PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

SUPERINTENDENCIA
DE NOTARIADO Y REGISTRO

JOSÉ RICARDO ACEVEDO SOLARTE
JEFE OFICINA DE TECNOLOGIA DE LA INFORMACIÓN
JUAN CARLOS VALENZUELA BUITRAGO
PROFESIONAL OFICINA DE TECNOLOGIA DE LA INFORMACIÓN
HUGO ALEJANDRO CASALLAS LARROTTA
PROFESIONAL OFICINA DE TECNOLOGIA DE LA INFORMACIÓN
MÓNICA YANETH GALVIS GARCÍA
COORDINADORA GRUPO ARQUITECTURA ORGANIZACIONAL Y MEJORAMIENTO CONTINUO DE LA OFICINA ASESORA DE PLANEACIÓN
JUAN CAMILO GUIRAN SÁNCHEZ
PROFESIONAL OFICINA ASESORA DE PLANEACIÓN

República de Colombia

Ministerio de Justicia y del Derecho

Superintendencia de Notariado y Registro

TABLA DE CONTENIDO

1. INTRODUCCION

La Superintendencia de Notariado y Registro reconoce que la información es un activo vital para el cumplimiento de su misión y visión institucionales. Por tanto, ha establecido como una prioridad fundamental la implementación y el mantenimiento de un Sistema de Gestión de Seguridad de la Información (SGSI). Este SGSI no solo garantizará la protección de los activos de información, sino que también respaldará el logro de los objetivos estratégicos de la organización en un entorno cada vez más digital y conectado.

Con el fin de llevar a cabo este compromiso, la Superintendencia ha diseñado un Plan Estratégico de Seguridad de la Información. Este plan detalla los procedimientos y las prácticas necesarias para una implementación efectiva del SGSI, basándose en estándares reconocidos a nivel nacional e internacional.

Además, el plan se adapta específicamente a las necesidades y características de la Superintendencia, considerando su contexto operativo y los riesgos asociados a sus actividades.

La elaboración de este plan se fundamenta en un análisis exhaustivo de la situación actual de seguridad de la información de la organización, así como en una visión clara de las metas y objetivos futuros. A través de este enfoque proactivo, la Superintendencia busca no solo garantizar la confidencialidad, integridad y disponibilidad de la información, sino también mejorar continuamente sus prácticas de seguridad y adaptarse a un entorno cambiante, fortaleciendo la confianza de la ciudadanía, en el marco de la Política Pública de Gobierno Digital.

2. MARCO LEGAL

El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- Resolución 1978 DE 2023 “por la cual se adopta la Versión 3 del Marco de Referencia de Arquitectura Empresarial para el Estado Colombiano como el instrumento para implementar el habilitador de arquitectura de la Política de Gobierno Digital y se dictan otras disposiciones” – Donde se establece la guía general MAE.G.AS - DOMINIO DE ARQUITECTURA DE SEGURIDAD.
- Resolución 500 de 2021. “*Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital*”.
- Decreto 612 de 2018, “*Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado*”, donde se encuentra el

presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.

- Decreto 767 de 2022 - Política de Gobierno Digital.
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.

3. OBJETIVO DEL PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Establecer de manera detallada las directrices, objetivos, metas y acciones específicas que la Superintendencia de Notariado y Registro seguirá para proteger la seguridad y privacidad de la información basado en la identificación y análisis, valoración y tratamiento de los riesgos a los cuales se ven sometidos los activos críticos de seguridad de la información, definiendo los controles de seguridad necesarios para protegerlos. Así mismo, asignará roles y responsabilidades, recursos y establecerá un cronograma para la implementación de las medidas de seguridad. Contribuyendo de manera significativa al mejoramiento de la seguridad de la información organizacional, a través del fortalecimiento de la confidencialidad, la integridad y la disponibilidad de sus activos de seguridad de la información, minimizando los riesgos a los que están expuestos.

3.1. OBJETIVOS ESPECÍFICOS

- Definir y establecer la estrategia de seguridad digital de la entidad, alineada con los objetivos organizacionales y estándares internacionales, para garantizar una protección integral de los activos de información, lo cual permitirá dar respuesta eficiente frente a los desafíos y las amenazas emergentes en el ámbito digital.
- Establecer las necesidades de la entidad para la implementación del Sistema de Gestión de Seguridad de la Información, asegurando que se cumplan los requisitos específicos y se aborden las vulnerabilidades identificadas.
- Priorizar los proyectos, con el fin de optimizar la asignación de recursos y maximizar el impacto en la seguridad de la entidad, a fin de realizar una correcta implementación del SGSI, considerando los recursos disponibles, el nivel de riesgo y la criticidad de los activos de información.
- Planificar la evaluación y seguimiento de los controles implementados en el marco del Sistema de Gestión de Seguridad de la Información, garantizando su eficacia y ajustándolos según sea necesario para mantener un nivel óptimo de seguridad.

- Implementar y fortalecer las actividades de arquitectura de seguridad de la información, garantizando la integración adecuada de controles y medidas de seguridad en la infraestructura tecnológica de la entidad para proteger los activos de información de manera proactiva y eficiente.

4. ALINEACIÓN INSTITUCIONAL

El Plan Estratégico de Seguridad de la Información (PESI) se integra de manera coherente y contribuye al logro del Plan Estratégico Institucional (PEI), alineándose con sus diversos componentes. El PEI establece ocho (8) focos estratégicos en estrecha articulación con las políticas del Gobierno Nacional. A partir de estos, se derivan los objetivos estratégicos institucionales que orientan el cumplimiento de la misión y visión de la entidad. A continuación, se relacionan los focos establecidos.

