SUPERINTENDENCIA DE NOTARIADO & REGISTRO La guarda de la fe pública	MACROPROCESO: SISTEMAS INTREGADOS DE GESTIÓN	Código : SIG - SGC - PO - 01 - FR - 06
	PROCESO: SISTEMA DE GESTIÓN DE CALIDAD	Versión: 01
	FORMATO ROLES, RESPONSABILIDADES Y AUTORIDAD	Fecha: 06-05-2022

INTRODUCCIÓN

Cuando se habla de la implementación de Sistema Integrado de Gestión, es importante identificar la estructura organizacional, con el fin de definir los roles, responsabilidades y autoridades para las diferentes tareas que se deben realizar, es necesario tener claridad de todas las funciones con el fin de lograr la eficiencia y efectividad que se requiere para el buen desarrollo de la entidad, por lo cual la Superintendencia de Notariado y Registro diseña este documento que ayuda a la articulación e implementación del Sistema de Gestión de la Calidad, Sistema de Gestión Ambiental, Sistema de Gestión de Seguridad de la Información y al Sistema de Gestión de Seguridad y Salud en el Trabajo, y/o procesos.

Por lo anterior se tomará como base la estructura definida en el Decreto 2723 del 29 de diciembre, de 2014, considerando el artículo 15 y sus numerales (1, 3, 5, 14, 17), la Oficina de Tecnologías de la Información en el artículo 17 y sus numerales (1, 2, 4, 7, 20 y 21), la Dirección de Talento Humano en el artículo 29 y sus numerales (2, 5 y 6), la Dirección Administrativa y Financiera en el artículo 31 y su numeral (1); y la resolución 11682 del 19 de octubre de 2015.

OBJETIVO

Establecer los roles, responsabilidades y autoridades dentro de la Superintendencia de Notariado y Registro, en relación Al Sistema de Gestión de Calidad, Sistema de Gestión Ambiental, Sistema de Gestión de Seguridad de la Información y al Sistema de Gestión de Seguridad y Salud en el Trabajo y procesos.

ALCANCE

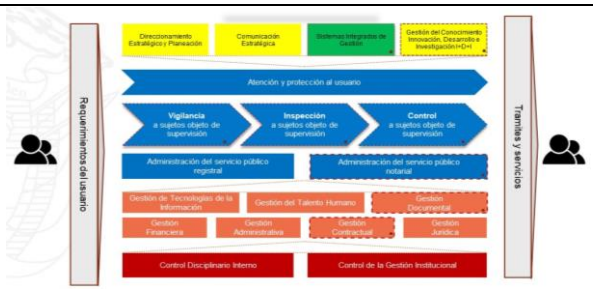
Inicial: Identificar las funciones y responsables de los sistemas integrados de gestión (Sistema de Gestión de la Calidad, Sistema de Gestión Ambiental, Sistema de Gestión de Seguridad de la Información y al Sistema de Gestión de Seguridad y Salud en el Trabajo), y procesos.

Final: Definición de roles, responsabilidades y autoridades de cada funcionario y contratista que se requiera para el cumplimiento de los objetivos de SNR.

