SUPERINTENDENCIA DE SOCIEDADES

DOCUMENTO DE POLITICAS DEL SGI

1. INTRODUCCIÓN.

La Superintendencia de Sociedades para la gestión y organización del SGI y de los requisitos de las normas ISO 9001:2015, ISO 14001:2015 y NTCISO 27001, en las cuales está certificado ha organizado por eficiencia, consolidación y control todas las políticas que surjan en el SGI, en este documento. Esto permite a la organización facilidades de consulta y actualización de la documentación de las políticas del SGI actuales y las nuevas que puedan surgir. Todo ello buscando siempre el mejoramiento continuo de los procesos y el mantenimiento del SGI.

El SGI requiere establecer, preparar, y mantener una serie de documentos (entre los cuales están las políticas de sus sistemas certificados), registros y evidencias que permiten mostrar la trazabilidad de la Organización, el cumplimiento de las políticas, los compromisos con los usuarios, el desarrollo y cumplimiento de los requisitos legales y reglamentarios necesarios de la Entidad para garantizar la prestación de sus servicios.

El presente documento podrá sufrir modificaciones futuras, de acuerdo a las novedades que se registren en la materia que trata, las cuales serán debidamente aprobadas y comunicadas.

2. POLITICAS DEL SISTEMA DE GESTION INTEGRADO.

A continuación, la Superintendencia de Sociedades recopila todas las políticas que el SGI debe divulgar y cumplir como parte de la gestión de los sistemas certificados en la Entidad.

2.1 POLÍTICA DEL SGI

La Superintendencia de Sociedades, con el fin contribuir a la preservación del orden público económico por medio de las funciones de fiscalización gubernamental sobre las sociedades comerciales y ejercer las facultades jurisdiccionales previstas en la ley, tanto en el ámbito de la insolvencia como en el de los conflictos societarios, se compromete con la implementación de un Sistema de Gestión Integrado (SGI) que contempla los siguientes aspectos:

- Establecer relaciones equitativas y justas con los grupos de interés, mediante la determinación y el mantenimiento de mecanismos de comunicación que permitan el contacto con los mismos, en pro del aumento de su satisfacción.
- Preservar la integridad, confidencialidad, disponibilidad y privacidad de los procesos, trámites, servicios, sistemas de información, infraestructura y en general todos los activos de información de la Entidad, a través de una gestión de riesgos efectiva que minimice el impacto de los incidentes que se generen sobre estos activos, para garantizar la continuidad del negocio frente a los incidentes y fortalecer la cultura de seguridad de la información en la Entidad.
- Proporcionar los recursos necesarios para la implementación y el funcionamiento del SGI y el mantenimiento de la infraestructura para el desarrollo de sus actividades.
- Identificar y evaluar los aspectos ambientales de cada una de las actividades que realiza la Entidad, con el objetivo de minimizar los impactos derivados de éstas, por medio de la implementación de los programas de gestión ambiental así como del cumplimiento de los requisitos legales y otros requisitos aplicables a la Entidad.
- Identificar los riesgos ambientales que conlleva la ejecución de los procesos y promover las mejores prácticas de gestión para minimizarlos, **comprometidos con la protección del medio ambiente, incluida la prevención de la contaminación** como clave para reducir la huella ecológica, y no limitado solamente a la Entidad, sino difundiendo estas prácticas a los diversos grupos de interés, con el fin conjunto de la sostenibilidad.
- Velar por el respeto de los derechos humanos y las prácticas de no discriminación.
- Asegurar el desarrollo de las competencias de los funcionarios, para mejorar continuamente la eficacia, eficiencia y efectividad de los procesos.

- Declarar y apoyar las diferentes actividades que sustentan la integridad física y mental de los funcionarios, instaurando como prioritario el cumplimiento de los requisitos legales a nivel ocupacional, la identificación, control y minimización de los factores de riesgos laborales que puedan derivar en incidentes y/o accidentes de trabajo y enfermedades de origen laboral, entendiendo y aceptando que los funcionarios son parte imprescindible en el éxito de los procesos de la Entidad.

Todo esto en el cumplimiento de la normativa vigente, dentro de un marco de ética y transparencia.

2.1.1 Incumplimiento de las Políticas:

Cualquier empleado, contratista y/o tercero que sea encontrado infringiendo las políticas resultará en acciones de tipo disciplinario o contractual, que pueden incluir, más no estar limitadas a:

- Acción de tipo disciplinario según los lineamientos establecidos por el Código Sustantivo del Trabajo, las Cláusulas Especiales que se establezcan con los empleados en sus Contratos Laborales y/o todo aquello que según las leyes colombianas definan como acciones disciplinarias patronales.
- Terminación del contrato o relación laboral (Basadas en las disposiciones emitidas por las leyes colombianas en materia laboral).
- Demanda de tipo civil o penal.

2.2 POLÍTICA DEL SISTEMA DE CONTROL INTERNO

Ámbito de aplicación

El presente documento de Política establece los lineamientos generales mínimos que deben observar los funcionarios de la Superintendencia de Sociedades, con el propósito de contar con un adecuado Sistema de Control Interno –SCI.

Declaración de compromiso

La Superintendencia de Sociedades asume el compromiso de establecer y mantener actualizado un Sistema de Control Interno eficiente y efectivo.

Cada funcionario de la Superintendencia de Sociedades aplicará los criterios definidos en esta Política para construir, mantener y ejercer controles efectivos y eficientes en los procesos y actividades a su cargo para contribuir con el mejoramiento continuo del Sistema de Control Interno.

Marco de actuación

La Superintendencia de Sociedades declara que en el desarrollo de su gestión contará con un Sistema de Control Interno, integrado por el conjunto de planes, métodos, principios, normas, procedimientos, gestión de riesgos y sus controles, sistemas de administración de la información y demás mecanismos de monitoreo, seguimiento, verificación y evaluación adoptados por la Entidad.

Lo anterior, teniendo en cuenta la articulación que debe existir entre el Modelo Integrado de Planeación y Gestión y el Sistema de Control Interno Institucional, el cual es transversal a la gestión y desempeño de la Entidad.

En consecuencia, para la administración de la Entidad el Sistema de Control Interno es considerado un elemento estratégico para asegurar razonablemente el cumplimiento de los objetivos, razón por la cual debe ser aplicado por todos los funcionarios en la gestión de los procesos estratégicos, misionales, de apoyo y de seguimiento y evaluación, que conforman el Sistema de Gestión Integrado de la Entidad.

Los elementos que conforman el Sistema de Control Interno de la Superintendencia de Sociedades y soportan su gestión transversal, en cumplimiento de lo previsto en la Séptima (7ª) Dimensión del Modelo Integrado de Planeación y Gestión (MIPG) y de acuerdo con los 5 componentes del Modelo Estándar de Control Interno - MECI, así:

1. Ambiente de control
2. Evaluación de riesgos
3. Actividades de control
4. Información y comunicación
5. Actividades de monitoreo

Dichos elementos se definen así:

Ambiente de control.

El ambiente o entorno de control es la base de la pirámide de Control Interno, aportando disciplina a la estructura.

En él se apoyan los restantes componentes, por lo que es fundamental para solidificar los cimientos de un eficaz y eficiente Sistema de Control Interno.

Igualmente, marca la pauta del funcionamiento de la Superintendencia de Sociedades e influye en la concientización de sus funcionarios.