El PESI abarca transversalmente todos los objetivos estratégicos, proporcionando un respaldo integral para salvaguardar la integridad, confidencialidad y disponibilidad de los activos de seguridad de la información.

Su propósito primordial es mitigar los riesgos asociados a estos, reduciendo la probabilidad, impacto y previniendo las diferentes amenazas y vulnerabilidades que puedan afectar los activos, ocasionando interrupciones parciales o totales en la operación o procesos de la entidad, los cuales podrían afectar diversas actividades y comprometer el cumplimiento de los objetivos institucionales.

De conformidad a lo anterior el Plan Estratégico de Seguridad de la Información, se alinea como soporte de forma global para el cumplimiento de los objetivos de la entidad, y genera una alineación directa con los objetivos relacionados con los focos estratégicos de "Transformación Digital" y “Gestión Integral”. apoyados desde los siguientes aspectos específicos:

- **Establecimiento del Sistema de Gestión de Seguridad de la Información:** Para proyectos que involucran gestión de información, tales como la conservación, digitalización, sistematización e indexación de datos registrales y notariales, así como la migración jurídica de información, se establecen medidas de seguridad para proteger la integridad y confidencialidad de los datos en cada fase. Además, se colabora con asesoría a los procesos responsables para asegurar el cumplimiento de los estándares de seguridad.

- **Aseguramiento de la integridad, confidencialidad y disponibilidad de la información:** Se garantizan en los sistemas de información misionales diseñados y desarrollados, implementando medidas de seguridad para su robustez y cumplimiento de los estándares requeridos. Se colabora en la definición de estándares y la integración de controles de seguridad durante el proceso de diseño y desarrollo del sistema.

- **Implementación de medidas de seguridad adecuadas para la protección de los servicios misionales y la información transmitida y almacenada:** Se garantiza la autenticación y autorización adecuadas para los usuarios, así como la identificación y gestión de riesgos asociados a la prestación de servicios digitales, promoviendo una cultura de seguridad de la información entre los usuarios y proveedores de servicios.

El Plan Estratégico de Seguridad de la Información (PESI) respalda además las siguientes premisas establecidas en el PEI:

- **Transformación Digital:** Abraza la transformación digital como pilar fundamental, asegurando la alineación de las iniciativas de seguridad de la información con las tecnologías emergentes y las necesidades de la organización en un entorno digital en constante evolución.
- **Retos Organizacionales:** Se adapta proactivamente para abordar los desafíos inherentes a la gestión de la seguridad de la información, garantizando la efectividad de las medidas de seguridad en todos los niveles de la organización.
- **Generación de Valor Público:** Se concibe como una herramienta para la generación de valor público, asegurando la protección de la información sensible y promoviendo la confianza de los ciudadanos en las actividades y servicios de la institución.
- **Articulación con las Políticas del Gobierno Nacional:** Con un enfoque en la implementación de la "Políticas de Gobierno Digital" y sus dos componentes, "TIC para el estado" y "TIC para la sociedad". Estos componentes están respaldados por tres habilitadores transversales, entre los cuales se encuentra la "Seguridad de la Información".

- **Gestión Integral:** Desde el proceso de Gestión de Tecnología de la Información y las Comunicaciones se encarga de definir y emplear una amplia gama de recursos tecnológicos, que van desde métodos y herramientas hasta equipos físicos, los cuales respaldan tanto la estrategia como los procesos organizacionales. Además, liderando la implementación del Sistema de Gestión de Seguridad de la Información (SGSI).

Para llevar a cabo lo anterior, se han definido varios proyectos y actividades con el propósito de actualizar y fortalecer los servicios tecnológicos, los cuales incluyen la adopción de las últimas tendencias en seguridad digital e implementación de estándares internacionales en seguridad de la información, con un enfoque que apoya el desarrollo e implementación del Modelo Integrado de Gestión y Planeación (MIPG), especialmente en la dimensión Gestión con Valores para Resultados. En el marco de la implementación de políticas de gobierno y seguridad digital, las cuales contribuyen al logro de la misión y visión de la Superintendencia de Notariado y Registro.

5. ALCANCE

El Plan Estratégico de Seguridad de la Información al buscar la implementación del Sistema de Gestión de Seguridad de la Información y la estrategia de seguridad digital de la entidad, comparte el alcance definido dentro de la Política General de Seguridad de la Información, donde se indica que se tendrán en cuenta todos los procesos de la entidad.

6. ESTADO ACTUAL DE LA SUPERINTENDENCIA DE NOTARIADO Y REGISTRO RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La Superintendencia de Notariado y Registro ha llevado a cabo exhaustivas evaluaciones y diagnósticos en relación con la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), con un enfoque especial en el Modelo de Seguridad y Privacidad de la Información (MSPI) establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones. Además, como parte de este ejercicio de autodiagnóstico, se ha realizado un análisis minucioso de la infraestructura existente. Permitiendo identificar los diversos componentes de seguridad, evaluar su estado actual, identificar riesgos y determinar los aspectos que requieren fortalecimiento para mejorar la postura de seguridad de la entidad.

