a continuación:

- Se prohíbe a trabajadores de la empresa almacenar, intercambiar o comercializar archivos de audio, video y/o fotografía en cualquier formato (Mp3, Mp4, etc.) para fines o beneficios personales. Asimismo, se impide guardar archivos que no sean de uso exclusivo de la empresa o para efectuar sus funciones.

- El tiempo de conservación de la información no pertinente es de 6 meses, una vez transcurrido este tiempo se realiza depuración de ésta.

- Antes de eliminar cualquier información del recurso compartido o carpetas virtuales, se verificará su importancia y deberá ser autorizada por SOCIETÁ S.A.S, en caso de no tener certeza, se consultará con el titular de la información.

- Solo se puede guardar información que se está trabajando en la red de la empresa y las carpetas virtuales adoptadas para el desarrollo de las funciones. El trabajador que tenga acceso a la red y a las carpetas virtuales deberá reportar al Representante Legal si encuentra información que no es de su área.

- Para el acceso a las carpetas virtuales o redes se deberá tener autorización para tal fin, la cual, será concedida por SOCIETÁ S.A.S, no sin antes evacuar el estudio y análisis de este. Aunado a ello, por ningún motivo se podrá almacenar información clasificada en servicios o portales en la nube públicos, privados o híbridos.

- Para evitar la eliminación de un documento confidencial e importante deberá llevar la denominación de “confidencial” y/o “información de acceso restringido”.

16. GESTION DE INCIDENTES DE SEGURIDAD

Los eventos e incidentes de seguridad que se presenten con la información física y/o virtual, deben ser comunicados y atendidos a tiempo, empleando los procedimientos definidos, con el fin de tomar las acciones correctivas a que haya lugar. Al respecto, es preciso que la sociedad observe las siguientes acciones:

- Se precisan roles y compromisos dentro de la empresa para valorar los riesgos e incidentes con el fin conservar la operación, continuidad y disponibilidad de las labores.

- Los trabajadores de la sociedad, se encuentra obligados a informar a SOCIETÁ SAS, de cualquier situación sospechosa de incidente o riesgo de seguridad informática, electrónica, virtual o física que comprometa la integridad, confidencialidad y disponibilidad de la información.

- Se deben gestionar los eventos de seguridad de la información para detectar e identificar si es necesario o no clasificarlos como incidentes o riesgos de seguridad de la información.

- Se debe llevar un registro detallado de los eventos de incidentes o riesgos de Seguridad de la información, para ser evaluados emitiendo respuesta oportuna, eficiente y adecuada en cada uno de ellos, contemplando los daños que se causaron por el mismo.

- Establecer las lecciones aprendidas que dejan los incidentes o riesgos de seguridad de la información y su gestión para aprender rápidamente, con el fin de mejorar el esqueleto global de la gestión de incidentes y riesgos de seguridad de la información. SOCIETÁ S.A.S., deberá instituir los procedimientos de control precisos para recolectar y salvaguardar la evidencia de las investigaciones que se efectúen durante el análisis de un incidente o riesgo de seguridad de la información.

- Teniendo en cuenta la identificación y priorización de riesgos e incidentes presentados, se deben tramitar en primer lugar los riesgos correspondientes a nivel alto, seguidos del nivel medio y finalizando con los de nivel bajo.

- En caso de cualquier filtración, alteración, modificación, acceso no autorizado, descarga de documentos o información que produzca un incidente o riesgo de seguridad por parte de algún trabajador de la empresa, se deberá realizar el trámite disciplinario respectivo y ejecutar los procedimientos necesarios para subsanar el yerro humano.

17. OPERACIONES QUE POTENCIALMENTE PUEDEN AFECTAR LA SEGURIDAD DE LA INFORMACION

A continuación, se exponen algunas actuaciones que, potencialmente, podrían derivar en la violación de la seguridad de la información establecida por SOCIETÁ S.A.S:

- No reportar los incidentes o riesgos de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.

- Clasificar y registrar de modo impropio toda la información, desconociendo los lineamientos de la presente política de seguridad de la información.

- No almacenar de forma segura la información, así como también, documentos impresos que contengan información privada de clientes, proveedores, contratistas, beneficiarios o terceros.

- No guardar la información digital o virtual, producto del procesamiento de la información perteneciente a la sociedad.

