MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ DISTRITO CAPITAL
COLOMBIA
2016

Dirección Cra 9 No. 94 A – 32 Oficina 102 Bogotá D.C. / Pbx: 746 23 01 / Móvil: 3212293946
info@splabogados.com - www.splabogados.com

TABLA DE CONTENIDO

1. INTRODUCCIÓN.

Spl Salgado Abogados y Consultores S.A.S., prevé la 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, así como también, la trasmitida por correos o por medios tecnológicos o divulgada de forma oral en conversaciones, por lo tanto, mediante la presente Política de Seguridad de la Información, se disponen las medidas que permitan la protección integra, disponibilidad y confidencialidad que corresponda al ciclo de vida de la información.

El presente Manual de Política de Seguridad de la Información, se encuentra enfocado a la debida observancia de la normatividad legal de Colombia vigente y las buenas prácticas de protección de la información, junto con el modelo de seguridad y privacidad de la información emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones.

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

2. OBJETIVO.

Instituir las políticas en seguridad de la información en Spl Salgado Abogados y Consultores S.A.S., con el fin de presentar de manera diáfana y coherente los elementos que la conforman a todos las personas naturales o jurídicas que tengan relación siquiera sumaria con la firma, propendiendo por el cumplimiento óptimo del principio de integridad, reserva, disponibilidad, legalidad y confiabilidad, previniendo de esta manera cualquier riesgo operacional y estratégico en el manejo de la información.

3. ALCANCE.

Esta política en seguridad de la información es de conocimiento por parte de todos los miembros de la empresa, por lo cual, es aplicable desde el momento de su publicación debiendo ser cumplida y acatada por los directivos, accionistas, empleados, clientes, contratistas, proveedores, usuarios, beneficiarios y terceros que presten sus servicios o tengan algún tipo de vinculación con la firma Spl Salgado Abogados y Consultores 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 del presente manual.

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 23 de 1982 - Propiedad Intelectual - Derechos de Autor.
- 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 1032 de 2006, por el cual, se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- 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 1437 de 2011 - Código de procedimiento administrativo y de lo contencioso administrativo.
- Ley 1581 de 2012 - Protección de Datos personales.
- Decreto 1377 de 2013 - Reglamenta parcialmente la Ley 1581 de 2012.

5. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN – SPL SALGADO ABOGADOS Y CONSULTORES S.A.S.

Spl Salgado Abogados y Consultores S.A.S., comprende la importancia del debido manejo y protección de la información, por lo tanto, propugna adecuadamente por la seguridad de esta 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 sin tener autorización 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, proveedores, contratistas, beneficiarios y terceros.

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

6. POLÍTICA SEGURIDAD DE LA INFORMACIÓN – SPL SALGADO ABOGADOS Y CONSULTORES S.A.S.

6.1 Política de Estructura de Organización.

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

Spl Salgado Abogados y Consultores S.A.S., mantendrá contacto con grupos especializados para la protección de 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 y los servicios en la nube están permitidos, no obstante, se debe cumplir con los acuerdos de confidencialidad, integridad y disponibilidad vigentes. Asimismo, los datos que se extraigan de las bases de datos y que pertenezcan a información de clientes, proveedores, contratistas, beneficiarios o terceros a través de distintos medios removibles deben permanecer bajo custodia en condiciones de seguridad.

Es menester colocar de presente que la firma 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.

6.2 Política de Bases de Datos.

La firma instituye 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, proveedores, 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.

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, Spl Salgado Abogados y Consultores 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.

Frente a la supresión de los datos, involucra la eliminación total o parcial de la información personal de acuerdo con lo peticionado por el titular en los registros, archivos, bases de datos o tratamientos realizados por Spl Salgado Abogados y Consultores S.A.S. El titular de los datos personales tiene derecho en cualquier instante a presentar solicitud ante la empresa para la eliminación de sus datos personales a partir de las siguientes situaciones:

- Cuando prevea que sus datos no están siendo tratados conforme a los principios, deberes y obligaciones previstas en la normatividad vigente.