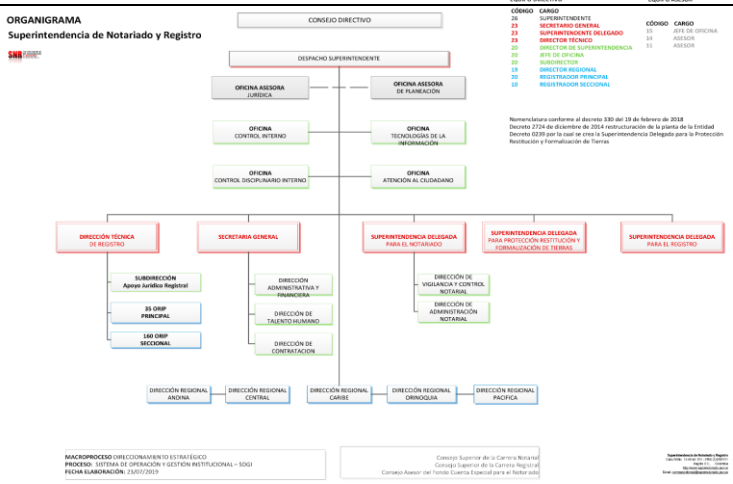
DEFINICIONES

•DENOMINACIÓN DE EMPLEO: Hace referencia al empleo que ejercerá el funcionario de acuerdo con la norma vigente de nomenclatura y clasificación de empleos.
•PUESTO DE TRABAJO: Conjunto de tareas ejecutado por una persona.
•CARGO DEL JEFE INMEDIATO: Este está relacionado por la persona que actuara como su jefe inmediato, vigilara y evaluara su trabajo.
•FUNCIÓN: Es un conjunto de tareas, que el ocupante del cargo ejerce de manera sistemática.
•TAREA: Un ejercicio con un principio y un fin para conseguir los objetivos propuestos.
•GESTIÓN: Actividades coordinadas para dirigir y controlar una entidad.
•SISTEMA DE GESTIÓN: Un sistema de gestión es un conjunto de normas y principios relacionados entre sí de forma ordenada, para contribuir a la gestión de procesos generales o específicos de una entidad. Permite establecer una política, unos objetivos y alcanzar dichos objetivos.
•ROL: El rol corresponde a una función que se desempeña según el lugar o situación.
•RESPONSABILIDAD: son las obligaciones por las que debe responder el colaborador según el cargo que desempeña.
•AUTORIDAD: La autoridad es el poder legítimo, es decir, el poder que una persona tiene en virtud del rol o la posición que tiene dentro de la estructura organizacional.
•SISTEMA DE GESTIÓN AMBIENTAL SGA: Es una parte del Sistema de Gestión de la empresa que permite fomentar y llevar a cabo la política ambiental y los objetivos marcados por la entidad.
•SISTEMA DE GESTIÓN DE CALIDAD SGC: Está formado por un conjunto de políticas, procesos y procedimientos documentados. Este conjunto define la forma en que la entidad elaborará y entregará el producto o servicio a sus usuarios, con el fin de asegurarse su satisfacción.
•SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI: El concepto clave de un SGSI es el diseño, implantación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.
•SISTEMA DE GESTION DESEGURIDAD Y SALUD EN EL TRABAJO SGSST: El Sistema de Gestión de Seguridad y Salud en el Trabajo es un sistema de gestión basado en una serie de procesos administrativos cuyo principal objetivo es la prevención y el control de los accidentes y las enfermedades ocupacionales que pueden surgir en el trabajo.
•INFORMACIÓN: La información constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

MAPA DE PROCESO



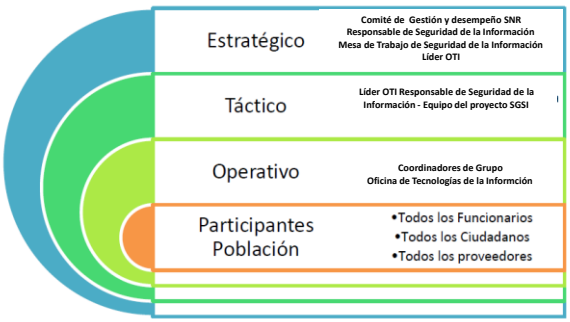
ORGANIGRAMA GENERAL



SUPERINTENDENCIA DE NOTARIADO & REGISTRO La guarda de la fe pública	MACROPROCESO: SISTEMAS INTREGADOS DE GESTIÓN	Código: SIG - SGC - PO - 01 - FR - 06
	PROCESO: SISTEMA DE GESTIÓN DE CALIDAD	Versión: 01
	FORMATO ROLES, RESPONSABILIDADES Y AUTORIDAD	Fecha: 06-05-2022