Los factores a considerar dentro del entorno de control son:

- La integridad, principios y valores del personal de la Superintendencia de Sociedades;
- La capacidad y competencias de los funcionarios de la Entidad;
- El estilo de dirección y de gestión;
- La manera en que la dirección asigna autoridad y responsabilidad;
- La estructura organizacional vigente; y
- Las políticas y prácticas de personal utilizadas.

Evaluación de riesgos.

La evaluación de riesgos consiste en la identificación y el análisis de los riesgos relevantes para la consecución de los objetivos, y sirve de base para determinar cómo deben ser gestionados.

A su vez, dados los cambios permanentes del entorno, es necesario que la Entidad disponga de mecanismos para identificar y afrontar los riesgos asociados al cambio.

Para la implementación de MIPG, la evaluación del riesgo también se fortalece a partir del desarrollo de otras dimensiones como el direccionamiento estratégico y planeación, la Gestión con valores para resultados y la Gestión del talento humano a través de las siguientes interacciones:

- Direccionamiento Estratégico: El representante legal y la alta dirección deben definir los lineamientos para la administración del riesgo; el equipo directivo debe identificar aquellos riesgos que impidan el logro de su propósito fundamental y las metas estratégicas.

- Política para la Gestión del Riesgo: Esta se constituye en un instrumento de operación para la Entidad, que sea aplicable a todos los procesos, proyectos y programas.

Actividades de control.

Las actividades de control son las políticas, procedimientos, técnicas, prácticas y mecanismos que permiten a la administración de la Entidad, administrar (mitigar) los riesgos identificados durante el proceso de evaluación de riesgos y asegurar que se llevan a cabo los lineamientos establecidos por ella.

Las actividades de control se ejecutan en todos los niveles de la Entidad y en cada una de las etapas de la gestión, partiendo de la elaboración de un mapa de riesgos.

El mapa de riesgos se complementa con la implementación de controles, es decir, de los mecanismos para dar tratamiento a los riesgos y definir y desarrollar las actividades de control que contribuyan a la mitigación de los riesgos hasta niveles aceptables para la consecución de los objetivos estratégicos y de proceso.

Los responsables de los procesos harán uso de los mecanismos definidos de control encaminados a asegurar el cumplimiento de las leyes y las regulaciones, la eficacia y la eficiencia operacional de la Entidad y la corrección oportuna de deficiencias.

Para asegurar que los funcionarios de la Entidad transiten por este camino, a la alta dirección le corresponde hacer seguimiento a la adopción, implementación y aplicación de los controles establecidos, conforme los realizan los responsables de la gestión.

Información y comunicación.

La comunicación de las responsabilidades de cada funcionario de la Entidad se realiza a través de los manuales de funciones, procedimientos e instructivos previstos para tal fin.

En dichos documentos se encuentran contemplados los roles y responsabilidades de cada funcionario, la forma como interactúan, su rol en el Sistema de Control Interno y cómo las actividades individuales están relacionadas en forma articulada con los demás funcionarios.

Se relaciona con la comunicación de la información relevante hacia el interior de la Entidad, para apoyar el funcionamiento del Sistema de Control Interno.
Igualmente, debe haber comunicación con los grupos de valor, sobre los aspectos claves que afectan el funcionamiento del Sistema de Control Interno y proporciona información hacia las partes externas en respuesta a las necesidades y expectativas.

Actividades de monitoreo.

El Sistema de Control Interno requiere de una adecuada supervisión, es decir, un proceso de verificación independiente que evalúe la consistencia de su funcionamiento a lo largo del tiempo.

Lo anterior se logra a través de actividades de seguimiento continuo, autoevaluaciones y evaluaciones independientes periódicas que realiza la Oficina de Control Interno. Estas evaluaciones permiten determinar si se han definido, puesto en marcha y aplicado los controles establecidos por la Entidad de manera efectiva.

La Oficina de Control Interno debe evaluar y comunicar las deficiencias identificadas en los procesos de forma oportuna a las partes responsables de aplicar medidas correctivas.

La evaluación continua por parte de la Oficina de Control Interno y la autoevaluación de cada líder de proceso permiten el monitoreo a la operación de la Entidad a través de la medición de los resultados generados en cada proceso, procedimiento, proyecto, plan o programa, teniendo en cuenta los indicadores de gestión, el manejo de los riesgos, los planes de mejoramiento, entre otros.

Es importante la autoevaluación de los funcionarios que dirigen y ejecutan los procesos, programas y/o proyectos según el grado de responsabilidad y autoridad para su operación.

3. POLÍTICA DE RIESGOS

3.1 OBJETIVO DE LA POLÍTICA

Orientar la toma de decisiones oportunas y minimizar efectos adversos en la Superintendencia de Sociedades, con el fin de dar continuidad a la función administrativa, asegurar el cumplimiento de la misión institucional y satisfacer las necesidades de los grupos de interés.

3.2 ALCANCE DE LA POLÍTICA

La política de riesgos es aplicable a todos procesos y proyectos de la Entidad y a todas las acciones ejecutadas por los funcionarios durante el ejercicio de sus funciones. Incluye los riesgos de seguridad de la información y de corrupción.

3.3 POLÍTICA DE RIESGOS

La Superintendencia de Sociedades declara que en el desarrollo de sus actividades existen riesgos, por lo cual se compromete a adoptar los mecanismos y acciones para prevención, administración y minimización e involucrar y comprometer a todos los funcionarios en la búsqueda de acciones encaminadas a prevenir, administrar y controlar los riesgos, para cuyo efecto debe darles a conocer el mapa de riesgos institucional de acuerdo a los procesos, el cual debe ser revisado con regularidad por los líderes de los mismos.

Adicionalmente se deben observar los siguientes lineamientos:

- La entidad establecerá los métodos y diseñará las herramientas que apoyen la identificación, análisis, valoración, tratamiento, comunicación y monitoreo de los riesgos.
- Los riesgos deben gestionarse bajo metodología expedida por el Departamento administrativo de la Función Pública y adoptada por la Entidad en el Sistema de Gestión Integral de la Entidad.
- los riesgos deben estar identificados por procesos e Intendencia Regional.
- Cuando se trate de los riesgos de procesos y de corrupción y su calificación inherente esté en los rangos moderados o bajo, debe realizarse la evaluación de los controles desde la auditoría interna.

- La Oficina Asesora de Planeación lidera y acompaña a los procesos e Intendencias Regionales en la identificación y definición de riesgos y controles.
- Los líderes de los diferentes procesos e Intendentes Regionales realizarán el monitoreo y evaluación de la gestión del riesgo y estado de los controles.
- La Oficina de Control Interno evalúa la efectividad del mapa de riesgos de los procesos e Intendencias Regionales y la gestión de los controles de los mismos a través de las auditorías internas.
- Se deben realizar revisiones a los riesgos y controles de los procesos e Intendencias Regionales a intervalos planificados, con el fin de mantener actualizado el mapa de riesgos, en la medida que cambie el contexto.
- Los cambios que se produzcan en la gestión de riesgos se comunicarán a todos los interesados de manera oportuna y conforme al Plan de Comunicaciones Institucional.

4. POLÍTICA DE GESTIÓN DOCUMENTAL

La Superintendencia de Sociedades implementará las mejores prácticas para la correcta gestión de sus documentos e información, los cuales son elementos fundamentales para el desarrollo de su misión y visión institucional.

La ejecución de la política de gestión documental estará a cargo del Grupo de Gestión Documental, bajo el liderazgo de la Secretaría General y de la Subdirección Administrativa, en el marco de sus niveles de competencia.