- Cuando trascurran más de ocho (08) años luego del recaudo de la información.

Se debe precisar que el derecho de supresión no es un derecho absoluto, por lo que, el responsable del tratamiento y la protección de datos correspondiendo a la firma, puede negar el ejercicio cuando:

- La exclusión de datos obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, requerimientos, investigaciones y persecución de delitos o la actualización de sanciones administrativas.

- El titular de los datos posea un deber legal o contractual de permanecer en la base de datos.

- Los datos sean necesarios para resguardar los intereses jurídicamente tutelados del titular y de la firma, con el fin de instaurar acciones en función del interés público o para cumplir con una obligación legalmente adquirida por el Titular.

6.3 Política de Uso de Internet.

Internet es un instrumento de trabajo que concede 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:

- La utilización de internet es exclusiva para actividades relacionadas con las funciones del objeto social de la firma, manteniéndose las restricciones de seguridad establecidas por esta.

- 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 firma.

- Spl Salgado Abogados y Consultores S.A.S., implementa herramientas para impedir la descarga de software no autorizado y/o malicioso en los equipos de la firma, así mismo, controla el acceso a la información comprendida en portales de almacenamiento dispuestos en internet para prevenir la fuga de información.

- Los trabajadores autorizados para el acceso de la información tienen rotundamente restringido el ingreso a redes sociales, sistemas de mensajería instantánea, acceso a sistemas de almacenamiento en la nube y cuentas de correo no institucional. En caso de ser requerido por las funciones del cargo, el Representante Legal de la empresa es la única persona para dar la debida autorización.

- 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.

- Para clientes, visitantes como aliados estratégicos, consultores, freelance y proveedores, contratistas y terceros se habilitará el acceso a la red pública de internet mediante una solicitud vía correo electrónico o verbal dirigida al Representante Legal de la firma. No se permite el uso de los recursos de internet corporativo para la descarga, distribución y/o reproducción de música, videos y similares, siempre y cuando, no tengan relación con las actividades ejecutadas con la empresa.

- 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 Spl Salgado Abogados y Consultores S.A.S.

- Descarga, instalación y manejo de programas de aplicación o software no relacionados con la actividad laboral que desarrolla la firma y que afecte el procesamiento de la estación de trabajo o de la red.

- Navegar en cuentas de correo de carácter personal, es decir, no corporativa o redes sociales, sin una justificación y/o autorización esgrimida por el Representante Legal.

- Emplear cuentas de correo externas no corporativas para la remisión o recepción de información institucional o de clientes, proveedores, contratistas, beneficiarios y terceros, por lo cual, se ejecutará el monitoreo permanente de tiempos de navegación y las páginas visitadas por los trabajadores de la firma, así como de contratistas y demás terceros autorizados.

- 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.

6.4 Política de Seguridad al Acceso físico y red.

Spl Salgado Abogados y Consultores S.A.S., mediante el presente numeral define las reglas para asegurar un acceso controlado, lógico, físico y de red, de toda la información y documental 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 llave y bajo la custodia del Representante Legal de la firma, para lo cual, se deberá tener autorización expresa por este.

- Todo trabajador que circule dentro de las instalaciones de la empresa deberá portar de manera visible el carnet que lo identifica como empleado.

- Para el ingreso de clientes, proveedores, contratistas y terceros visitantes, el trabajador que autorice su ingreso lo acompañará de manera permanente mientras permanezca dentro de las instalaciones de la empresa.

- 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.

- Ningún cliente, proveedor, contratista o tercero tendrá acceso a los computadores de la empresa, así como también de la información o documentos que reposan en archivo, a menos que, sean autorizados por el Representante Legal de la firma. Igualmente, Cualquier usuario interno o externo que requiera acceso remoto a la red de la empresa, deberá estar autorizado por el Director Jurídico de esta.