6.1. RIESGOS CRÍTICOS DE SEGURIDAD DE LA INFORMACIÓN

De acuerdo con el diagnóstico, se han identificado riesgos críticos de grado extremo cuya materialización tendría serias implicaciones tanto para la entidad como para el país. Estos riesgos afectarían principalmente la disponibilidad de los sistemas misionales, lo que tendría un impacto significativo en la ciudadanía. Además, se han observado posibles repercusiones en términos de reputación, aspectos legales y cumplimiento normativo debido a la exposición de información sensible.

Se recomienda abordar prioritariamente estos riesgos críticos en los planes de adquisiciones para el año 2024, es esencial priorizarlos debido al impacto crítico que podrían tener en la Superintendencia de Notariado y Registro si no se gestionan en el menor tiempo posible.

	RIESGO	AMENAZAS	NIVEL DE RIESGO	PLAN DE TRATAMIENTO PRIORITARIO
1	AFECTACIÓN DE LA DISPONIBILIDAD DE LOS SERVICIOS DE LA SNR	FALLA DE EQUIPOS	CRÍTICO	• Renovación de licenciamiento soporte y garantía. • Actualización de equipos. • Ejecución de diagnóstico y mantenimiento de los equipos por el proveedor y fabricante • Ejecución hardening. • Inclusión de renovación en presupuesto anual.
		DAÑO DE LA INFRAESTRUCTURA TECNOLÓGICA		
		DAÑOS POR CONDICIONES AMBIENTALES		
		EQUIPOS DESACTUALIZADO O VULNERABLE		

	RIESGO	AMENAZAS	NIVEL DE RIESGO	PLAN DE TRATAMIENTO PRIORITARIO
		AUSENCIA DE CONTRATOS DE SOPORTE, GARANTÍA Y MANTENIMIENTO DE EQUIPOS		
		ATAQUES Y/O INFECCIONES POR RANSOMWARE, MALWARE Y DENEGACIÓN DE SERVICIOS		
2	AFECTACIÓN DE LA DISPONIBILIDAD O PERDIDA DE COMUNICACIÓN Y SISTEMAS DE INFORMACIÓN CON SEDES NIVEL CENTRAL Y ORIPS TERRESTRES	FALLA DE EQUIPOS	CRÍTICO	• Generación proyecto para adquisición de equipos en alta disponibilidad. • Instalación y configuración de equipos nuevos de conectividad. • Inclusión de renovación equipos en presupuesto anual
		EQUIPO OBSOLETO O SIN SOPORTE		
		EQUIPOS DESACTUALIZADO O VULNERABLE		

	RIESGO	AMENAZAS	NIVEL DE RIESGO	PLAN DE TRATAMIENTO PRIORITARIO
3	AFECTACIÓN DE LA CONFIDENCIALIDAD INTEGRIDAD Y DISPONIBILIDAD DE LOS SERVICIOS	SOFTWARE DESACTUALIZADO Y VULNERABLE CLAVES Y USUARIOS EXPUESTOS PARAMETRIZACIÓN INCORRECTA	CRÍTICO	• Cambio inmediato de contraseñas de las cuentas. • Integración urgente con Directorio Activo • Implementación de MFA • Adquirir software para acceso • Realizar configuración de la plataforma
4	AFECTACIÓN DE LA CONFIDENCIALIDAD INTEGRIDAD Y DISPONIBILIDAD DE LOS SERVICIOS	EQUIPOS OBSOLETOS SIN SOPORTE	CRÍTICO	• Adquisición de licencias de protección para cobertura de todos los equipos de la entidad. • Cambio de equipos obsoletos.
5	AFECTACIÓN DE LA CONFIDENCIALIDAD	USO INADECUADO DE LOS RECURSOS DE LA ENTIDAD	CRÍTICO	• Adquisición de servicio filtrado **malicioso**.

	RIESGO	AMENAZAS	NIVEL DE RIESGO	PLAN DE TRATAMIENTO PRIORITARIO
	INTEGRIDAD Y DISPONIBILIDAD DE LOS SERVICIOS	ATAQUES Y/O INFECCIONES POR RANSOMWARE, MALWARE Y DENEGACIÓN DE SERVICIOS		• Instalación y configuración de equipo filtrado.
6	FALTA DE RESPUESTA ANTE INVESTIGACIONES POR AUSENCIA DE MECANISMOS DE AUDITORÍA	DEFICIENCIA DE LOGS INVESTIGACIONES	CRÍTICO	• Gestión de logs, equipo para correlación de eventos **o un servicio tercerizado que realice estas gestiones.**
7	AFECTACIÓN DE LA DISPONIBILIDAD DE LOS SERVICIOS DE LA SNR POR FALTA DE ESTANDARIZACIÓN DE CONTROLES O UN	FALLA DE EQUIPOS CORRUPCIÓN DE DATOS FALTA DE SISTEMAS DE MONITOREO	CRÍTICO	• Definición e inicio de implementación de Plan Estratégico de Seguridad de la Información

	RIESGO	AMENAZAS	NIVEL DE RIESGO	PLAN DE TRATAMIENTO PRIORITARIO
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	ATAQUES Y/O INFECCIONES POR RANSOMWARE, MALWARE Y DENEGACIÓN DE SERVICIOS		
		ABUSO DE DERECHOS		
		ROBO DE INFORMACIÓN		
8	SANCIONES POR INCUMPLIMIENTO LEGAL O NORMATIVO	INCUMPLIMIENTO GOBIERNO DIGITAL	**CRÍTICO**	
		INCUMPLIMIENTO LEY DE PROTECCIÓN DE DATOS		
9	AFECTACIÓN DE LA INTEGRIDAD Y DISPONIBILIDAD DE LOS SERVICIOS	DEFICIENCIAS DE ESQUEMAS DERESPALDO	**ALTO**	• Definición de lineamientos de respaldo. • Estrategias de uso y apropiación de herramientas para respaldos.