De esta manera, los funcionarios del grupo de Gestión Documental, en el desarrollo de sus actividades, se comprometen a incorporar y mantener actualizado el programa de gestión documental, mediante capacitaciones programadas junto con el área de Gestión del Talento Humano. Asimismo, a realizar la planeación de su gestión documental y la incorporación de nuevas tecnologías de la información y la comunicación para la eficiencia de los procesos.

4.1 PRINCIPIOS DE LA POLÍTICA DE GESTIÓN DOCUMENTAL

Los siguientes son los principios que adopta la Superintendencia de Sociedades para orientar la política de gestión documental:

Transparencia: Los documentos e información generada por la Entidad deben estar disponibles para el ejercicio del control ciudadano.

Orientación al ciudadano: Todas las actividades generadas para el desarrollo de la política estarán orientadas a que los documentos sean fuente de información para los grupos de interés.

Modernización: Se utilizarán las tecnologías de la información y las comunicaciones para el desarrollo de los procesos de la Gestión Documental Institucional.

Eficiencia: Sólo se producirán los documentos necesarios para el cumplimiento de los objetivos, funciones y procesos de acuerdo con los lineamientos del Sistema de Gestión Integral.

Protección del medio ambiente: Con la adopción de los lineamientos establecidos dentro de la política *Cero Papel*, para la reducción del consumo de papel, siempre y cuando por razones de orden legal y de conservación histórica sea permitido.

Cultura archivística: Se adelantará la sensibilización de los funcionarios y contratistas respecto de la importancia y el valor de la información, los documentos y los archivos de la institución.

4.2 LINEAMIENTOS GENERALES DE LA POLÍTICA

Gestión de la Información: Se adoptarán modelos para la información física y electrónica de acuerdo con las disposiciones del Archivo General de la Nación, el Ministerio de Tecnologías de la Información y las Comunicaciones, y/o el Instituto Colombiano de Normas Técnicas y Certificación - ICONTEC.

Metodología General: Se analizará, identificará y aplicará las mejores prácticas en la creación, uso, mantenimiento, retención, acceso y preservación de la información, independiente de su soporte y medio de creación.

Programa de Gestión Documental: Se diseñará e implementará el Programa de Gestión Documental, el cual estará soportado en diagnósticos, cronogramas de implementación y recursos presupuestales. Este programa será una herramienta de planificación estratégica para el manejo documental.

Articulación y coordinación: Se fomentará la articulación y cooperación permanente entre las áreas responsables de la gestión documental con la alineación a los demás programas del sistema de gestión integral, con el fin de mejorar y complementar la gestión documental.

5. POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Las siguientes políticas de seguridad de la información aplican para el control de la misma sobre el alcance definido por la Superintendencia de Sociedades, las cuales son de obligatorio cumplimiento, por parte de los funcionarios, auxiliares de la justicia, contratistas y toda aquella persona que haga uso de la información de la Entidad, exigido por el Sistema de Gestión Integrado.

5.1 POLÍTICA DE ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN

Las directivas de la Superintendencia de Sociedades garantizan que las responsabilidades para la gestión de la seguridad de los activos de información están claramente asignadas en todos los niveles organizacionales.

Se apoya en el Grupo de Arquitectura de Negocio y del Sistema de Gestión Integrado, quien a su vez se soporta en recursos internos y externos con el objetivo de direccionar y hacer cumplir los lineamientos, así como revisar las incidencias y acciones a tomar para mantener la seguridad de la información en niveles adecuados.

El detalle de las funciones y responsabilidades se encuentran documentados en el **MODELO DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN** contenido en el Documento de Modelos del SGI.

Todos los funcionarios, contratistas y personas externas con acceso a los activos de información de la Organización deben cumplir con las políticas de SEGURIDAD DE LA INFORMACION.

La Superintendencia de sociedades tendrá contacto, comunicación y participación con grupos de interés específicos y autoridades especializadas y relacionadas con la seguridad de la Información para intercambiar experiencias, participar en grupos de trabajo y mejorar procedimientos.

Todos los proyectos donde exista procesamiento de datos e información, deben contemplar controles desde el inicio del mismo hasta su implementación.

5.2 POLITICA DE CUMPLIMIENTO DE DERECHOS DE PROPIEDAD INTELECTUAL

La Superintendencia de Sociedades utilizará herramientas, componentes y software debidamente licenciado y velará por que no se violen los derechos de propiedad intelectual.

Todos los funcionarios de La Superintendencia de Sociedades deberán respetar los derechos de propiedad intelectual sobre sistemas, aplicativos e información de propiedad de La Superintendencia de Sociedades, de sus usuarios, proveedores, contratistas y terceros conservando la confidencialidad e integridad necesarias según sea el caso.

La información y aplicativos o sistemas desarrollados en La Superintendencia de Sociedades, son propiedad de la misma aunque hayan sido generados por alguno de sus funcionarios, contratistas, proveedores o terceros en desarrollo de su labor, salvo que contractualmente esté establecido la propiedad de un tercero, llámese funcionario, proveedor o contratista de La Superintendencia de Sociedades.

Los funcionarios de La Superintendencia de Sociedades no podrán duplicar, convertir en otro formato, ni extraer información de grabaciones (películas, audio) diferentes a los permitidos por la ley de derechos de autor. Tampoco podrán copiar total ni parcialmente libros, artículos, informes, ni otros documentos diferentes a los permitidos por la misma ley.

Todo lo anterior según lo contempla la cláusula de seguridad de la información firmada al momento de la contratación.

5.3 POLITICA DE RESPALDO DE LA INFORMACIÓN

La Superintendencia de Sociedades asegurará la protección de la información crítica y sensible, realizando copias de respaldo de la información propia y de sus usuarios necesarias para el cumplimiento de sus funciones.

Dicha protección debe cumplir con los requerimientos del **MODELO DE RESPALDO DE INFORMACIÓN** contenido en el Documento de Modelos del SGI.

5.4 POLITICA DE ESCRITORIO DESPEJADO Y PANTALLA LIMPIA

Todos los funcionarios de la Superintendencia de Sociedades deberán mantener la información objeto de su labor debidamente custodiada y salvaguardada del acceso de personas no autorizadas, según la clasificación de los activos de información.

Los puestos de trabajo físicamente deberán permanecer organizados y la información no pública – confidencial (de la Entidad o de los Usuarios) que reposa en ellos, deberá guardarse bajo llave en cajoneras y/o en lugares vigilados mientras el funcionario responsable de la misma no esté utilizando dicha información.

En cuanto a la información que se maneja en los equipos de cómputo (de la Entidad o de los Usuarios), todo usuario dentro de la Superintendencia de Sociedades deberá conservar la pantalla libre de accesos directos a información no pública (confidencial) de los funcionarios o de la compañía; para efectos de control de acceso a equipos de cómputo en tiempos de ausencia de funcionarios de su puesto de trabajo, se deberá realizar el bloqueo de la sesión, a través de las teclas (Ctrl + Alt + Supr ó Tecla Windows + L).

