



**SUPERINTENDENCIA
DE SOCIEDADES**

SUPERINTENDENCIA DE SOCIEDADES

SISTEMA GESTIÓN INTEGRADO

PROCESO GESTION INTEGRAL

DOCUMENTO DE POLITICAS DEL SGI

Código: GC-PO-001

Fecha: 28 de diciembre de
2020


Versión: 011

Número de página 1 de 38



**SUPERINTENDENCIA
DE SOCIEDADES**

**DOCUMENTO DE POLITICAS
DEL SGI**


 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 2 de 38

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.

Por otra parte, el estado colombiano ha venido estableciendo diferentes regulaciones como el Decreto 1008 de 2018 la Política de Gobierno Digital (**PGD**), el modelo de seguridad y privacidad de la Información (**MPSI**), el Modelo Integrado de planeación y Gestión (**MIPG**), la ley de protección de datos personales (**ley 1581 de 2012**) y la Política de Seguridad Digital (**COMPES 854**), que son integradas a los procesos de la Superintendencia de Sociedades y que forman parte de la evaluación de desempeño institucional.

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 3 de 38


1. POLÍTICAS 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.

1.1 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.

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 4 de 38

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

1.1.1 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.

1.2 POLÍTICAS DE GESTIÓN Y DESEMPEÑO INSTITUCIONAL

La superintendencia se compromete a implementar los lineamientos que dan cumplimiento al marco normativo para la aplicación de las 17 políticas para la implementación adecuada y fácil del Modelo, establecidas en el Manual Operativo del Modelo Integrado de Planeación y Gestión, emitido por el Departamento Administrativo de la Función Pública apalancada en el Decreto 1499 de 2017.


Las políticas adoptadas son las siguientes:

1. **Política de Gestión Estratégica del Talento Humano:** El propósito de esta política es permitir que la Superintendencia cuente con talento humano integral, idóneo, comprometido y transparente, que contribuya a cumplir con la misión institucional y los fines del Estado, para lograr su propio desarrollo personal y laboral.
2. **Política de Integridad:** El propósito de esta política es desarrollar mecanismos que faciliten la institucionalización de la política de integridad en la Superintendencia con miras a garantizar un comportamiento probo de los servidores públicos y controlar las conductas de corrupción que afectan el logro de los fines esenciales del Estado.
3. **Política de Planeación institucional:** El propósito de esta política es permitir que la Superintendencia definan la ruta estratégica y operativa que guiará la gestión de la entidad, con miras a satisfacer las necesidades de sus grupos de valor.
4. **Política de Gestión Presupuestal y Eficiencia del Gasto Público:** El propósito de esta política es permitir que la Superintendencia utilice los recursos presupuestales de que disponen de manera apropiada y coherente con el logro de metas y objetivos

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 5 de 38


institucionales, ejecutar su presupuesto de manera eficiente, austera y transparente y llevar un adecuado control y seguimiento.

5. **Política de Fortalecimiento organizacional y simplificación de procesos:** El propósito de esta política es fortalecer las capacidades organizacionales mediante la alineación entre la estrategia institucional y el modelo de operación por procesos, la estructura y la planta de personal, de manera que contribuyan a la generación de mayor valor público en la prestación de bienes y servicios, aumentando la productividad estatal.
6. **Política de Fortalecimiento organizacional y simplificación de procesos:** El propósito de esta política es fortalecer las capacidades organizacionales mediante la alineación entre la estrategia institucional y el modelo de operación por procesos, la estructura y la planta de personal, de manera que contribuyan a la generación de mayor valor público en la prestación de bienes y servicios, aumentando la productividad de la Superintendencia.
7. **Política Gobierno Digital Gobierno Digital:** Esta política busca promover el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones -TIC, para consolidar una entidad competitiva, proactiva, e innovadora, que genere valor público en un entorno de confianza digital.
8. **Política de Seguridad Digital:** En materia de Seguridad Digital, el Documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, para orientar y dar los lineamientos respectivos, los cuales la Superintendencia acatará y aplicará en la ejecución de esta política.
9. **Política de Defensa Jurídica:** La política ayuda a que la Superintendencia oriente sus actividades en el marco de un modelo de Gerencia Jurídica Pública eficiente y eficaz que permita lograr de manera sostenible una disminución del número de demandas en su contra y del valor de las condenas a su cargo. Lo anterior aunado a un mejoramiento de su desempeño en la etapa judicial y en la recuperación por vía de la acción de repetición o del llamamiento en garantía con fines de repetición de las sumas pagadas por sentencias, conciliaciones o laudos arbitrales cuando a ello haya lugar.
10. **Política de Mejora normativa:** tiene como objetivo promover el uso de herramientas y buenas prácticas regulatorias, a fin de lograr que las normas expedidas por la Rama Ejecutiva del Poder Público, en los órdenes nacional y territorial, revistan los parámetros de calidad técnica y jurídica y resulten eficaces, eficientes, transparentes, coherentes y simples, en aras de fortalecer la seguridad jurídica y un marco regulatorio y reglamentario que facilite el emprendimiento, la competencia, la productividad, el desarrollo económico y el bienestar social.
11. **Política de Servicio al ciudadano:** El propósito de esta política es facilitar el acceso de los ciudadanos a sus derechos, mediante los servicios de la entidad, en todas sus