	RIESGO	AMENAZAS	NIVEL DE RIESGO	PLAN DE TRATAMIENTO PRIORITARIO
11	AFECTACIÓN DE LA CONFIDENCIALIDAD INTEGRIDAD Y DISPONIBILIDAD DE LOS SERVICIOS	AUSENCIA DE GESTIÓN DE VULNERABILIDADES	**ALTO**	• Adquisición de servicios de ethical hacking **y remediación de vulnerabilidades**
12	AFECTACION DE LA INTEGRIDAD, DISPONIBILIDAD Y CONFIDENCIALIDAD, POR FALTA DE VISIBILIDAD	INFECCIONES POR RANSOMWARE, MALWARE Y DENEGACIÓN DE SERVICIOS	**MEDIO**	• Renovación de licenciamiento soporte y garantía. • Adquisición de equipo para visibilidad de red
		DEFICIENCIAS EN GESTIÓN DE LOGS		
		INVESTIGACIONES		

	RIESGO	AMENAZAS	NIVEL DE RIESGO	PLAN DE TRATAMIENTO PRIORITARIO
10	DETRIMENTO O SUBUTIZACIÓN DE RECURSOS, ASI COMO ACCESOS NO AUTORIZADOS AFECTANDO LA CONFIDENCIALIDAD INTEGRIDAD Y DISPONIBILIDAD DE LOS SERVICIOS	SISTEMAS DE INFORMACIÓN CON PARAMETRIZACIÓN DEFICIENTE O INADECUADA ACCESO NO AUTORIZADO	**MEDIO**	• Renovación de licenciamiento soporte y garantía. • Actualización del equipo. • Ejecución de diagnóstico y mantenimiento de equipos. • Ejecución hardening **y despliegue de la plataforma.** • Inclusión de renovación en presupuesto anual

6.2. DIAGNÓSTICO DE SEGURIDAD DE LA INFORMACIÓN

Para evaluar el estado del Sistema de Gestión de Seguridad y Privacidad de la Información, se llevó a cabo el diligenciamiento del **INSTRUMENTO DE DIAGNÓSTICO DE SEGURIDAD DE LA INFORMACIÓN** establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC). Este instrumento está diseñado para medir el progreso en la implementación del Modelo de Seguridad y Privacidad de la Información. En este proceso, se consideraron la definición de lineamientos y controles, su aplicación, el análisis de la infraestructura, la adopción de una cultura de seguridad, infraestructura tecnológica y entrevistas con diversos colaboradores del proceso. Se asignó una valoración a cada uno de los controles.

A continuación, se presenta el resultado del autodiagnóstico que servirá como punto de referencia para el año 2024. Además, con base en las evaluaciones y diagnósticos efectuados, se estableció una línea base utilizando los dominios de la norma **ISO 27001:2022**. Para este proceso se empleó el "Instrumento de Autodiagnóstico de Seguridad y Privacidad de la Información", y el resultado de la calificación de implementación de los dominios para la entidad es el siguiente:

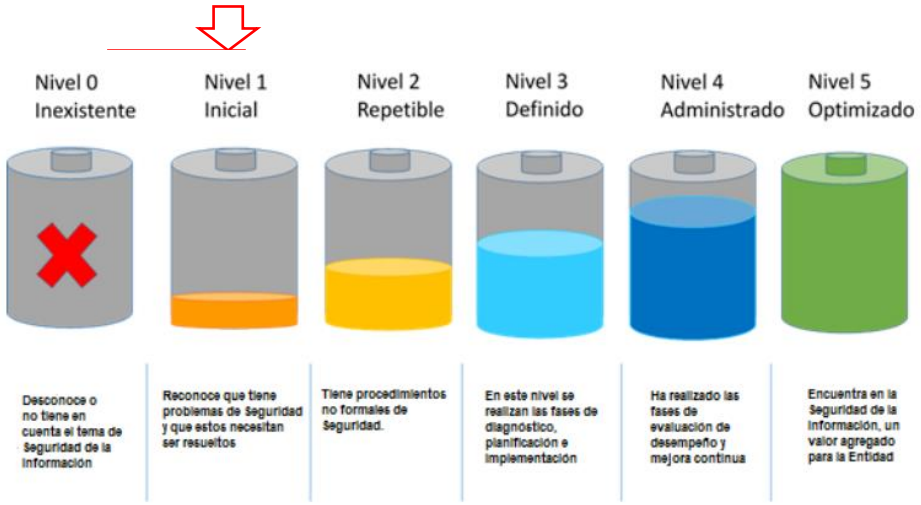
No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	CONTROLES ORGANIZACIONALES	20	100	INICIAL
A.6	CONTROLES DE PERSONAS	29	100	REPETIBLE
A.7	CONTROLES FISICOS	31	100	REPETIBLE
A.8	CONTROLES TECNOLÓGICOS	18	100	INICIAL
PROMEDIO EVALUACIÓN DE CONTROLES		25	100	

Año	CLÁUSULAS		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2024	Contexto de la organización	25%	100%
	Liderazgo	20%	100%
	Planificación	20%	100%
	Soporte	44%	100%
	Operación	13%	100%
	Evaluación del desempeño	13%	100%
	Mejora	10%	100%
TOTAL		21%	100%

En la gráfica anterior, que muestra la calificación de cada uno de los controles por dominio de la norma ISO 27001, se observa que la mayoría de los puntos requieren ser fortalecidos para cumplir con los estándares internacionales de seguridad, como los establecidos por la ISO 27001. Este fortalecimiento es fundamental para garantizar el cumplimiento de las normativas del Modelo de Seguridad y Privacidad del MINTIC, así como para alinearse con el Modelo Integrado de Planeación y Gestión (MIPG) y cumplir con la política de Gobierno Digital.