5.5 POLÍTICA DE CONTROL DE ACCESO A LOS SISTEMAS

Los requerimientos de control de acceso a nivel físico, nivel de red, sistema operativo y aplicaciones se establecerán según el **MODELO DE CONTROL DE ACCESO A LOS SISTEMAS** contenido en el Documento de Modelos del SGI; los controles deben estar soportados por una cultura de seguridad en La Superintendencia de Sociedades y limitar el acceso de los usuarios hacia los activos de información (Radicador, STORM, ESTONE, KACTUS, SIGS, Correo, Bases de datos, Switch, Firewall, entre otros) al mínimo requerido para la realización de su trabajo, de acuerdo con el tratamiento correspondiente al nivel de

clasificación de cada activo. Además, deben permitir identificar de manera inequívoca cada usuario y mantener trazabilidad de las actividades que éste realiza.

Los usuarios de los activos de información son responsables de realizar un adecuado uso de los mismos, dentro de los cuales se encuentra el uso de sus cuentas de usuario y toda actividad realizada con ellas.

5.6 POLITICA DE SEGURIDAD DEL TALENTO HUMANO

Todo el talento humano de la Organización de la Superintendencia de Sociedades, empleados, contratistas y proveedores deben cumplir las Políticas de Seguridad de la Información, al igual que, conocer y firmar el Acuerdo de Confidencialidad de Información.

Cualquier incumplimiento a las políticas de seguridad de la información, serán sancionados según lo estipulado en la **POLÍTICA DEL SISTEMA DE GESTION INTEGRADO**.

Es responsabilidad del Grupo de Desarrollo del Talento Humano incluir en los programas de inducción y capacitación, la sensibilización en Seguridad de la Información. También debe tener en cuenta:

- **Antes de la contratación:** Realizar las verificaciones de los antecedentes de todos los candidatos a un empleo y se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.

  Se debe incluir en los procesos de nombramiento la firma y aceptación del **GTH-F-026 Formato Acuerdo Confidencialidad**

- **Durante la ejecución del contrato:** Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo, mediante programas de inducción y capacitación en Seguridad de la Información. Si un individuo es contratado para un rol de seguridad de la información específico, la entidad debe asegurar que el nuevo

funcionario tenga la competencia necesaria para desempeñar el cargo o de lo contrario debe asegurar su preparación.

- **Terminación o cambio de contrato:** Las responsabilidades y deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de contrato se definen, comunican al empleado o contratista y se deben hacer cumplir. Esto incluye:

  - La devolución de los activos informáticos (incluida la información confidencial).
  - La deshabilitación de los usuarios, roles y perfiles.
  - La habilitación de nuevos roles y perfiles, en caso de cambio de cargo.
  - Modificación y comunicación de las funciones

Por otro lado, los responsables de los contratos con externos y/o proveedores deben realizar la difusión de las Políticas de Seguridad de la Información Corporativas en apoyo con la Seguridad de la Información de la Organización e incluir en los contratos el **Anexo De Seguridad De Información Para Contratos Con Proveedores**.

5.7 POLITICA DE RESPONSABILIDAD POR LOS ACTIVOS

Se debe definir y realizar un inventario de los activos de información de Supersociedades y asignar a cada activo un responsable para que se encargue de protegerlos adecuadamente.

Los empleados y usuarios de partes externas que usan activos de la organización o tienen acceso a ellos deberían tomar conciencia de los requisitos de seguridad de la información de los activos de la organización asociados con información y con instalaciones y recursos de procesamiento de información. Deberían ser responsables del uso que hacen de cualquier recurso de procesamiento de la información, y de cualquier uso ejecutado bajo su responsabilidad.

En los contratos de trabajo con empleados, contratistas y terceros o acuerdos comerciales donde se tramiten activos de información debe quedar en claro que al terminar estos, la información se debe retornar a la superintendencia de Sociedades.

Para efecto especificar la responsabilidad de los activos esta política se relaciona con el **MODELO DE RESPONSABILIDAD POR LOS ACTIVOS** contenido en el Documento de Modelos del SGI.

5.8 POLITICA DE MANEJO DE MEDIOS

La información puede estar en diferente medio (digital, físico o papel, imagen, etc) el objetivo de la presente política es evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada en estos medios.

En la superintendencia de sociedades se deben desarrollar procedimientos para la gestión de medios en cualquier formato que se posea, para su transferencia o intercambio y para su disposición final, acorde con la clasificación de la información contenida en ellos.

Esta política se relaciona con el **MODELO DE MANEJO DE MEDIOS** contenido en el Documento de Modelos del SGI.

5.9 POLITICA DE SEGURIDAD FISICA

Toda área donde se procesa información de la Superintendencia de Sociedades, debe cumplir con todos los controles definidos de Seguridad Física **(MANUAL DE MANEJO Y CONTROL ADMINISTRATIVO DE BIENES, INSTRUCTIVO: INGRESO INSTALACIONES)**, con el fin de evitar el acceso por personas no autorizadas, daño e interferencia a los recursos e infraestructura de información de la Superintendencia de Sociedades.

5.10 POLÍTICA DE TRABAJO REMOTO Y DISPOSITIVOS MOVILES

El Trabajo Remoto que implique el acceso a la plataforma tecnológica de servicios no publicados hacia redes externas o que impliquen la administración remota de la plataforma, deberá ser aprobado por el oficial de seguridad de la información o quien haga sus veces, previa justificación del jefe superior inmediato y solicitud a través del formato **Trámite 46001 Autorización Servicios Informáticos para Usuarios.**

No se permite la instalación o uso de software que permita tomar control o establecer conexiones desde redes externas no pertenecientes a la Superintendencia de Sociedades a cualquier elemento de la plataforma tecnológica.

Se debe garantizar la seguridad de acceso, la transmisión de datos, el soporte técnico en el punto de trabajo y los dispositivos o equipos desde los cuales se hace conexión.

Para el uso de dispositivos móviles desde los cuales se pueda acceder a la plataforma tecnológica de Supersociedades hay que gestionar los riesgos que genera este tipo acceso de tal manera que no se comprometa la información del negocio.

Para efecto de realizar TELETRABAJO y su requerimiento de acceso remoto, las exigencias de control se establecerán según el **MODELO DE TELETRABAJO Y DISPOSITIVOS MOVILES** contenido en el Documento de Modelos del SGI.

5.11 POLÍTICA DE USO ADECUADO DE LOS RECURSOS

Las personas tendrán a su disposición el uso de recursos tecnológicos de acuerdo a las funciones laborales que así lo requieran.

Dichas personas antes de usar los recursos aceptan y se acogen al cumplimiento de las Políticas de Seguridad de la Información incluyendo las siguientes normas:

Reglas Generales

- Si para el uso del recurso se requiere un usuario y una contraseña
  - Se debe cumplir la **POLÍTICA DE USO DE CONTRASEÑAS**.
  - Se hace responsable de cualquier violación a las Políticas de Seguridad de la Información realizadas con su usuario y acepta las sanciones estipuladas en éstas.
- No se permite el uso compartido de usuarios y contraseñas.
- Los recursos deben usarse estrictamente para fines laborales y nunca deben transmitir, procesar y/o almacenar información personal.
- No se permite transmitir, almacenar y/o procesar información que atente contra propiedad intelectual o derechos de autor.
- Se prohíbe la transmisión, almacenamiento y/o procesamiento de SPAM, pornografía y pornografía infantil.
- Se prohíbe el uso de software ilegal.
- Todo intercambio realizado con los recursos debe acoger a la **POLÍTICA DE INTERCAMBIO DE INFORMACIÓN.**
- Los recursos pueden ser accedidos y su uso monitoreado por cualquier organismo de control o control interno de la Entidad, sin incurrir en violación de la privacidad. Verificar el alcance del acceso y monitoreo, teniendo en cuenta que se puede incurrir en el derecho de privacidad de las personas

Correo Electrónico

- Se prohíbe el uso del correo electrónico para el envío de masivos, cadena de correos que contengan información de carácter personal, comercial, social y demás distintas a las generadas en el estricto cumplimiento de las funciones asignadas al cargo que desempeña en la planta de personal de la Entidad
- Se prohíbe usar el correo electrónico como un sitio de almacenamiento de documentos de propiedad de la Superintendencia de Sociedades. Se recomienda almacenarlos en un sitio adecuado según su nivel de clasificación.
- Cada usuario es responsable de la información contenida en las comunicaciones generadas desde su cuenta de correo electrónico.