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 6 de 38

sedes y a través de los distintos canales. El servicio al ciudadano se enmarca en los principios de información completa y clara, de igualdad, moralidad, economía, celeridad, imparcialidad, eficiencia, transparencia, consistencia, calidad y oportunidad, teniendo presente las necesidades, realidades y expectativas del ciudadano.

12. **Política de Racionalización de trámites:** tiene como propósito reducir los costos de transacción en la interacción de los grupos de interés con la entidad, a través de la racionalización, simplificación y automatización de los trámites; de modo que los grupos de interés accedan a sus derechos, cumplan obligaciones y desarrollen actividades comerciales o económicas de manera ágil y efectiva frente al Estado.
13. **Política de Participación Ciudadana en la Gestión Pública:** Esta política tiene como propósito permitir que la Superintendencia garantice la incidencia efectiva de los ciudadanos y sus organizaciones en los procesos de planeación, ejecución, evaluación -incluyendo la rendición de cuentas- de su gestión, a través de diversos espacios, mecanismos, canales y prácticas de participación ciudadana.
14. **Política Gestión Documental:** El propósito de la política es lograr mayor eficiencia para la implementación de la gestión documental y Administración de Archivos con el fin de propiciar la transparencia en la gestión pública y el acceso a los archivos como garante de los derechos de los ciudadanos, los servidores públicos y las entidades del Estado; recuperar, preservar y difundir el patrimonio documental de la nación en diferentes medios y soportes como fuente de memoria e identidad cultural; promover el gobierno abierto (transparencia, colaboración y participación) a través de los archivos como herramienta de control social de la gestión pública; fomentar la modernización de los archivos a través de la generación de estrategias que propicien el uso de tecnologías y proyectos de innovación; impulsar en los servidores públicos, la cultura archivística y el desarrollo de estrategias que permitan fortalecer las capacidades para el adecuado manejo y tratamiento de los archivos; así como velar por la recuperación, protección y custodia de los Archivos de los Derechos Humanos, grupos étnicos, comunidades indígenas y población vulnerable.
15. **Política de Transparencia, acceso a la información pública y lucha contra la corrupción:** Esta política le permite a la Superintendencia articular acciones para la prevención, detección e investigación de los riesgos de en los procesos de la gestión administrativa y misional de las entidades públicas, así como garantizar el ejercicio del derecho fundamental de acceder a la información pública a los ciudadanos y responderles de buena fe, de manera adecuada, veraz, oportuna y gratuita a sus solicitudes de acceso a la información pública.
16. **Política de Gestión de la Información Estadística:** Esta política busca que la Superintendencia genere y disponga la información estadística, así como la de sus registros administrativos, de acuerdo con los lineamientos establecidos por el líder de Política, para mejorar la efectividad de su gestión y planeación basada en evidencias; garantizando una continua disponibilidad de información de calidad a lo largo del ciclo de la política pública; fomentando el diálogo social con la ciudadanía y


 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 7 de 38

los grupos de interés, en el marco de la construcción participativa de las soluciones sociales, y generando una herramienta de control político y social que permita la transparencia de las actuaciones del Estado. Adoptada de manera posterior a actualización del Modelo Integrado de Planeación y Gestión del que trata el Decreto 1499 de 2017, mediante el decreto 454 de 2020.