Además, siguiendo la metodología establecida por el MINTIC para evaluar el nivel de madurez del Sistema de Gestión de Seguridad de la Información, es necesario continuar con un proceso sistemático de evaluación y mejora continua. Este enfoque garantizará que la entidad esté preparada para hacer frente a los desafíos y riesgos en constante evolución en el ámbito de la seguridad de la información.

Se determina que el SGSI de la Superintendencia de Notariado y Registro se encuentra actualmente en el siguiente nivel:



Con base a la gráfica anterior, el nivel 1 Inicial con avance intermedio, traduce la siguiente descripción.

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información

A continuación, se proporciona un desglose de los aspectos más destacados dentro de cada dominio del sistema, donde se identifican áreas que requieren acciones de mejora. Estas acciones son esenciales para garantizar que la entidad alcance un nivel mínimo aceptable en su sistema de gestión de seguridad de la información.

CONTROLES	SITUACIÓN ACTUAL	SITUACIÓN DESEADA
POLITICA DE SEGURIDAD DE LA INFORMACIÓN	• La política de seguridad no ha sido revisada desde el 2021. • Se encuentra inmersa junto al manual de políticas de seguridad, lo que no permite delimitar lo que hace parte de la política general y que hace parte del manual. • No existe objetivo general y los objetivos específicos con más de 15 y en su mayoría no son medibles. • No hay evidencia de una apropiación adecuada de la política general ni de las políticas específicas.	• Una política actualizada, con objetivos precisos y medibles, que permitan asegurar el compromiso de la alta dirección y de todos los procesos de la entidad. • Una política debidamente comunicada y apropiada por parte de la entidad.
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Los roles y responsabilidades establecidas no se vienen ejecutando de forma estricta, al igual que los posibles entregables o reportes.	Fomentar el cumplimiento de los roles y responsabilidades definidos para el SGSI, incluyendo una participación por parte de las diferentes áreas involucradas.
SEGURIDAD DE LOS RECURSOS HUMANOS	La entidad cuenta con mecanismos para verificar los antecedentes de los nuevos empleados y su retiro, sin embargo, hay deficiencias en la parte de capacitaciones respecto a las temáticas de seguridad y acuerdos de confidencialidad.	Procedimientos de vinculación y desvinculación del personal totalmente concertados y aplicados entre la OTI, Talento Humano y la oficina de Contratación, con procesos de inducción constantes donde se

CONTROLES	SITUACIÓN ACTUAL	SITUACIÓN DESEADA
		incluyan las políticas de seguridad y las buenas prácticas de seguridad.
GESTIÓN DE ACTIVOS	Existen unas metodologías complejas para la gestión de activos, las cuales no son aplicadas. No existen inventarios de activos por proceso.	• Metodología y herramientas adecuadas para la gestión de activos de información en la SNR. • Inventarios de activos de información plenamente documentados y gestionados por los procesos.
CONTROL DE ACCESO	Existen herramientas tecnológicas para controlar el acceso a los sistemas de información, sin embargo, no existen lineamientos específicos para la gestión de los usuarios, usuarios privilegiados o de auditoría.	Lineamientos precisos y aplicables para blindar los sistemas de la entidad de accesos no autorizados e implementar accesos con el menor privilegio posible.
CRIPTOGRAFÍA	Controles criptográficos insuficientes para las implementaciones necesarias en la entidad. Ausencia de inventario actualizado de controles criptográficos.	Cobertura de los activos necesarios con controles criptográficos (incluyendo cifrado de equipos en los activos que lo requieran).
SEGURIDAD FÍSICA Y DEL ENTORNO	Existen controles de seguridad física, sin embargo, no se observa una política particular para la seguridad física en la entidad, que defina las áreas seguras y los lineamientos específicos para esta temática.	Lineamientos definidos y aplicados respecto a la seguridad física en la entidad, las áreas seguras y otras condiciones de seguridad en la SNR.