SISTEMA Y/O PROCESO

Organigrama



MATRIZ DE ROLES, RESPONSABILIDAD Y AUTORIDAD

ROL	RESPONSABILIDAD	AUTORIDAD	RENDICION DE CUENTAS		
			¿Qué cuentas rinde?	¿A Quien?	¿Cada Cuanto?
Comité Institucional de Gestión y desempeño de la SNR	Tomar decisiones y aprobar los recursos necesarios para la implementación del SGSI. Aprobar los lineamientos en materia de seguridad de la información Hacer seguimiento a las políticas y al Sistema de Gestión de Seguridad de la Información en General. Velar por el cumplimiento de las políticas de Seguridad de la información en toda la Entidad. Aprobar la clasificación de los activos de información. Analizar y Aprobar el riesgo residual. (Fuente: MSPI - Guia No.4 Roles y Responsabilidades).	Impartir y hacer seguimiento a lineamientos estratégicos asociados con la gestión de la Seguridad de la Información.	Apoyar y promover la implementación del sistema y aprobar documentos tales como procedimientos, políticas y demás exigidos por la normat en la implementación y mejora del SGSI	Entidades normativas y regulatorias	Cuando sea requerido.
Mesa de Trabajo de Seguridad de la Información **Los integrantes son los representantes de:** **• Oficina de Tecnologías de la Información (OTI).** **• Planeación (OAP)** **• Gestión Documental** **• Control Interno** **• Subdirección Técnica de Registro** **• Demás actores que puedan interactuar en el proceso y/o sus delegados.**	Revisar y preaprobar las políticas, procedimientos, metodologías, formatos y demás elementos del Sistema de Gestión de Seguridad de la Información. Revisar informes de diagnósticos (herramientas formales internas-MINTIC) del estado de la seguridad de la información de la Entidad. Revisar la gestión de seguridad de la información en cuanto a cumplimiento de las políticas establecidas y la normativa legal vigente. Validar el cumplimiento de los requisitos legales, contractuales, normativos y buenas prácticas de seguridad de la información y privacidad de los datos personales. Presentar al Comité Institucional de Gestión y Desempeño de la entidad, los documentos generados al interior del equipo técnico de seguridad de la información que impacten de manera transversal a la misma.	Validar que los documentos, metodologías, procedimientos y en general de instrumentos implementados en el SGSI cumplan con los requerimientos normativos de Seguridad de la Información.	Presentar observaciones a los documentos e instrumentos en general que forman parte del SGSI en los tiempos establecidos (5 días hábiles siguientes a la presentación por parte del Equipo de implementación SGSI) y presentar Acta de revisión con los documentos Anexos.	Comité de Gestión y desempeño Institucional	Cuando sea requerido.
Oficial / responsable de Gestión de Seguridad de la Información	Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad. Gestionar recursos con el Comité de Gestión y desempeño para el cumplimiento de los objetivos y los lineamientos de gestión de la seguridad de la información. Informar acerca del avance en la gestión de la seguridad de la información al Comité de Gestión y desempeño de la Entidad. Recomendar roles y responsabilidades específicas relacionados con la seguridad de la información para mejorar la gestión. (Fuente: MSPI - Guia No.4 Roles y Responsabilidades).	Responsable de la Implementación del SGSI al interior de la Entidad y de direccionar acciones de segunda línea de defensa de seguridad de la información.	Presentar avances del plan de trabajo y recomendaciones sobre el uso de recursos y estrategias para proyectar y mantener el SGSI	Comité de Gestión y desempeño Institucional	Informes bimestrales
Grupo de Implementación SGSI.	Sugerir lineamientos para cubrir brechas identificadas en los diagnósticos. Programar plan de ejecución de diagnósticos. Promover y acompañar el desarrollo de proyectos de seguridad de la información. Participar en la formulación y evaluación de planes de acción para mitigar riesgos (Identificación de Vulnerabilidades y amenzas y establecimiento de controles). Establecer y proponer estrategias de comunicación, sensibilización (consolidación de comportamientos alineados con la Seguridad de la Información) y capacitación. Hacer seguimiento y control al cumplimiento de las políticas, gestión de riesgos y definición de controles que permitan la mejora continua de la seguridad de la información de la Entidad (planeación PHVA). Sugerir estrategias que permitan el mejoramiento de la seguridad de la información (incluye el mejoramiento en la privacidad de los datos personales - Confidencialidad) en la Entidad. Revisar y proponer estrategias para la gestión de los activos de información de la Entidad y para la gestión de sus riesgos asociados.	Las establecidas como Segunda línea de defensa de seguridad de la información.	Presentar informes periódicos de avance de la implementación del SGSI de acuerdo con el plan oficial de implementación con vigencia anual.	Oficial de seguridad de la información	Una vez al mes
Equipo de Respuesta a incidentes de seguridad de la información	Preparar la plataforma tecnológica. Investigar y/o implementar productos y proyectos de seguridad de la información. Gestionar procedimientos de gestión de incidentes de seguridad de la información y planes de capacitación. Diseñar política de publicación y publicar incidentes de seguridad de la información. Detectar incidentes de seguridad de la información Atender incidentes de seguridad Analizar incidentes de seguridad de la información Mitigar y remediar incidentes de seguridad de la información (contención y erradicación) Gestionar vulnerabilidades de seguridad de la información.	Gestionar un enfoque estructurado y planificado para la atención de incidentes de seguridad de la información y vulnerabilidades, de acuerdo a matriz RACI en documento "Roles y responsabilidades equipo de Respuesta a incidentes de seguridad de la información".	Atención y solución de los incidentes de seguridad de la información y vulnerabilidades y orientación metodológica.	Comité de Gestión y desempeño Lider OTI. Oficial de seguridad de la información.	Cuando sea requerido (cuando se presenta incidentes - riesgos materializados) Seguimiento a planes de gestión de vulnerabilidades en reporte cuatrimetral. Seguimiento mensual para Jefatura OTI (Incidentes y vulnerabilidades).
Coordinadores de Grupo (Lideres de Proceso)	Identificar, inventariar y clasificar los nuevos activos (análogos y digitales de información), los riesgos de seguridad de la información asociados y su plan de tratamiento. Asegurar la implementación de controles para disminuir el riesgo residual. Cumplir con los lineamientos del modelo de gestión en cuanto a control de riesgos Primera Linea de defensa.	Responsabilidad alineada con Primera Línea de Seguridad de la Información	Gestionar el registro y clasificación de los Activos de Información a su cargo y del plan de tratamiento de riesgos de seguridad de la información asociados.	Jefes de Area	Gestión de transacciones a Activos de información cuando sea requerido. Revisión de los activos de información mínimo una vez al año. Gestión continua del plan de tratamiento de riesgos de seguridad de la información.