- 17. Política de Gestión del Conocimiento y la Innovación:** La gestión del conocimiento y la innovación como política de gestión y desempeño tiene como propósito facilitar el aprendizaje y la adaptación de la Superintendencia a los cambios y a la evolución de su entorno, a través de la gestión de un conocimiento colectivo y de vanguardia, que permita generar productos/servicios adecuados a las necesidades de los ciudadanos y, además, propicie su transformación en entidades que a través de su dinámica, faciliten la innovación institucional en el marco de un Estado eficiente y productivo.
- 18. Política de Control Interno:** la entidad busca “Desarrollar una cultura organizacional fundamentada en la información, el control y la evaluación, para la toma de decisiones y la mejora continua”.

Así mismo la Superintendencia de Sociedades asigna líderes de política que garanticen y orienten el cumplimiento de dichas políticas en el marco del Modelo Integrado de Planeación y Gestión mediante acto administrativo, quedando como líderes de política los siguientes responsables:

DIMENSIÓN MIPG	POLÍTICAS DE GESTIÓN Y DESEMPEÑO INSTITUCIONAL	DEPENDENCIA / LÍDER DE LA IMPLEMENTACIÓN DE LA POLÍTICA
Talento Humano	Gestión Estratégica del Talento Humano	Gestión de Desarrollo del Talento Humano
	Integridad	Gestión de Desarrollo del Talento Humano, Atención al Ciudadano
Direccionamiento Estratégico y Planeación	Planeación Institucional	Oficina Asesora de Planeación
	Gestión Presupuestal y Eficiencia del Gasto Público	Subdirección Financiera – Subdirección Administrativa
Gestión con Valores para Resultados	Fortalecimiento Organizacional y Simplificación de Procesos	Oficina Asesora de Planeación
	Gobierno Digital	Dirección de Informática y Desarrollo
	Seguridad Digital	Dirección de Informática y Desarrollo – Oficina Asesora de Planeación
	Defensa Jurídica	Oficina Asesora Jurídica
	Mejora Normativa	Oficina Asesora Jurídica
	Servicio al Ciudadano	Atención al Ciudadano
	Participación Ciudadana en la Gestión Pública	Atención al Ciudadano
Racionalización de trámites	Oficina Asesora de Planeación	

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 8 de 38

Evaluación de Resultados	Seguimiento y Evaluación del Desempeño Institucional	Oficina Asesora de Planeación
Información y Comunicación	Gestión Documental	Gestión Documental
	Transparencia, Acceso a la Información Pública y Lucha Contra la Corrupción	Oficina Asesora de Planeación
	Información estadística	Dirección de Informática y Desarrollo – Grupo de Arquitectura de datos
Gestión del Conocimiento y la Innovación	Gestión del Conocimiento y la Innovación	Oficina Asesora de Planeación, quien lidera, con el apoyo de la Gestión del Talento Humano, Dirección de Informática y Desarrollo, Gestión Documental y el área de Comunicaciones
Control Interno	Control Interno	Oficina de Control Interno

1.3 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.

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 9 de 38

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.

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 10 de 38

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.

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 11 de 38

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.

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 12 de 38

2. POLÍTICA DE RIESGOS

2.1 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.

2.2 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.

2.3 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.

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 13 de 38

- 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.

3. 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.

3.1 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.

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 14 de 38

- **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.

3.2 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.

4. POLÍTICAS 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.

4.1 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.

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 15 de 38

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.

Esta política integra lo relacionado con la seguridad de la información, seguridad digital, ciberseguridad, modelo de seguridad y privacidad de la información, la protección de datos personales y la política de gobierno digital.

4.2 POLÍTICA 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.

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 16 de 38

4.3 POLÍTICA 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.


El respaldo de la información institucional es responsabilidad de la Dirección de informática y Desarrollo, por lo tanto, el plan de respaldo de información debe contener lo correspondiente a la información institucional. El respaldo de la información de trabajo que reposa en los equipos de escritorio es responsabilidad de los funcionarios, quienes deben solicitar a la Dirección de informática y Desarrollo, la copia de su información mediante requerimiento a mesa de ayuda.