- Los equipos de contratistas, clientes, proveedores y demás terceros que requieran acceder a las redes de Spl Salgado Abogados y Consultores S.A.S., deben cumplir un procedimiento de sanitización informática antes de otorgarles dicho permiso.

- La sociedad proveerá a los trabajadores las claves concernientes para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados por el Representante Legal, por tanto, las contraseñas son de uso personal e intransferible.

- El cambio de contraseña solo podrá ser solicitado por el trabajador y titular de la cuenta, comunicándolo al Director Jurídico de la firma, el cual, analizará y estudiará dicha petición; en

caso de hallar que efectivamente es necesario un cambio de clave procederá a asignarle una nueva.

- La información, las aplicaciones, los sistemas, los servicios y los equipos (dispositivos móviles, redes, portátiles, impresoras, Internet, equipos de escritorio, herramientas de acceso remoto, aplicaciones, correos electrónicos, teléfonos y faxes, etc.) de los trabajadores, son activos de información que se proporcionan a estos para cumplir con sus respectivas actividades laborales.

6.5 Política de Trabajadores.

La empresa constituye 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 Spl Salgado Abogados y Consultores 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.

- Reportar de manera inmediata al Director Jurídico de la firma, la sospecha u ocurrencia de eventos considerados incidentes de Seguridad de la Información.

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

- Los trabajadores de Spl Salgado Abogados y Consultores 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.

6.6 Política de Gestión de Incidentes y Riesgos.

Para Spl Salgado Abogados y Consultores S.A.S., son de vital importante los eventos e incidentes de seguridad que se presenten con la información o documental física y virtual que reposan en las instalaciones de la firma, pues deben ser comunicados y atendidos a tiempo, empleando los procedimientos definidos, con el fin de tomar pertinentemente las acciones correctivas a que haya lugar:

- 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 al Director Jurídico 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.

- 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.

- Spl Salgado Abogados y Consultores 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.

6.7 Política de Uso Compartido de Redes o Carpetas Virtuales

La directriz del 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 esta.

- Antes de eliminar cualquier información del recurso compartido o carpetas virtuales, se verificará su importancia y deberá ser autorizada por el Director Jurídico de la firma, 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 el Director Jurídico, 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.

- El incumplimiento de esta política atenta y va en contra vía de la seguridad de la información y es sancionado de acuerdo con el procedimiento disciplinario definido.

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

6.8 Política de Seguridad de los Equipos.

Los equipos (dispositivos móviles, redes, portátiles, impresoras, Internet, equipos de escritorio, herramientas de acceso remoto, aplicaciones, correos electrónicos, teléfonos y faxes, etc.) dispuestos por Spl Salgado Abogados y Consultores S.A.S., se encuentran destinados para el desarrollo de su objeto social, motivo por el cual, se implementan los instrumentos necesarios para la protección y seguridad de la información física, electrónica y virtual. Conforme a ello, se esgrimen los siguientes puntos:

- Los equipos que hacen parte del esquema tecnológico de la sociedad, deben estar ubicados y protegidos apropiadamente para prevenir el daño, robo, perdida o acceso no autorizado a los mismos.

- Spl Salgado Abogados y Consultores S.A.S., establece gestiones para evitar la divulgación, propaganda, modificación, retiro, alteración o destrucción no autorizada de la información almacenada en los medios proporcionados por la firma a los trabajadores, velando por la integridad, disponibilidad y confidencialidad de la información.

- Se adoptarán controles oportunos para mantener los equipos apartados de sitios que puedan presentar algún tipo de riesgo o amenaza potencial, tales como: fuego, explosivos, agua, polvo, vibración, interferencia electromagnética, vandalismo, etc.

- Los medios y equipos donde se almacenan, procesan y resguardan información, deben contener las medidas de protección físicas, lógicas y virtuales, que consientan su monitoreo y correcto estado de funcionamiento, para ello, se deben ejecutar los mantenimientos preventivos y correctivos que se requieran.