Red e Internet

- El usuario debe cumplir con los accesos autorizados y definidos en la **POLÍTICA DE CONTROL DE ACCESO A LOS SISTEMAS.**

Portátiles y Equipos de Escritorio

- Los usuarios no podrán conectar a la red productiva de La Superintendencia de Sociedades portátiles y/o equipos de escritorio personales.
- Cada usuario es responsable de respaldar la información personal que almacene en sus equipos de trabajo
- Los usuarios deben bloquear la sesión de sus equipos de trabajo cuando no estén en uso.
- La conexión de dispositivos de almacenamiento externos debe ser solicitado a través del **trámite 46001 Autorización Servicios Informáticos para Usuarios** al grupo de sistemas y arquitectura de tecnología quien aprobara de acuerdo con las políticas establecidas y reportara al oficial de seguridad de la información o quien haga sus veces, para validación, lo anterior con previa justificación del jefe superior inmediato.

USB y Medios de Almacenamiento

En la Superintendencia de Sociedades el uso de cualquier medio de almacenamiento (USB, Discos Externos) se realizará bajo la responsabilidad de los Funcionarios, los cuales serán responsables por la materialización y remediación de fuga de información a través de estos medios, igualmente están obligados a:

- Vacunar el dispositivo cada vez que lo usen.
- Informar a la mesa de ayuda frente a cualquier incidente de seguridad que se presente con el uso del dispositivo, tales como eventos de virus, malware, spyware o cualquier código malicioso detectado, al igual que en el evento de pérdida o robo de estos dispositivos de almacenamiento.

Uso de equipos Portátiles para visitas, diligencias judiciales o trabajos temporales

Todo equipo portátil que se requiera para llevar a cabo visitas, diligencias judiciales o trabajos temporales deberá ser solicitado a la Dirección de Informática y Desarrollo, quien se encargara de suministrarlo al funcionario solicitante, para lo cual debe garantizar lo siguiente:

1. El equipo debe ser entregado al solicitante sin información (utilizando borrado seguro)
2. El equipo no debe tener privilegios de administrador
3. El equipo debe ir con los programas básicos (office)
4. El equipo deberá iniciar sesión con la solicitud de usuario y contraseña

El funcionario a quien le sea asignado el equipo portátil, es el responsable por la custodia de la información contenida en el mismo, por la materialización y remediación de los riesgos derivados de la pérdida o fuga de información durante el traslado del sitio de la visita o diligencia hasta la Entidad.

5.12 POLÍTICA DE USO DE LOS SERVICIOS DE RED

Los funcionarios de la Superintendencia de Sociedades sólo tendrán acceso a los servicios de red para cuyo uso estén específicamente autorizados.

La autorización para el acceso a la red y para el uso de los servicios de red de la Superintendencia de Sociedades, será solicitada por el jefe inmediato a través del **trámite 46001 Autorización Servicios Informáticos para Usuarios** al grupo de sistemas y arquitectura de tecnología quien aprobará de acuerdo con las políticas establecidas y reportará al oficial de seguridad de la información o quien haga sus veces, para validación.

La Dirección de Informática y Desarrollo de la Superintendencia de Sociedades implementará los controles de Seguridad Lógica necesarios para proteger el acceso a las conexiones y servicios de red.

Adicionalmente se debe tener en cuenta el cumplimiento de las Normas Generales para el uso de Internet relacionadas en la **POLÍTICA PARA EL USO DE INTERNET.**

5.13 POLÍTICA PARA EL USO DE INTERNET

El acceso a Internet dentro de La Superintendencia de Sociedades estará limitado exclusivamente a aquellos usuarios que por su labor requieran la conexión. Estos usuarios serán responsables del buen uso que den a este acceso**.**
La organización se reserva el derecho de monitorear el acceso y uso del Internet, para tomar las acciones disciplinarias y legales correspondientes.

Normas Generales para el uso de Internet

- Es responsabilidad del usuario autorizado para ingresar a Internet, el buen uso que haga de dichos accesos y la fuga o pérdida de información que se pueda presentar por su utilización indebida.
- El acceso al Internet es una herramienta valiosa y limitada que deberá ser usada con racionalidad. Su mal uso va en detrimento de la calidad del servicio.
- Desde el equipo asignado será posible hacer uso de la red Internet, únicamente para fines laborales y de forma consistente con las funciones laborales del empleado.
- El uso de comunicación interactiva y/o redes sociales está completamente prohibido para actividades no relacionadas con el desarrollo de sus funciones.
- No se permite el uso de sistemas de búsqueda y/o descarga y/o instalación de archivos de audio, videos, imágenes o software. Sólo los funcionarios de la Dirección de Informática y Desarrollo podrán descargar software legal o libre necesario para el desarrollo de su labor.

5.14 POLITICA DE USO DE CONTRASEÑAS

Los empleados, contratistas y cualquier otro usuario serán responsables de no comprometer la seguridad de la Información de La Superintendencia de Sociedades a través de uso de contraseñas débiles, u omitiendo alguna recomendación del **MODELO DE CONTRASEÑAS** contenido en el Documento de Modelos del SGI.

Cualquier tipo de acceso que requiera autenticación debe utilizar una contraseña fuerte y debe ser cambiada periódicamente (hay configuración automática para la exigencia de cambio de contraseña) (debería ser por lo menos cada 60 días) mínimo 2 veces al año), la cual debe cumplir el **MODELO DE CONTRASEÑAS** contenido en el Documento de Modelos del SGI.

Los sistemas o software desarrollado por La Superintendencia de Sociedades o por terceros que requieran uso y almacenamiento de contraseñas, deben utilizar algoritmos de cifrado según la **POLÍTICA DE USO DE CONTROLES CRIPTOGRÁFICOS**.

Finalmente, se debe generar una contraseña de super usuario por cada uno de los sistemas de información críticos de Entidad, la cual debe ser impresa y enviada al Oficial de Seguridad de la Información o quien haga sus veces, para su custodia y uso en casos de contingencia, tal como se describe en el **MODELO DE CONTRASEÑAS** contenido en el Documento de Modelos del SGI.

5.15 POLITICA DE USO DE CONTROLES CRIPTOGRÁFICOS

La Superintendencia de Sociedades asegurará la protección de la información garantizando la confidencialidad, disponibilidad e integridad, en procesos de comunicaciones y almacenamiento, utilizando esquemas de cifrado seguro en los diferentes escenarios a que exista dicha necesidad, siguiendo la **POLÍTICA DE INTERCAMBIO DE INFORMACIÓN.**

Dicha protección se deberá cumplir con el **MODELO DE USO DE CONTROLES CRIPTOGRÁFICOS** contenido en el Documento de Modelos del SGI y la evaluación de riesgos, donde se deberá identificar el nivel requerido de protección teniendo en cuenta tipo, fortaleza y calidad del algoritmo de cifrado requerido.