4.4 POLÍTICA 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 solo debe existir información pública reposando sobre ellos, otro tipo de información (Pública clasificada o pública reservada) 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 directorios de información no pública (confidencial) de los funcionarios o de la compañía, asimismo, no deben tener archivos de trabajo con información no pública en la pantalla de escritorio. 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).

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 17 de 38

4.5 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, STONE, 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.

4.6 POLÍTICA 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. Esto incluye:
 - Hoja de vida
 - Referencias personales y laborales
 - Información académica y crediticia.
 - Antecedentes fiscales y judiciales.

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

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 18 de 38

- 1) **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.

- 2) **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**.


4.7 POLÍTICA 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.

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 19 de 38

4.8 POLÍTICA 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.

4.9 POLÍTICA 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.


4.10 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.

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 20 de 38

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.

4.11 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

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 21 de 38

- 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, sin autorización.
- Cada usuario es responsable de respaldar la información de trabajo individual que almacene en sus equipos de cómputo, en las carpetas de grupo o individuales asignadas al proceso donde labora. Estas carpetas se encuentran en el plan de respaldo de información preparado por tecnología.
- Los usuarios deben bloquear la sesión de sus equipos de trabajo cuando no estén en uso. (tecla Windows + tecla L+ enter).
- 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.
- Mientras el portátil se encuentre en el escritorio del funcionario, debe estar anclado con guaya de seguridad asignada.

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.

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 22 de 38


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 o su representante en caso de las intendencias, 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
5. Tener actualizado el antivirus
6. Contar con actualización de parches de seguridad.

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. Así mismo, debe tener en cuenta las siguientes recomendaciones:

- Debe configurársele una contraseña fuerte.
- No debe llevar información confidencial
- Debe utilizarse únicamente para llevar información referente a la visita
- Una vez terminada la visita y vuelto al sitio de trabajo corporativo se deben descargar los archivos al sitio share point definido y borrar del portátil los archivos.
- No dejar descuidado los dispositivos portátiles en lugares públicos, salas de reuniones y áreas no protegidas.
- En lo posible, los portátiles deben estar asegurados contra robo y daños físicos.
- Configure portátil para que no se conecte automáticamente por WiFi o Bluetooth.
- No conectarlo a redes públicas.
- Cuando un portátil es asignado y utilizado en salas de reuniones o audiencias en la entidad, se deben cumplir los siguientes controles:
 - Debe configurársele una contraseña estándar fácil de recordar.
 - En lo posible debe estar anclado con guaya de seguridad.
 - No debe contener información confidencial.
 - Debe utilizarse únicamente para las presentaciones y conexiones de conferencias autorizadas y aseguradas.
 - Debe tener un responsable asignado.
 - Mientras se encuentre inactivo debe estar apagado.

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 23 de 38

4.12 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**.


4.13 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.

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 24 de 38

4.14 POLÍTICA 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.


4.15 POLÍTICA 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.

4.16 POLÍTICA DE INTERCAMBIO DE INFORMACIÓN

En cumplimiento de la política de gobierno Digital y a la implementación de los servicios ciudadanos digitales en lo referente a Interoperabilidad, Supersociedades adoptará las indicaciones del Manual o Guía del servicio de Interoperabilidad emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones.

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 25 de 38

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.

Si para efectos de cumplir con las labores de vigilancia y control de las sociedades, de acuerdo con el artículo 26 (Prohibición) de la ley 1581 de 2012 y el Artículo 24 (Transferencia y transmisión internacional de datos personales) del decreto 1377 de 2013, solo se podrá transferir y recibir información personal de otros países siguiendo los protocolos y regulaciones establecidas por la Superintendencia de Sociedades y el Gobierno Nacional.

4.17 POLÍTICA DE CLASIFICACIÓN Y ETIQUETADO DE ACTIVOS DE INFORMACIÓN

Toda la información de la Superintendencia de Sociedades deberá recibir 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 las instrucciones del formato GC-F-012 Inventario y Clasificación de Activos.