- Los trabajadores velarán por el uso adecuado de los equipos que les hayan sido designados, debido a ello, dichos equipos no deberán ser prestados a personas ajenas o no autorizadas.

- El servicio de acceso a Internet, cuentas de redes, navegadores, carpetas virtuales, medios de almacenamiento, sistemas de información, aplicaciones (Software) y equipos son propiedad de Spl Salgado Abogados y Consultores S.A.S., debiendo ser usados únicamente para el cumplimiento de la misión de la firma.

- Se precisa que, respecto de la infraestructura utilizada para el procesamiento de la información, las comunicaciones y la seguridad informática, se realicen mantenimientos periódicos a los equipos de la empresa, con el fin de que dichas actividades no se vean afectadas por circunstancias de caducidad. Por lo tanto, se revisará constantemente la vida útil de cada uno de los recursos que componen dicha estructura de acuerdo con la descripción y recomendaciones de sus fabricantes.

- Está restringida para los trabajadores la reproducción o descarga de archivos en medios removibles de almacenamiento, por lo cual, únicamente el Directo Jurídico tendrá la potestad de realizar dicha gestión o autorizar al personal competente.

- Los equipos portátiles deberán estar reforzados con la guaya o el dispositivo que se defina para su protección, sea dentro o fuera de las instalaciones de la sociedad.

6.9 Política de Uso Redes Sociales y Servicios de Mensajería Virtuales.

Spl Salgado Abogados y Consultores S.A.S., define los mecanismos generales para asegurar una apropiada protección de la información de todos sus clientes, proveedores, contratistas, trabajadores, beneficiarios y terceros, en el uso del servicio de mensajería instantánea y de las redes sociales, por tal motivo, 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 firma, 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 Spl Salgado Abogados y Consultores S.A.S., debe ser autorizada por el Representante Legal de esta y con un vocabulario jurídico. No se debe utilizar el nombre de la empresa, trabajadores, clientes, proveedores, beneficiarios, contratistas y terceros en las redes sociales para denigrar o afectar la imagen y reputación de los seguidores cuando manifiestan comentarios en contra de la filosofía de la firma.

- Los trabajadores deberán aplicar complejidad en las contraseñas de las cuentas de la sociedad, obedeciendo los protocolos de seguridad de estas y ejecutando el cambio periódicamente, de acuerdo con el presente manual de políticas de seguridad de la información.

- El equipo de publicidad y marketing de la empresa realiza la verificación y adopción de medidas o controles de seguridad, encaminados a impedir el acceso abusivo a las plataformas virtuales que posee la firma, derivando en la afectación de la imagen y la credibilidad de la sociedad. Este acompañamiento es realizado por el publicista de Spl Salgado Abogados y Consultores S.A.S., quien es el encargado de crear, gestionar todo el tema de mercadeo y publicidad.

- 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 firma en dispositivos móviles personales.

- La información que se comparte usando Microsoft Office 365, como herramienta de red social para conectar o compartir información atinente a las labores diarias de la firma, sólo podrá ser utilizada mediante autorización verbal o escrita por el Director Jurídico de la firma. Esta plataforma es usada también para agendar reuniones.

6.10 Política de Puesto de Trabajo.

Se definen las pautas generales para disminuir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera de la jornada y horario laboral de los trabajadores:

- Los trabajadores, contratistas, personas en comisión, pasantes y terceros que tengan algún vínculo con Spl Salgado Abogados y Consultores S.A.S., deben conservar su escritorio libre de información, propia de la firma o de sus clientes, beneficiarios, proveedores y terceros que pueda ser conocida, copiada o utilizada por personas que no tenga autorización para su uso o conocimiento.

- Los sistemas de información y comunicaciones, así como, las aplicaciones y servicios de red que reposen en los equipos de la empresa deben ser cerrados cuando no se utilicen para el desarrollo de las labores diarias de la empresa. Igualmente, se debe ejecutar el bloqueo de pantalla siempre que el responsable del equipo se encuentre ausente del lugar.