5.16 POLÍTICA DE INTERCAMBIO DE INFORMACIÓN

Toda necesidad de intercambio de información con entidades u organizaciones externas, deberá contar con un acuerdo establecido y aprobado por las partes, con la identificación de las cuestiones y requisitos de seguridad.

Se deben establecer controles adecuados para el intercambio de información ya sea a nivel de medios de comunicación electrónicos

Es necesario además de los requerimientos de intercambio de información establecido en el **MODELO DE INTERCAMBIO DE INFORMACIÓN** presentado en el Documento de Modelos del SGI, seguir las buenas prácticas de manejo de información confidencial.

Los usuarios son responsables de cumplir los lineamientos y serán responsables de cualquier violación o incumplimiento de los requerimientos definidos.

5.17 POLITICA DE CLASIFICACIÓN Y ETIQUETADO DE ACTIVOS DE INFORMACIÓN

Toda la información de la Superintendencia de Sociedades deberá reciba el nivel de clasificación acorde a su sensibilidad, y que permita establecer y aplicar los controles de etiquetado y seguridad de información necesarios, que aseguren su confidencialidad, integridad y disponibilidad

Toda información que es recibida, procesada y/o almacenada en medio físico y/o magnético en la Superintendencia de Sociedades es propiedad de la Entidad y debe ser utilizada para fines laborales y conforme a lo acordado con los Usuarios.

Adicionalmente, para definir los controles apropiados cada una de las Intendencias Regionales de La Superintendencia de Sociedades debe mantener un inventario actualizado de los activos de información los cuales deben estar clasificados y etiquetados siguiendo el **PROCEDIMIENTO DE CLASIFICACIÓN Y ETIQUETADO DE ACTIVOS DE INFORMACIÓN.**

5.18 POLÍTICA DE SEGMENTACIÓN DE REDES.

La infraestructura de red de La Superintendencia de Sociedades debe cumplir con los siguientes requerimientos, con el fin de garantizar la Confidencialidad, Integridad y Disponibilidad de la información que ésta transmite.

Las redes de La Superintendencia de Sociedades deben tener por lo menos los siguientes segmentos de red de acuerdo con lo establecido en el MODELO DE SEGMENTACIÓN DE REDES contenido en el Documento de Modelos del SGI:

Producción
Se localizan los servidores de La Superintendencia de Sociedades tales como servidores de aplicaciones que soportan el negocio. Las reglas de control de acceso solo deben permitir el acceso a los servicios prestados.

El acceso para los usuarios de soporte remoto debe realizarse de forma autenticada a través de VPN.

Bases de Datos
Se encuentran las bases de datos de producción. Por tratarse de un activo de información crítico, a este segmento solo pueden acceder los servidores de aplicaciones provenientes del segmento de Producción y a través de VPN, los administradores de Bases de Datos.

Conexiones con Terceros
En este segmento se deben configurar todas las conexiones con terceros. Desde este segmento solo podrán existir conexiones al segmento de Producción con unas reglas de control de acceso definidas y sustentadas. Todas las conexiones con terceros deben ser aisladas entre éstas.

Servicios de Apoyo
Se deben ubicar aquellos servidores que soportan los servicios de apoyo al usuario tales como DNS, Servicio de Directorios, Correo Electrónico entre otros.

Zona Desmilitarizada (DMZ)
Se localizan los servidores que soportan los servicios publicados a Internet. A éste solo deben tener acceso desde internet y para efecto de administración se debe realizar a través de VPN.

Administración y Monitoreo
Este segmento corresponde a las interfaces de administración de los dispositivos de red, servidores, appliances, servicios de monitoreo, correlación de eventos entre otros. A éste solo deben tener acceso los administradores de red y/o plataforma a través de VPN.

Desarrollo y Pruebas
Corresponde al segmento donde deben ubicarse los servidores y/o dispositivos dedicados a pruebas y a desarrollos. A este segmento solo deben tener acceso los desarrolladores y los ejecutores de pruebas.

Usuario
Se deben ubicar los dispositivos usados por los usuarios para sus labores al interior de La Superintendencia de Sociedades.

Es necesario además atender lo descrito en el **MODELO DE SEGMENTACION DE REDES** contenido en el Documento de Modelos del SGI.

5.19 POLÍTICA DE CONTINUIDAD DE NEGOCIO

La Superintendencia de Sociedades debe gestionar y proporcionar los recursos necesarios para la implementación del proceso de continuidad del negocio, para prevenir, atender, recuperar y restaurar las funciones críticas del negocio ante eventos tales como: fallas en los sistemas, fallas de seguridad, perdida del servicio, indisponibilidad de infraestructura física, desastres naturales o los causados por el hombre.

La ejecución de la continuidad del negocio se debe gestionar como un proceso con mejoramiento continuo, involucrando y comprometiendo a todos los Funcionarios en la ejecución de las acciones encaminadas a mantener la continuidad en la prestación del servicio.

Adicionalmente se deben observar los siguientes lineamientos:

1. La prioridad es la protección y seguridad del personal, tanto en situación normal como en situación de contingencia.
2. Planes de Continuidad de Negocio desarrollados e implantados de forma adecuada, teniendo en cuenta todas las áreas, proveedores y servicios críticos.

3. Actualización permanente, pruebas y ajustes al Plan de Continuidad de Negocio ante cambios significativos en premisas, personas, procesos, tecnología o estructura organizativa; con la participación activa en las revisiones de los distintos Grupos de trabajo de la Entidad de los procesos identificados como críticos.

4. Disponibilidad de recursos necesarios para todos los sistemas de información soporte de los procesos identificados como críticos para el negocio, que deben poseer planes de contingencia dentro del Plan de Continuidad de Negocio.

Es necesario además atender lo descrito en el **MODELO DE PLAN DE CONTINUIDAD DE NEGOCIO** contenido en el Documento de Modelos del SGI.

5.20 POLÍTICA DE DESARROLLO SEGURO.

El desarrollo e implementación de nuevos proyectos, sistemas de información, cambios tecnológicos, procesos, servicios y procedimientos deben incluir requerimientos de seguridad de la información en todo su ciclo de vida.

Además de tener en cuenta los requerimientos de seguridad de la información en el desarrollo o mantenimiento de activos de información, estos desarrollos y actualizaciones deben realizarse mediante un procedimiento formal de gestión de cambios. Asimismo, se debe asegurar la existencia de pruebas a los sistemas, la revisión técnica de los aplicativos, una metodología de desarrollo, los ambientes de desarrollo específico, la protección de datos usados en las pruebas y el control de versiones de los sistemas operacionales y de los aplicativos.

Es complemento de esta política lo descrito en el **MODELO DE DESARROLLO SEGURO** contenido en el Documento de Modelos del SGI.

5.21 POLÍTICA DE RELACIONES CON PROVEEDORES.

Se entiende por proveedor a toda persona jurídica o natural, como terceros, contratistas o consultores que provean servicios o productos a Supersociedades.

Para todos los proveedores de servicios o productos en Supersociedades y que actúen con activos de información, se debe realizar un análisis de riesgo con el fin de establecer los requisitos de seguridad que se requieran.

Se deben establecer, acordar y documentar todos los requisitos de seguridad de la información pertinentes con cada proveedor que tenga acceso, procesamiento, almacenamiento, comunicación o suministro de activos de información.

