SUPERINTENDENCIA
DE SOCIEDADES

DOCUMENTO DE POLITICAS DEL SGI

1. INTRODUCCIÓN.

La Superintendencia de Sociedades para la gestión y organización del SGI y de los requisitos de la norma NTC GP-1000 y la norma NTC ISO 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 continúo de los procesos y el mantenimiento del SGI.

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

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

2. POLITICAS DEL SISTEMA DE GESTION INTEGRADO.

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

NUESTRA POLITICA

2.1 POLÍTICA DEL SGI

La Superintendencia de Sociedades con el fin de anticipar y prevenir la crisis empresarial y la atención oportuna de la insolvencia en el sector real, mediante una gestión socialmente responsable, se compromete con la implementación de un Sistema de Gestión Integrado (SGI) que contempla los siguientes aspectos:

- Estableciendo relaciones equitativas y justas con usuarios, proveedores y ciudadanos, mediante la determinación y mantenimiento de mecanismos de comunicación que permitan el contacto con las partes interesadas en pro del aumento de la satisfacción de los usuarios.
- Asegurando las características de Integridad, Confidencialidad y Disponibilidad de los procesos y sus activos de información, a través de una gestión de riesgos apoyada en la gestión de incidentes, continuidad del negocio y de la cultura organizacional.
- Proporcionando los recursos necesarios para la implementación y el funcionamiento del SGI y el mantenimiento de la infraestructura para el desarrollo de sus actividades.
- Apoyando y promulgando las diferentes actividades orientadas a la sostenibilidad y sustentabilidad del Ambiente. Instaurando como prioritario el cumplimiento de los requisitos legales, el control, mitigación y prevención de los impactos ambientales, mediante la gestión sostenible de sus procesos, consumo eficiente de los recursos y la promoción de buenas prácticas ambientales.
- Velando por el respeto de los derechos humanos y las prácticas de no discriminación.
- Asegurando el desarrollo de las competencias de sus funcionarios, para mejorar continuamente la eficacia, eficiencia y efectividad de sus procesos.
- Declarando y apoyando las diferentes actividades que sustentan la integridad física y mental de sus trabajadores, instaurando como prioritario el

cumplimiento de los requisitos legales a nivel ocupacional, la identificación, control y minimización de los factores de riesgos laborales que puedan derivar en incidentes y/o accidentes de trabajo y enfermedades de origen laboral, entendiendo y aceptando que los funcionarios son parte imprescindible en el éxito de los procesos de la Entidad.

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

Incumplimiento de las Políticas:

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

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

2.2 POLÍTICA 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.

2.2.1. PRINCIPIOS DE LA POLÍTICA DE GESTIÓN DOCUMENTAL

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

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

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

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

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

Protección del medio ambiente: Con la adopción de los lineamientos establecidos dentro de la política de 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.

2.2.2. 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.

2.3 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

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

2.3.1 POLÍTICA DE ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN

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

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

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

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

POLITICA DE CUMPLIMIENTO DE DERECHOS DE PROPIEDAD INTELECTUAL

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

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

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

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

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

2.3.2 POLITICA DE RESPALDO DE LA INFORMACIÓN

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

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

2.3.3 POLITICA DE ESCRITORIO DESPEJADO Y PANTALLA LIMPIA

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

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

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

2.3.4 POLÍTICA DE CONTROL DE ACCESO A LOS SISTEMAS

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

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

2.3.5 POLITICA DE SEGURIDAD DEL TALENTO HUMANO

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

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

Es responsabilidad del Grupo de Desarrollo del Talento Humano incluir en los programas de inducción y capacitación, la sensibilización en Seguridad de la Información. De igual forma debe incluir en los procesos de nombramiento la firma y aceptación del **GTH-F-026 Formato Acuerdo Confidencialidad**

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**.

2.2.7 POLITICA DE SEGURIDAD FISICA

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

2.2.8 POLÍTICA DE TRABAJO REMOTO

El Trabajo Remoto que impliquen 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.

2.2.9 POLÍTICA DE USO ADECUADO DE LOS RECURSOS

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

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

Reglas Generales

- Si para el uso del recurso se requiere un usuario y una contraseña

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

Correo Electrónico

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

Red e Internet

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

Portátiles y Equipos de Escritorio

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

USB y Medios de Almacenamiento

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

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

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

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

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

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

2.2.10 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 aprobara de acuerdo con las políticas establecidas y reportara 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.**

2.2.11 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 a 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.