CONTROLES	SITUACIÓN ACTUAL	SITUACIÓN DESEADA
SEGURIDAD DE LAS OPERACIONES	La infraestructura de seguridad se encuentra sin cobertura y soporte adecuados, adicionalmente, no hay certeza de su funcionamiento y despliegue en su totalidad. Así mismo, si bien la entidad cuenta con procedimientos documentados como el procedimiento gestión de cambios. Los mismos no están adaptados a las necesidades de la entidad y no se encuentran apropiados.	• Infraestructura de seguridad debidamente cubierta por garantías, soporte y mantenimiento. • Nueva infraestructura y servicios de seguridad que aumenten los niveles de protección de la SNR. • Actualización de procedimientos
SEGURIDAD DE LAS COMUNICACIONES	La infraestructura de comunicaciones se encuentra sin cobertura y soporte adecuados. Deben realizarse mejoras respecto al cuidado de la infraestructura física de redes.	• Infraestructura de seguridad debidamente cubierta por garantías, soporte y mantenimiento. • Nueva infraestructura de red que aumente la disponibilidad y el performance en la SNR.
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	No hay una organización definida respecto a la adquisición, desarrollo y mantenimiento de los sistemas de información, hay falencias en el manejo de ambientes y versionamiento.	• Procedimientos de adquisición, desarrollo y mantenimiento de sistemas de información alineados a las necesidades y recursos de la SNR. • Prácticas de desarrollo seguro debidamente apropiadas por el personal de la SNR. • Manejo de versiones,

CONTROLES	SITUACIÓN ACTUAL	SITUACIÓN DESEADA
RELACIONES CON LOS PROVEEDORES	Existen lineamientos para seguimiento de relación con contratistas o terceros, orientado a la supervisión de proyectos. Sin embargo, no se encuentran los aspectos relacionados con riesgos, ANS, cadena de suministro, acuerdos de confidencialidad.	• Proveedores con condiciones de seguridad establecidas desde la firma de los contratos. • Análisis de riesgos de seguridad realizados previo al inicio de los contratos. • Acuerdos de confidencialidad incluidos dentro de los procesos de contratación con terceros y contratistas.
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	El procedimiento sigue un flujograma confuso, no se están teniendo en cuenta los eventos de seguridad (los cuales deben incluirse aquí). Así mismo, se asume que el oficial tiene que ejecutar la gran mayoría de actividades y hay otros roles que se deben involucrar.	Definir un procedimiento de gestión de incidentes adecuado y alineado con los roles y personal que tiene la SNR para este fin, para posteriormente ser difundido y apropiado por toda la entidad, tanto por usuarios finales para que sepan como reportar los incidentes como por el personal de la OTI para ejecutar adecuadamente el procedimiento.
GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	No existe documentación estratégica respecto a la continuidad de negocio, sin embargo, existen controles a nivel técnico que soportan estrategias básicas de restauración de servicios y redundancias	Plan de continuidad de TI debidamente soportado por: • Análisis de Riesgos de Disponibilidad • Análisis BIA
CUMPLIMIENTO	Se tienen identificadas normativas en seguridad de la información, sin embargo, no están actualizadas.	Normograma actualizado e informado en la entidad, respecto a las normativas tanto en seguridad de la información como en protección de datos personales.
SEGURIDAD EN LA NUBE	No existen controles para la infraestructura en la nube que	Lineamientos y controles de seguridad de la información con

CONTROLES	SITUACIÓN ACTUAL	SITUACIÓN DESEADA
	actualmente se encuentra desplegada. Si bien la SNR está iniciando transición hacia modelos híbrido debe incorporar desde el inicio controles de seguridad.	alcance extendido hacia la infraestructura desplegada en la nube, esto incluye control de cambios, gestión de incidentes, control de acceso lógico etc.…

7. ESTRATEGIA DE SEGURIDAD DIGITAL

La Superintendencia de Notariado y Registro, en su compromiso por brindar servicios innovadores y con un enfoque en confianza y seguridad digital, integrará en su estrategia de seguridad medidas que promuevan la implementación de controles y estándares de seguridad robustos, así como la adopción del Modelo de Seguridad y Privacidad del MINTIC. Estas medidas incluirán la implementación de controles de seguridad adecuados, la adopción de estándares reconocidos internacionalmente y el cumplimiento de las directrices establecidas por el MINTIC en materia de seguridad de la información.

Dado que la Superintendencia cuenta con servicios e información críticos para el país, es imperativo garantizar su operación continua y evitar posibles impactos a nivel nacional. Por lo tanto, se implementarán medidas para fortalecer su postura de seguridad para proteger los activos de información crítica, asegurando así la estabilidad y confiabilidad de los servicios notariales y registrales, y mitigando cualquier riesgo que pueda afectar el funcionamiento del país.

En este contexto, la Superintendencia establecerá una estrategia de seguridad digital integral, donde se integrarán los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información. Esta estrategia estará centrada en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) del MINTIC, así como en la guía de gestión de riesgos de seguridad de la información, implementación de controles tecnológicos y el fortalecimiento de la cultura organizacional en seguridad de la información.

Por consiguiente, la Superintendencia de Notariado y Registro ha delineado los siguientes cinco ejes, los cuales conformarán una estrategia integral de seguridad digital:

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Establecer una estructura organizacional sólida y un liderazgo claro en materia de seguridad de la información, asegurando que esta sea una prioridad en todos los niveles de la organización. Este objetivo se logra mediante la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), a través de la aprobación de la política general y sus lineamientos específicos destinados a proteger la confidencialidad, integridad y disponibilidad de los activos de seguridad de la información. Esto requiere el compromiso activo de la alta dirección y de los líderes de los diferentes procesos dentro de la entidad. Además, en este eje se definen roles y responsabilidades claros en seguridad de la información, promoviendo una cultura organizacional que valore la seguridad y fomente la concientización y responsabilidad compartida entre los colaboradores.
Gestión de riesgos	Identificar, evaluar y gestionar los riesgos relacionados con la seguridad de la información en la organización. Su objetivo es establecer un proceso sistemático para detectar y mitigar amenazas que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información.