- Abandonar información privada y reservada, en carpetas compartidas o en lugares distintos al servidor de archivo (DRIVE) que posee la sociedad, obviando las medidas de seguridad.

- Dejar las gavetas abiertas o con las llaves puestas en los escritorios. De igual manera, mantener los computadores encendidos en horas no laborables.

- Modificar, alterar o publicar datos personales de las bases de datos de la sociedad sin la debida autorización del Representante Legal.

- Llevar a cabo diligencias fraudulentas, ilegales o intentar acceder sin estar autorizado a la infraestructura de tecnologías de la información que posee SOCIETA S.A.S.

- Ejecutar operaciones tendientes a evitar o transformar los controles establecidos por la sociedad para la protección de la información, conforme lo estable esta política de seguridad.

- Realizar cambios no autorizados en la plataforma tecnológica dispuesta por SOCIETÁ S.A.S.

18. SANCIÓN DEBIDO A LA VULNERACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

La presente política de seguridad de la información será de conocimiento privado, pues tendrán acceso y conocimiento de esta únicamente los trabajadores, clientes, contratistas y terceros que tengan acceso a la información y documental física, electrónica y virtual que posea la sociedad. En caso de violación o desconocimiento de la política se efectuarán las acciones disciplinarias para cada caso en concreto; y, en tratándose de sujetos ajenos a la sociedad se les conminará para que respondan solidariamente por cualquier requerimiento, proceso administrativo o judicial que derive en una sanción afectando los intereses de la sociedad.

Es responsabilidad de todos los empleados de SOCIETÁ S.A.S notificar cualquier evento o situación que pudiera suponer el incumplimiento de alguna de las directrices definidas por la presente Política.

19. ACUERDO DE CONFIDENCIALIDAD.

Todos los trabajadores y contratistas se encuentran obligados a firmar la cláusula y/o acuerdo de confidencialidad que deberá ser parte integral de los contratos laborales y de prestación de servicios, utilizando cláusulas legalmente ejecutables y con la debida observancia de las responsabilidades y labores de los firmantes para evitar la divulgación, supresión, modificación, fraude, uso inadecuado, exportación, operación, publicidad, alteración, hurto, filtración, eliminación y demás acciones atinentes a la información restringida y no autorizada. Este requerimiento y política de seguridad de la información también será aplicable en los casos de contratación temporal o cuando se permita el acceso a información y/o a los recursos a personas externas de la compañía, tales como, clientes, proveedores, beneficiarios y terceros.

Cualquier reclamo, petición o queja respecto del consentimiento frente al tratamiento de datos personales puede ser radicado directamente al correo electrónico info@societa.com.co.

20. AUDITORÍAS DE SEGURIDAD Y GESTIÓN DE VULNERABILIDADES

Se deberá realizar una identificación periódica de vulnerabilidades técnicas de los sistemas de información y aplicaciones empleadas en la organización, de acuerdo a su exposición a dichas vulnerabilidades y adoptando las medidas adecuadas para mitigar el riesgo asociado.

Una vez identificadas las vulnerabilidades, la organización deberá aplicar las medidas correctoras necesarias tan pronto como sea posible. La identificación, gestión y corrección de las vulnerabilidades debe hacerse conforme a un enfoque basado en riesgos, teniendo en cuenta la criticidad y la exposición de los activos.

21. REVISIÓN DE LA POLÍTICA

La presente Política de Seguridad de la Información, será revisada y aprobada anualmente por el representante legal de la sociedad. No obstante, si tuvieran lugar cambios relevantes en la sociedad o se identificaran cambios significativos en el entorno de amenazas y riesgos, ya sean estos de tipo operativo, legal, regulatorio o contractual, se procederá a su revisión siempre que se considere necesario, asegurando así que la Política permanece adaptada en todo momento a la realidad de SOCIETÁ S.A.S.

En los casos que esto ocurra se publicará en las páginas web de la compañía www.societa.com.co y www.regimensimple.com de forma que sea accesible por todas las personas de la sociedad

22. APROBACIÓN IMPLEMENTACIÓN

Esta política de seguridad de la información fue aprobada por la Asamblea de Accionistas de la compañía en la reunión extraordinaria celebrada el 2 de julio de 2024.