ROL	RESPONSABILIDAD	AUTORIDAD	RENDICION DE CUENTAS		
			¿Qué cuentas rinde?	¿A Quien?	¿Cada Cuanto?
Jefe de la OTI	Participar en el diseño del cronograma de capacitación de seguridad digital en la entidad, alineado con el plan de capacitaciones de talento humano.	Coordinar la asignación de recursos y gestión de iniciativas que propendan por la mejora de la seguridad de la información y de manera alineada con los planes de tratamiento de riesgos para los Activos bajo su custodia.	Cumplir el plan de implementación de iniciativas a su cargo para mejorar la Seguridad de la Información.	Alta Gerencia	Informe mensual de avance.
	Implementar las mejoras identificadas en la plataforma de seguridad que estén relacionadas con hardware, software, canales de comunicaciones de datos o infraestructura TI.				
	Comunicar a los funcionarios, contratistas y/o particulares que participan en actividades de forma directa o indirecta con la SNR, la importancia de satisfacer los requisitos y cumplir las políticas de seguridad digital.				
	Hacer seguimiento al cumplimiento de las políticas y al Sistema de Gestión de Seguridad de la Información conforme con los requisitos legales, normativos y técnicos establecidos por el marco regulatorio y otros adoptados o definidos por la Entidad (MSPI-ISO 27001). Ejecutar Auditorías Internas anuales, realizadas por auditores certificados en la norma, con el fin de validar el cumplimiento de las políticas de seguridad de la información implementadas en la Entidad, a fin de comprobar si la entidad ha avanzado en la implementación de controles, protección de los activos, mantenimiento de la integridad de los datos. (Se tomará como referencia para la realización de las Auditorias la Guía No.15 del Ministerio de las Tecnologías de la información. - Guía de auditoría seguridad y privacidad de la información".				
	Tomar decisiones sobre los incidentes de seguridad y continuidad de las operaciones en términos de la afectación de los servicios que presta la Entidad y de su objetivo como Entidad.				
Oficina Control Interno	Recomendar acciones tendientes a mejorar la efectividad del sistema de gestión de seguridad de la información y comunicar a las partes interesadas.	Responsabilidad alineada con Tercera Línea de defensa de Seguridad de la Información	Reportar recomendaciones para mejor alineamiento de políticas y gestión del Sistema de Gestión de seguridad de la información	Comité de Gestión y desempeño Institucional	Cuando lo considere necesario.
Partes interesadas (funcionarios, Contratistas y Proveedores):	Cumplir con las políticas de seguridad y privacidad de la información y cláusulas establecidas en el MSPI.	Reportar oportunidades de mejoramiento de seguridad de la información.	Promover el uso de iniciativas efectivas que promuevan mejoras en la seguridad de la información.	Grupo de Implementación SGSI	Cuando sea requerido.
	Reportar oportunidades de mejoramiento en seguridad de la información por los canales establecidos.				