En la Superintendencia de sociedades, para todos los efectos, la clasificación de la información se realizará siguiendo las definiciones de la ley 1712 de 2014, de la siguiente manera:

a) **Información.** Se refiere a un conjunto organizado de datos contenido en cualquier documento que la Superintendencia de Sociedades genere, obtenga, adquiera, transforme o controle;

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 26 de 38

b) **Información pública.** Es toda información que la Superintendencia de Sociedades genere, obtenga, adquiera, o controle.

c) **Información pública clasificada.** Es aquella información que estando en poder o custodia de la Superintendencia de Sociedades, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 de 2014.

d) **Información pública reservada.** Es aquella información que estando en poder o custodia de la Superintendencia de Sociedades, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la ley 1712 de 2014.

4.18 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.

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 27 de 38

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.

4.19 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, pérdida 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:

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 28 de 38

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 y redundantes 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.
5. Disponibilidad de instalaciones requeridas y redundantes para operar en eventos de emergencia o de desastre.

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

4.20 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.

4.21 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.

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 29 de 38

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.

Para los proveedores que tengan acceso a información de la Superintendencia de Sociedades, se les debe realizar una evaluación de controles de seguridad de la información.

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

4.22 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 los 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 artículo 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

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 30 de 38

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 Tecnología de la Información y las 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.
- En caso de eventos de seguridad de la información que afecten la infraestructura crítica tecnológica o la información de los procesos institucionales, el área encargada de la seguridad de la información debe reportar al CSIRT gobierno, a las Unidades cibernéticas de las Fuerzas Militares y al Comando Conjunto Cibernético de la Policía Nacional, para efectos de realizar investigaciones conjuntas y buscar soluciones para prevenir a otras entidades del estado.

4.23 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.**

4.24 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.**

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 31 de 38

4.25 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 auditoría.

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

4.26 POLÍTICA DE MANTENIMIENTO DE HARDWARE 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 SEGURIDAD EN EL MANTENIMIENTO DE INFRAESTRUCTURA TECNOLÓGICA.**

4.27 POLÍTICA DE GESTIÓN DE LA VULNERABILIDAD TÉCNICA.

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 32 de 38

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.

5. POLÍTICA 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.

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 33 de 38

- 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.

6. POLÍTICA 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.

Es así, como desde la protección del ambiente se podrán adoptar, en lo posible, las fichas técnicas con criterios de sostenibilidad que expida el Ministerio de Ambiente y Desarrollo Sostenible, para los procesos contractuales de adquisición de bienes y servicios entre otros en las siguientes categorías:

- Obras civiles
- Insumos de oficina
- Servicios generales
- Servicios de transporte
- Equipos eléctricos


7. POLÍTICAS PARA EL GOBIERNO DE INFORMACIÓN

7.1 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.

7.2 POLÍTICA PARA LA GESTIÓN CENTRALIZADA DEL MODELO DE DATOS EMPRESARIAL

La Superintendencia de Sociedades, por medio del grupo de arquitectura de datos de la Dirección de Tecnología de la Información y las Comunicaciones, 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.

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 34 de 38

7.3 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.

7.4 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.

7.5 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.

7.6 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.

7.7 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.

7.8 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.

7.9 POLÍTICA DE INFORMACIÓN COMO UN ACTIVO

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 35 de 38

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.

7.10 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.

7.11 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.

8. 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.

9. POLÍTICA DE GOBIERNO DIGITAL

La Superintendencia de Sociedades de acuerdo con el Decreto 1008 de 2018, "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital", para su implementación, adoptará y aplicará el Manual de Gobierno Digital que define los lineamientos, estándares y acciones a ejecutar, y realizará las siguientes actividades:

- Sensibilizaciones de la política de Gobierno Digital.
- Creación de un plan de implementación de la política de Gobierno Digital.
- Ejecución de los lineamientos y estándares de la política de Gobierno Digital.
- Generación de los indicadores de cumplimiento y resultado que permitan medir el grado de implementación de la política de Gobierno Digital.

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 36 de 38

10. POLÍTICA DE SEGURIDAD DIGITAL.

La Superintendencia de Sociedades en cumplimiento de la normatividad que promueve la Política de Gobierno Digital y el Modelo Integrado de Planeación y Gestión (MIPG) del Estado colombiano, y con el fin de cumplir con los propósitos de contar con servicios digitales de confianza y calidad, procesos internos seguros y eficientes, decisiones basadas en datos, empoderamiento ciudadano y ayudar a tener territorios y ciudades inteligentes, fortalecerá su gestión para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en las actividades de transformación digital, mejoramiento continuo de sus procesos y sistemas de información y en el uso de tecnologías disruptivas.