Es necesario además atender lo descrito en el **MODELO DE RELACION CON PROVEEDORES**.

5.22 POLÍTICA DE GESTIÓN DE INCIDENTES.

La gestión de incidentes es la herramienta que permite identificar aquellas debilidades existentes en la seguridad y procesamiento de la información. La Superintendencia de Sociedades debe proporcionar la guía o procedimiento de gestión de incidentes de seguridad de la información y los lineamientos necesarios para su implementación.

Es necesario que exista dentro de la administración de incidentes un equipo responsable del registro, atención, clasificación, comunicación y cierre de incidentes, así como un repositorio actualizado donde queden registrados los diferentes incidentes que se presenten sobre los activos de información.

Para la gestión adecuada de los incidentes deben tenerse en cuenta las siguientes responsabilidades:

- El área de tecnología debe proporcionar un canal apropiado para el reporte, registro y atención de eventos tecnológicos y de incidentes de seguridad de la información.

- Todos los funcionarios, contratistas, terceros y proveedores que usen los activos de información tienen la responsabilidad y el deber de reportar las incidentes, riesgos, debilidades, eventos que observen, detecten o sufran durante su actividad laboral dentro y fuera de Supersociedades.

- En cumplimiento de la ley 1581 de 2012, TÍTULO VI DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO Y ENCARGADOS DEL TRATAMIENTO, artículo 17 Deberes de los Responsables del Tratamiento literal n, y articulo 18 Deberes de los Encargados del Tratamiento literal k, cuando un evento tecnológico o incidente de seguridad involucre violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares, se debe Informar a la autoridad de protección de datos de la Superintendencia de Industria y Comercio.

- La dirección de Informática y Desarrollo debe mantener un procedimiento estándar de registro de incidentes y una sola herramienta de gestión, la cual contendrá un único catálogo unificado de incidentes de seguridad de la información.

5.23 POLÍTICA DE PROTECCION CONTRA CODIGOS MALICIOSOS.

En la superintendencia de sociedades se debe asegurar que la información y la infraestructura de procesamiento de datos estén protegidas contra códigos maliciosos tipo virus.

Se deben implementar controles de detección, prevención y de recuperación, complementados con la toma de conciencia apropiada de los usuarios, para proteger la entidad contra ataques de virus informáticos y códigos maliciosos.

Es necesario además atender lo descrito en el **MODELO DE PROTECCION CONTRA CODIGOS MALICIOSOS**.

5.24 POLÍTICA DE REVISIONES DE SEGURIDAD DE LA INFORMACIÓN.

La superintendencia de sociedades debe asegurar que la seguridad de la Información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.

Para esto debe establecer las revisiones internas y externas, que verifiquen el cumplimiento de políticas y normas de seguridad, así como verificar el cumplimiento técnico.

Es necesario además atender lo descrito en el **MODELO DE REVISION DE SEGURIDAD DE LA INFORMACIÓN**.

5.25 POLÍTICA DE SEGURIDAD EN LAS OPERACIONES.

La superintendencia de sociedades debe asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

Para esto debe establecer los procedimientos documentados de operación para el procesamiento de la información, tales como:

- La gestión de cambios sobre la infraestructura tecnológica, de comunicaciones y de información.
- El establecimiento de diferentes ambientes de trabajo.
- Los procesos de respaldo.
- El registro de eventos y seguimiento.
- El control de software en producción.
- La gestión de vulnerabilidades.
- La gestión de archivos de auditoria.

Es necesario además atender lo descrito en el **MODELO DE SEGURIDAD EN LAS OPERACIONES**.

5.26 POLÍTICA DE MANTENIMIENTO DE HARWARE Y SOFTWARE.

La superintendencia de sociedades debe asegurar la disponibilidad de su infraestructura tecnológica, de sus servicios y de las instalaciones de procesamiento de información.

Para esto debe establecer los procedimientos documentados de mantenimiento de infraestructura tecnológica, teniendo en cuenta los siguientes aspectos:

- El inventario de la infraestructura tecnológica.

- Los planes de mantenimiento.
- La ejecución y control de los planes de mantenimiento
- El control de proveedores
- El soporte técnico de los proveedores

Es necesario además atender lo descrito en el MODELO DE S**EGURIDAD EN EL MANTENIMIENTO DE INFRAESTRUCTURA TECNOLOGICA**.

5.27 POLÍTICA DE GESTIÓN DE LA VULNERABILIDAD TECNICA.

La superintendencia de sociedades debe obtener información oportuna acerca de las vulnerabilidades que existan en la plataforma tecnológica.

Una vez obtenida la información de las vulnerabilidades debe realizar un análisis de los riesgos asociados y tomar las medidas apropiadas para tratar estos riesgos. Si no se cuenta con herramientas propias, se debe realizar contratación externa.

La obtención de las vulnerabilidades técnicas debe realizarse con herramientas especializadas y aceptadas en tecnología sobre los activos internos y externos de las infraestructuras de:

- Procesamiento.
- Comunicaciones.
- Almacenamiento.
- Sistemas y aplicaciones.

Es necesario además atender lo descrito en el **MODELO DE SEGURIDAD EN LAS OPERACIONES**, en lo referente a la gestión de la vulnerabilidad técnica.

6. POLITICA DE GESTION AMBIENTAL

La Superintendencia de Sociedades consciente de la importancia de contribuir con la preservación del medio ambiente se compromete a; identificar y evaluar los aspectos ambientales de cada una de las actividades que realiza la Entidad, con el objetivo de minimizar los impactos derivados de estas, por medio de la implementación de los programas

de gestión ambiental así como el cumplimiento de los requisitos legales y otros requisitos aplicables a la Entidad.

Igualmente, se compromete a identificar los riesgos ambientales que conlleva la ejecución de los procesos y promover las mejores prácticas de gestión para minimizarlos, preservar el medio ambiente, incluida la prevención de la contaminación como clave para reducir la huella ecológica, y no limitado solamente a la Entidad, sino difundiendo estas prácticas a los diversos grupos de interés, con el fin conjunto de la sostenibilidad.

Asimismo, la Superintendencia de Sociedades se compromete con la mejora continua del Sistema de Gestión Ambiental optimizando el desempeño ambiental.

La Superintendencia de Sociedades, enmarca su política del Sistema de Gestión Ambiental bajo los siguientes objetivos:

- Cumplir con la legislación y los requisitos ambientales aplicables a la Entidad.
- Optimizar el consumo de los recursos naturales.
- Proteger el medio ambiente a través de la implementación de los programas del Sistema de Gestión Ambiental.
- Fomentar en los funcionarios una mayor consciencia ambiental.

7. POLITICA PARA COMPRAS SOSTENIBLES

La Superintendencia de Sociedades, adoptará buenas prácticas encaminadas a la protección del ambiente, la reducción en el consumo de recursos, la inclusión y la justicia social, a través de las adquisiciones que generen valor por dinero (eficiencia, eficacia y economía) para cubrir las necesidades de la Entidad.