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
	Esto implica la implementación de metodologías para analizar los riesgos, la evaluación de su impacto y la definición de medidas de seguridad adecuadas para mitigarlos. Además, se establecen procesos de monitoreo y revisión continua para adaptar las medidas de seguridad según sea necesario, garantizando así una gestión proactiva y efectiva de los riesgos de seguridad de la información. Este proceso se realiza a través de la planificación y valoración de los riesgos, con el objetivo de prevenir o reducir los efectos indeseados, y se fundamenta en la implementación de controles de seguridad para el tratamiento adecuado de los riesgos identificados.
Cultura de seguridad de la información	Fortalecer la construcción de una cultura organizacional que priorice la seguridad de la información. Para ello, se promueven políticas, procedimientos, normas, buenas prácticas y otros lineamientos en todos los niveles de la organización. Se enfatiza la transferencia de conocimiento y la asignación y divulgación de responsabilidades relacionadas con la seguridad y privacidad de la información a todo el personal. Además, se busca crear conciencia sobre la importancia de proteger la información sensible y promover comportamientos seguros en su manejo.
Implementación de controles	Desarrollo e implementación de medidas y controles de seguridad adecuados para mitigar los riesgos identificados. Esto incluye la formulación de políticas de seguridad, la aplicación de controles técnicos y la elaboración de procedimientos operativos. Además, se planifican y ejecutan acciones necesarias para alcanzar los objetivos de seguridad y privacidad de la información, asegurando así la confianza en la ejecución de los procesos de la Entidad. Estas medidas se subdividen en controles tecnológicos y administrativos para una gestión integral de la seguridad de la información.
Gestión de incidentes	Establecer un proceso estructurado y eficaz para detectar, responder y resolver incidentes de seguridad de la información de manera oportuna y efectiva. Su objetivo principal es minimizar el impacto de los incidentes en la organización y garantizar la continuidad operativa. Además, busca fortalecer la resiliencia y la capacidad de respuesta frente a futuros eventos, así como mitigar la posibilidad de que los mismos vuelvan a presentarse.
Mejora continua	Estableciendo un enfoque iterativo y proactivo, la organización busca fortalecer constantemente su postura de seguridad. Esto se logra mediante la revisión y actualización regular de políticas y controles de seguridad, la

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
	evaluación periódica de riesgos y vulnerabilidades, la actualización continua de tecnologías y prácticas de seguridad, así como la integración de los resultados de la formación del personal y las lecciones aprendidas de incidentes. Orientando la entidad a una adaptación ágil a las cambiantes amenazas cibernéticas, garantizando una protección sólida de los activos de seguridad de la información.

7.1. PORTAFOLIO DE PROYECTOS Y ACTIVIDADES

Para cada estrategia específica, la SUPERINTENDENCIA DE NOTARIADO Y REGISTRO define las siguientes actividades, proyectos y productos, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI):

ESTRATEGIA/ EJE	ACTIVIDADES/PROYECTOS	PRODUCTOS ESPERADOS
Liderazgo de seguridad de la información	Establecer el Plan Estratégico de Seguridad de la Información	Plan Estratégico de Seguridad de la Información establecido y aprobado por el Comité Institucional.
	Revisar y actualizar la Política General de Seguridad de la Información	Política General de Seguridad de la Información Actualizada y Aprobada por el Comité Institucional.
	Revisar y actualizar el Manual de Políticas de Seguridad de la Información	Manual de Políticas de Seguridad de la Información actualizado y aprobado por el Comité Institucional.

ESTRATEGIA/ EJE	ACTIVIDADES/PROYECTOS	PRODUCTOS ESPERADOS
	Revisar y actualizar los roles y responsabilidades en Seguridad de la Información.	Roles y Responsabilidades actualizados y aprobados por el Comité Institucional.
	Revisar y actualizar la resolución vigente que adopta el (SGSI) Sistema de Gestión de Seguridad de la Información, la política general de seguridad y el manual de políticas de seguridad.	• Borrador de resolución que simplifique y consolide todas las resoluciones existentes en materia de seguridad de la información. • Resolución aprobada mediante el trámite correspondiente.
Gestión de riesgos	Revisar y actualizar la política para administración de riesgos de la SNR, para incorporar los riesgos de seguridad de la información.	Política de Administración de Riesgos de la SNR actualizada, incluyendo los riesgos de seguridad digital dentro de su alcance.
	Establecer los lineamientos e instrumentos necesarios para la generación de los inventarios de activos de información en la entidad.	• Manual/Guía para la gestión de activos de información. • Formato para Inventario de Activos de información actualizado.