2.2.12 POLITICA DE USO DE CONTRASEÑAS

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

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

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

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

2.2.13 POLITICA DE USO DE CONTROLES CRIPTOGRÁFICOS

La Superintendencia de Sociedades asegurará la protección de la información garantizando la confidencialidad, disponibilidad e integridad, en procesos de comunicaciones y almacenamiento, utilizando esquemas de cifrado seguros 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.

2.2.14 POLÍTICA DE INTERCAMBIO DE INFORMACIÓN

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

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

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

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

2.2.15 POLITICA DE CLASIFICACIÓN Y ETIQUETADO DE ACTIVOS DE INFORMACIÓN

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

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

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

2.2.16 POLÍTICA DE SEGMENTACIÓN DE REDES.

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

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

Producción

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

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

Bases de Datos

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

Conexiones con Terceros

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

Servicios de Apoyo

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

Zona Desmilitarizada (DMZ)

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

Administración y Monitoreo

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

Desarrollo y Pruebas

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

Usuario

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

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

2.2.17 POLÍTICA DE CONTINUIDAD DE NEGOCIO

La Superintendencia de Sociedades debe proporcionar los lineamientos necesarios para la preparación, planificación, desarrollo e implementación del Plan de Continuidad de Negocio de sus procesos productivos, sustentados en principios extraídos de las necesidades del negocio y el entendimiento de los riesgos de los activos de La Superintendencia de Sociedades.

Dichos principios son:

1. La prioridad es la protección y seguridad del personal, tanto en situación normal como en situación de contingencia.
2. Planes de Continuidad de Negocio desarrollados e implantados de forma adecuada, teniendo en cuenta todas las áreas, proveedores y servicios críticos.
3. Actualización permanente, pruebas y ajustes al Plan de Continuidad de Negocio ante cambios significativos en premisas, personas, procesos, tecnología o estructura organizativa; con la participación activa en las revisiones de los distintos Grupos de trabajo de la Entidad de los procesos identificados como críticos.
4. Disponibilidad de recursos necesarios para todos los sistemas de información soporte de los procesos identificados como críticos para el negocio, que deben poseer planes de contingencia dentro del Plan de Continuidad de Negocio.

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

2.3 POLITICAS DE GESTION AMBIENTAL

2.3.1 POLITICA PARA COMPRAS SOSTENIBLES

La Superintendencia de Sociedades, orientada a cambiar los patrones de consumos hacia la sostenibilidad ambiental, incluirá dentro de sus procesos de contratación de bienes, servicios y obras, criterios de calidad ambiental con el fin de avanzar hacia los modelos de desarrollo sostenible y la calidad de vida.

2.4 POLITICAS DE SEGURIDAD Y SALUD EN EL TRABAJO

2.4.1 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.

2.5 POLÍTICAS PARA EL GOBIERNO DE INFORMACIÓN

2.5.1 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.

2.5.2 POLÍTICA PARA LA GESTIÓN CENTRALIZADA DEL MODELO DE DATOS EMPRESARIAL

La Superintendencia de Sociedades, por medio del comité de gobierno de datos, establecerá un esquema para la toma de decisiones relacionadas al diseño y mantenimiento de los modelos de datos requeridos para el almacenamiento de la información de la entidad, con el fin de garantizar la integración de los modelos de datos de cada sistema en un modelo de datos empresarial.

2.5.3 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.

2.5.4 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.

2.5.5 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.

2.5.6 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.

2.5.7 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.

2.5.8 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.

2.5.9 POLÍTICA DE INFORMACIÓN COMO UN ACTIVO

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

2.5.10 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.

2.5.11 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.

3. CONTROL DE CAMBIOS

Versión	Vigencia Desde	Vigencia Hasta	Identificación de los cambios	Responsable
001	16 de mayo de 2014	16 de enero de 2015	Creación del documento	Coordinador Grupo de Arquitectura Empresarial y SGI.
002	16 de enero de 2015	26 de Febrero de 2015	Ajuste de las políticas e inclusión de las Políticas para el Gobierno de Información	Coordinador Grupo de Arquitectura de Negocio y SGI.
003	26 de Febrero de 2015	30 de octubre de 2015	Inclusión política de Uso de equipos Portátiles para visitas, diligencias judiciales o trabajos temporales	Coordinador Grupo de Arquitectura de Negocio y SGI.
004	30 de octubre de 2015		Actualización políticas de gobierno de la información y los formatos relacionados en las diferentes políticas	Coordinador Grupo de Arquitectura de Negocio y SGI. Coordinadora Grupo datos