- El personal deberá bloquear su estación cada vez que se retire de su puesto de trabajo y sólo se podrá desbloquear con la contraseña dispuesta para ello.

- No se debe utilizar escáneres, fotocopiadoras, cámaras digitales, equipos de fax y en general equipos tecnológicos que se encuentren inhabilitados o que no pertenezcan a la empresa. Así mismo, los trabajadores deberán retirar de manera inmediata todos los documentos con

información sensible, crítica, confidencial y secreta que envíen a las impresoras y dispositivos de copiado.

- En la pantalla de los computadores o portátiles no debe permanecer ningún acceso directo o archivo, pues esta debe encontrarse completamente despejada.

- En horas no hábiles o cuando el área de trabajo se encuentre sin personal, los medios que contengan información crítica deberán encontrarse protegidos bajo llave restricción electrónica.

- Queda prohibido reutilizar papel que contenga información sensible a cualquier persona que se encuentre dentro de las instalaciones de la firma.

- El personal es responsable por la custodia y las acciones que se realicen a través de los activos informáticos establecidos, por lo tanto, debe estar presente en el sitio de trabajo cuando se ejecute cualquier mantenimiento o actualización de dichos activos.

6.11 Política de Protección de Datos y Privacidad.

En cumplimiento de la de Ley 1581 de 2012, mediante la cual, se dictan disposiciones para la protección de datos personales, Spl Salgado Abogados y Consultores S.A.S., propenderá por la protección de los datos personales de sus beneficiarios, trabajadores, proveedores, clientes, contratistas y demás terceros de los cuales reciba y administre información.

Se implementarán los términos, circunstancias y finalidades para las cuales la firma, 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, Spl Salgado Abogados y Consultores 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, 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 de privacidad y protección de datos personales en Spl Salgado Abogados y Consultores S.A.S.:

- Para el tratamiento de datos personales de beneficiarios, trabajadores, clientes, proveedores, 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 firma.

- La sociedad debe asegurar que únicamente aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.

- Los trabajadores de la firma deben guardar discreción oportuna y reserva absoluta con respecto a la información de Spl Salgado Abogados y Consultores S.A.S., o de sus clientes, proveedores, contratistas, beneficiarios o terceros de los cuales tengan conocimiento en el ejercicio de sus cargos.

- Corresponde a los trabajadores como deber fundamental, corroborar la identidad de todas aquellas personas a quienes se les entrega información por fax, teléfono, correo electrónico o correo certificado, etc.

6.12 Política de Software No Autorizado.

Spl Salgado Abogados y Consultores S.A.S., proporcionará los dispositivos necesarios que garanticen la protección de la información y los recursos tecnológicos que utilice la firma para el desarrollo de su objeto social, adoptando la vigilancia necesaria para evitar la divulgación, modificación o daño permanente producidos por el contagio de un software malicioso. Así mismo, suministrará los procedimientos necesarios para generar cultura de seguridad entre sus trabajadores y contratistas frente a los ataques de software malicioso:

- Todos los recursos informáticos y la infraestructura de procesamiento, comunicaciones y seguridad de la información que posee la firma, deberán estar resguardados mediante herramientas y software de seguridad (antivirus) que prevengan el ingreso de códigos maliciosos a la red interna, así como también, de mecanismos atinentes a revelar, advertir y recuperar posibles fallos presentados por algún código malicioso.

- Los trabajadores, contratistas o aquellas personas que tengan acceso a los recursos tecnológicos de la empresa, no deben cambiar o suprimir la configuración del software de antivirus definida por el área de tecnología; por consiguiente, sólo se podrán efectuar labores de escaneo de virus en los diferentes medios o equipos.