Asimismo, participará activamente como parte integral del Sector Industria, Comercio y Turismo, en la definición de los activos de información críticos, los controles y buenas practicas a implementar para prestar al ciudadano servicios y tramites en condiciones adecuadas de disponibilidad, confiabilidad, seguridad digital y cibernética.

Para incrementar la capacidad de defensa ante amenazas y riesgos actuales de seguridad digital, la Superintendencia de Sociedades reconoce como instancias de ayuda y soporte a las siguientes entidades:


- El Comité de Seguridad Digital del que trata el Acuerdo 002 de 5 de junio de 2018 del Consejo para la Gestión y el Desempeño Institucional
- La Coordinación Nacional de Seguridad Digital (Presidencia de la República)
- Las unidades cibernéticas de las Fuerzas Militares
- Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC, Grupo de Respuestas a Emergencias Cibernéticas de Colombia - ColCERT
- Equipo de respuesta a incidentes de seguridad informática CSIRT de Gobierno
- CAI Virtual Policía Nacional de Colombia
- Fiscalía General de la Nación y sus centros de investigación

En conjunto con estas entidades y en el momento que se requiera, se conformarán equipos que puedan ayudar a superar incidentes de seguridad digital.

11. POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

La Superintendencia de Sociedades de acuerdo con el Decreto 1377 de 2013 y ley 1581 de 2012, se compromete a su cumplimiento mediante la generación y aplicación de los lineamientos, procedimientos y medidas de seguridad que permitan proteger los datos personales existentes en las diferentes bases de datos y en uso en sus procesos operativos y administrativos.

12. POLÍTICAS DE SEGURIDAD Y SALUD EN EL TRABAJO

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 37 de 38


12.1 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.

13. 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 de 2018	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	12 de Octubre de 2018	Se incluyen otras 19 políticas en concordancia con la norma ISO 27001-	Coordinador Grupo Administrativo-Líder

 SUPERINTENDENCIA DE SOCIEDADES	SUPERINTENDENCIA DE SOCIEDADES	Código: GC-PO-001
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de diciembre de 2020
	PROCESO GESTION INTEGRAL	Versión: 012
	DOCUMENTO DE POLITICAS DEL SGI	Número de página 38 de 38

	2018		2013 y se actualiza la política ambiental.	Ambiental – Jefe Oficina Asesora de 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	15 de marzo de 2020	Actualización de: Política de relación con proveedores, Política de compras sostenibles y de la Política de continuidad del negocio	Jefe Oficina Asesora de Planeación
009	16 de marzo de 2020	15 de octubre de 2020	Se incluye lo correspondiente a nuevas reglamentaciones (Gobierno Digital, Seguridad Digital, MIPG y protección de datos personales (ley 1581 de 2012). Se actualizan las políticas: 5.11; 5.16; 5.17. Se adicionan políticas de Laboratorio forense, Gobierno Digital, Protección de datos personales y Seguridad Digital.	Jefe Oficina Asesora de Planeación
010	16 de octubre de 2020	31 de octubre de 2020	Inclusión del numeral de políticas de desempeño institucional.	Jefe Oficina Asesora de Planeación
011	01 de noviembre de 2020	21 de Diciembre de 2020	Inclusión de los lineamientos para la protección del medio ambiente de la Política para Compras Sostenibles de la Entidad	Líder ambiental
012	28 de Diciembre de 2020		Se incluyen como instancias de apoyo y soporte a las entidades del estado nombradas en el numeral 10. Política de Seguridad Digital.	Jefe Oficina Asesora de Planeación

Elaboró: Profesional Grupo de Arquitectura de Negocio y SGI – Contratista seguridad de la información	Revisó: Jefe Oficina Asesora de Planeación	Aprobó: Jefe Oficina Asesora de Planeación
--------------------------------------------------------------------------------------------------------------	---------------------------------------------------	---------------------------------------------------

Fecha: 28 de diciembre de 2020

Fecha: 28 de diciembre de 2020

Fecha: 28 de diciembre de 2020