8. POLITICAS DE SEGURIDAD Y SALUD EN EL TRABAJO

8.1 POLÍTICA DE PREVENCIÓN DEL CONSUMO DE ALCOHOL, CONTROL DE TABAQUISMO Y SUSTANCIAS PSICOACTIVAS.

La Superintendencia de Sociedades considera como violación a la política de consumo de alcohol, control de tabaquismo y sustancias psicoactivas, los siguientes comportamientos:

- Presentarse a laborar bajo el efecto de alcohol y de sustancias psicoactivas a las instalaciones de la Superintendencia y de las empresas intervenidas.
- El consumo de alcohol y drogas, por parte de los funcionarios y contratistas, dentro de las instalaciones la superintendencia de sociedades.
- La posesión, distribución y venta de alcohol y drogas ilegales por parte de funcionarios y contratistas en las instalaciones de la Entidad.
- El consumo de tabaco en zonas no autorizadas por la Superintendencia de Sociedades.
- La automedicación de algún tipo de medicamento que afecte el desarrollo de las actividades laborales en forma segura.

9. POLÍTICAS PARA EL GOBIERNO DE INFORMACIÓN

9.1 POLÍTICA GENERAL DEL GOBIERNO DE INFORMACIÓN

La Superintendencia de Sociedades establecerá y mantendrá un esquema de gobierno de la información actualizado y reconocido en la organización, que determinará el marco rector para la generación, obtención, manejo, producción y tratamiento de la información, así como los principios que regirán el ciclo de vida de la misma, los roles y responsabilidades que garantizarán su proceso óptimo de transformación.

9.2 POLÍTICA PARA LA GESTIÓN CENTRALIZADA DEL MODELO DE DATOS EMPRESARIAL

La Superintendencia de Sociedades, por medio del comité de gobierno de datos, establecerá un esquema para la toma de decisiones relacionadas al diseño y mantenimiento de los modelos de datos requeridos para el almacenamiento de la información de la entidad, con el

fin de garantizar la integración de los modelos de datos de cada sistema en un modelo de datos empresarial.

9.3 POLÍTICA DE GESTIÓN DE DATOS NO ESTRUCTURADOS

La Superintendencia de Sociedades definirá un estándar de administración de información para los formatos no estructurados (documentos, audios, videos e imágenes), el cual abarcará la respectiva identificación del objeto, clasificación, almacenamiento, calidad, medios de acceso y confidencialidad de acuerdo a los requerimientos establecidos.

9.4 POLÍTICA DE CALIDAD DE LA INFORMACIÓN

La Superintendencia de Sociedades deberá asegurar que los datos almacenados en sus sistemas de información cuenten con un nivel de calidad acorde a los requerimientos definidos, mediante la implementación de controles y mediciones de calidad en cada uno de los pasos del ciclo de vida de la información.

9.5 POLÍTICA DE DISPONIBILIDAD Y OPORTUNIDAD DE LA INFORMACIÓN

La Superintendencia de Sociedades implementará un sistema de monitoreo a los acuerdos de niveles de servicios para la captura, adquisición y entrega de información que apoye la eficiencia de los procesos misionales de la Entidad.

9.6 POLÍTICA DE INFORMACIÓN PARA LA TOMA DE DECISIONES

La Superintendencia de Sociedades implementará una estrategia de integración de datos que proporcione un único punto de acceso a la información, el cual debe contener todos los datos oficiales de la Entidad requeridos para el análisis y la toma de decisiones.

9.7 POLÍTICA DE GESTIÓN DE SEGURIDAD DE LOS DATOS

La Superintendencia de Sociedades se compromete a cumplir con los requisitos de seguridad de los datos que garantice el cumplimiento de los parámetros definidos en la política de seguridad del SGI.

9.8 POLÍTICA DE RESPONSABILIDAD Y PROPIEDAD DE LA INFORMACIÓN

La Superintendencia de Sociedades definirá por cada uno de los activos de información las personas responsables de la calidad en el contenido de los datos, de la custodia técnica y aquellas que harán parte del comité de Gobierno de Datos encargado de la toma de decisiones relacionadas con los datos institucionales.

9.9 POLÍTICA DE INFORMACIÓN COMO UN ACTIVO

La Superintendencia de Sociedades gestionará la información como un activo más de la organización, definiendo de manera formal estándares para el uso y manejo adecuado, asegurando el entendimiento de su valor para la Entidad por parte de todos los funcionarios, estableciendo un esquema de rendición de cuentas y responsabilidad para su gestión.

9.10 POLÍTICA DE GESTIÓN DE SERVICIOS

La Superintendencia de Sociedades deberá establecer y mantener un portafolio de servicios de información, así como identificar los proyectos e iniciativas necesarios para mejorarlos.

9.11 POLÍTICA DE GESTIÓN DE METADATOS DE LA INFORMACIÓN

La Superintendencia de Sociedades deberá establecer y mantener una estrategia con metas claras y objetivos específicos para el uso de metadatos.

9.12 POLÍTICA DE LABORATORIO FORENSE

La Superintendencia de Sociedades en cumplimiento de la ley 1778 de 2016 en lo que corresponde a la investigación y sanción sobre la responsabilidad de las personas jurídicas por actos de corrupción transnacional y soborno de servidores públicos extranjeros en transacciones comerciales internacionales, debe contar con:

- Herramientas especializadas y necesarias para obtención de información y datos probatorios, de manera segura.
- Funcionarios preparados para la extracción y tratamiento de la información forense.
- Instalaciones seguras y apropiadas para almacenamiento y tratamiento de información forense.

3. CONTROL DE CAMBIOS

Versión	Vigencia Desde	Vigencia Hasta	Identificación de los cambios	Responsable
001	16 de mayo de 2014	16 de enero de 2015	Creación del documento	Coordinador Grupo de Arquitectura Empresarial y SGI.
002	16 de enero de 2015	26 de Febrero de 2015	Ajuste de las políticas e inclusión de las Políticas para el Gobierno de Información	Coordinador Grupo de Arquitectura de Negocio y SGI.
003	26 de Febrero de 2015	30 de octubre de 2015	Inclusión política de Uso de equipos Portátiles para visitas, diligencias judiciales o trabajos temporales	Coordinador Grupo de Arquitectura de Negocio y SGI.
004	30 de octubre de 2015	10 de noviembre de 2017	Actualización políticas de gobierno de la información y los formatos relacionados en las diferentes políticas	Coordinador Grupo de Arquitectura de Negocio y SGI. Coordinador Grupo datos
005	10 de noviembre 2017	11 de Abril de2018	Se genera una política exclusiva para el SGA con sus respectivos objetivos e indicadores y se elimina el objetivo del SGI correspondiente al Sistema de Gestión Ambiental.	Coordinador Grupo Administrativo-Líder Ambiental
006	11 de Abril de 2018	12 de Octubre de 2018	Se incluyen otras 19 políticas en concordancia con la norma ISO 27001-2013 y se actualiza la	Coordinador Grupo Administrativo-Líder Ambiental – Jefe Oficina Asesora de

			política ambiental.	Planeación.
007	12 de Octubre de 2018	28 de mayo de 2019	Se realizaron ajustes en las políticas del Sistema de Calidad y Ambiental.	Líder Ambiental – Jefe Oficina Asesora de Planeación.
008	29 de mayo 2019		Actualización de: Política de relación con proveedores, Política de compras sostenibles y de la Política de continuidad del negocio	Jefe Oficina Asesora de Planeación

Elaboro: Profesional Grupo de Arquitectura de Negocio y SGI – Contratista seguridad de la información **Fecha : 29 de mayo de 2018**	**Reviso:** Coordinador Grupo de Arqu Negocio y SGI. **Fecha : 29 de mayo de 2018**	**Aprobó:** Jefe oficina asesora de planeación **Fecha : 29 de mayo de 2018**