- Las herramientas y demás mecanismos de protección implementados no deberán ser inhabilitados o desinstalados sin autorización del área jurídica y tecnológica, debiendo ser actualizados periódicamente.

- Los trabajadores y contratistas deben asegurarse que, los archivos anexos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, procedan de fuentes acreditadas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos que tiene la empresa.

- Los trabajadores y contratistas que sospechen o descubran algún contagio por software malicioso deben notificar al Representante Legal y al área de tecnología, para que, a través de estos, se tomen las medidas de control pertinente, evitando así, algún incidente o riesgo de seguridad de la información.

- No está permitido escribir, crear, reunir, copiar, irradiar, ejecutar o intentar ingresar cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier equipo o red que posea Spl Salgado Abogados y Consultores S.A.S.

6.13 Política de Copias de Seguridad.

La firma efectuará las medidas necesarias para la generación de copias de respaldo y almacenamiento de su información crítica y reservada, suministrando en los equipos los recursos necesarios para la realización de estas acciones. Todas las áreas de la firma junto con el apoyo de las tecnologías dispuestas para la efectiva copia de seguridad definirán la estrategia a seguir y los periodos de conservación para el respaldo y almacenamiento de la información. Así mismo, Spl Salgado Abogados y Consultores S.A.S., velará porque los medios magnéticos y equipos que contienen información crítica sean resguardados en una ubicación diferente a las instalaciones donde se encuentra dispuestos.

7. OPERACIONES QUE AFECTAN LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

Para la firma es menester la seguridad de la información, por ende, mediante la presente cláusula se presentan las posibles actuaciones que pueden derivar en la violación de la seguridad de la información establecida por Spl Salgado Abogados y Consultores 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 cuando el trabajador se ausenta de su puesto de trabajo o al terminar la jornada laboral, 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 firma.

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

- Permitir que personas ajenas a la firma y sin algún vínculo siquiera sumario, circulen sin acompañamiento, al interior de las instalaciones.

- Almacenar información de la sociedad en computadores personales de los trabajadores.

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

- La suplantación de un trabajador burlando las medidas de seguridad de la información.

- No mantener la confidencialidad de las contraseñas de acceso de los equipos, los recursos tecnológicos o los sistemas de información de la sociedad o consentir que otras personas ajenas accedan con el usuario y clave del titular a éstos.

- Permitir el acceso u otorgar privilegios de acceso a las redes de datos de la empresa a personas no autorizadas.

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

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

- Sustraer de las instalaciones de la sociedad, equipos que contengan información institucional sin la debida autorización otorgada por el Representante Legal.

- Retirar de las instalaciones de la empresa, documentos con información calificada como información reservada o clasificada, y abandonarlos en lugares públicos o de fácil acceso.

- Ceder, enseñar y divulgar información de la firma, calificada como información reservada y clasificada a personas o entidades públicas o privadas no autorizadas por el Director Jurídico.

- Realizar cambios no autorizados en la plataforma tecnológica dispuesta por Spl Salgado Abogados y Consultores S.A.S.

- Acceder, almacenar o distribuir pornografía infantil.

- Instalar programas o software no autorizados en los equipos de cómputo, cuyo uso no esté autorizado por el área de tecnología y el Representante Legal.

- Copiar sin autorización las aplicaciones de software de la sociedad o violar los derechos de autor o acuerdos de licenciamiento.

8. 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, proveedores y terceros que tengan acceso a la información y documental física, electrónica y virtual que posea la firma. 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 firma Spl Salgado Abogados y Consultores S.A.S. Las investigaciones disciplinarias y las respectivas sanciones le corresponden tramitarlas al Gerente de Recursos Humanos de la sociedad.

9. 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 firma, 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 de la firma: info@splabogados.com; el cual, será resuelto de manera clara, precisa y de fondo por parte del Oficial de Protección de Datos.

- Versión Actualizada a quince (15) de enero de 2020. Motivo modernización razón social Spl Salgado Abogados y Consultores S.A.S.