ESTRATEGIA/ EJE	ACTIVIDADES/PROYECTOS	PRODUCTOS ESPERADOS
	Acompañar a los líderes de los procesos para generar los inventarios de activos de información para cada uno de los procesos de la entidad.	• Inventarios de activos de información debidamente definidos en todos los procesos.
	Acompañar a los líderes de los procesos para generar las matrices de información para cada uno de los procesos de la entidad.	• Matrices de riesgos de seguridad de la información definidos en todos los procesos.
Cultura de seguridad de la información	Formular el Plan de Comunicación y Sensibilización en Seguridad de la Información	Plan de Comunicación y Sensibilización en Seguridad de la Información debidamente establecido y formalizado con la oficina de comunicaciones y la OTI.
	Sensibilizar al Personal respecto a los aspectos principales del Sistema de Gestión de Seguridad de la Información	Sesiones de sensibilización y comunicación ejecutadas con el personal de la SNR. Personal con conocimientos en las políticas de seguridad vigentes en la SNR. Personal con conocimientos en ataques y amenazas comunes, que pueden afectar la entidad.
	Realizar ejercicios de ingeniería social en ambientes controlados	Ejercicios de ingeniería social que generen oportunidades de mejora o métricas que contribuyan al SGSI.
	Formular el indicador de concientización	Indicador relacionado con el conocimiento de las políticas de seguridad por parte del personal

ESTRATEGIA/ EJE	ACTIVIDADES/PROYECTOS	PRODUCTOS ESPERADOS
		de la SNR o relacionado con las pruebas de ingeniería social ejecutadas.
Implementación de controles	Renovación de mantenimiento garantía y soporte de infraestructura de seguridad Perimetral (Firewalls) (Centro Alterno y Principal)	Infraestructura de seguridad debidamente asegurada con soporte y garantía durante las vigencias siguientes. Documentos y lineamientos del SGSI liberados y apropiados.
	Generación y actualización de documentación del SGSI de la entidad (Controles criptográficos, Control de acceso lógico, Información en tránsito, control de acceso físico, gestión de proveedores de TI, adquisición desarrollo y mantenimiento de software, gestión de vulnerabilidades técnicas, monitoreo, gestión y monitoreo de logs, Gestión de Cambios, Mantenimiento, Reutilización y baja de equipos y gestión de ambientes)	
	Adquisición de licencias o software de uso específico para VPN	Software de VPN con conexiones estables y flexibles para control de acceso remoto adecuado.
	Renovación de mantenimiento garantía y soporte de equipos WAF (Firewalls de aplicaciones web)	Infraestructura de protección WAF debidamente asegurada con soporte y garantía durante las vigencias siguientes.
	Adquisición y renovación de licenciamiento de EndPoint (Antivirus avanzado)	Equipos de cómputo protegidos con solución de endpoint avanzado.

ESTRATEGIA/ EJE	ACTIVIDADES/PROYECTOS	PRODUCTOS ESPERADOS
	Adquisición de equipo o licenciamiento proxy (Filtrado de contenido WEB)	Navegación controlada con base a perfiles y necesidades de la entidad, disminuyendo la probabilidad de filtración de información y/o incidentes por malware.
	Implementación Solución NAC	Control de acceso a la red corporativa más estricto, permitiendo únicamente equipos de cómputo que cumplan con estrictas normas de seguridad.
	Ejecución de ejercicios de Ethical Hacking y Remediación para los sistemas de información críticos de la SNR	Ejercicios de Ethical Hacking que permitan identificar brechas de seguridad de manera oportuna, junto a servicio de remediación que ayude a la mitigación de los hallazgos.
	Adquisición de solución para protección de correos electrónicos	Correos electrónicos protegidos ante ataques de phishing y malware que puedan afectar la seguridad de la información y la infraestructura de la entidad.
	Adquisición de servicio SOC/NOC (Servicio de monitoreo y respuesta	Servicio NOC/SOC que permita realizar un monitoreo 7/24 de la infraestructura tecnológica y que permita identificar tempranamente incidentes o eventos de seguridad.
	Adquisición e Implementación de sistema detección y respuesta de la red (NDR)	Sistema NDR implementado, el cual permite identificar movimientos laterales y posibles incidentes de seguridad, tráfico anómalo y

ESTRATEGIA/ EJE	ACTIVIDADES/PROYECTOS	PRODUCTOS ESPERADOS
	Adquisición e Implementación de sistema AntiDDoS (Sistema Anti-Denegación de Servicio).	Sistema AntiDDoS que proteja los principales servicios digitales ofrecidos a la ciudadanía de ataques de denegación.
	Implementación de servicios de seguridad para Infraestructura IAAS - SNR	Controles de seguridad establecidos en la nube de la SNR, que incluyan servicios de Firewall, WAF, AntiDDoS que protejan los servicios allí alojados.
Gestión de incidentes	Actualizar el procedimiento de Gestión de Incidentes de seguridad de la información, adaptándolo a las necesidades de la entidad.	Procedimiento y manual de gestión de incidentes de seguridad de la información.
	Ejecutar proceso de designación de responsabilidades en la gestión de incidentes y ejecutar la apropiación de los lineamientos y procedimientos.	Roles de gestión de incidentes formalmente establecidos y lineamientos apropiados en la entidad.
	Ejecución de simulacros de incidente de seguridad para verificar respuesta por parte del equipo de TICs.	Documentación de simulacro de incidente debidamente documentado.

7.2. CRONOGRAMA DE ACTIVIDADES / PROYECTOS

Con base a los proyectos definidos en la sección anterior, se establece el siguiente cronograma de actividades donde se evidencie como se llevarán a cabo cada uno de los proyectos previstos. Las actividades podrán desarrollarse de forma secuencial o paralela según se considere.

<table>
<tr><th colspan="3">AÑO 2024</th><th colspan="2">AÑO 2025</th><th colspan="2">AÑO 2026</th></tr>
<tr><th colspan="2">SEMESTRE 1</th><th>SEMESTRE 2</th><th>SEMESTRE 1</th><th>SEMESTRE 2</th><th>SEMESTRE 1</th><th>SEMESTRE 2</th></tr>
<tr><td rowspan="2">Realizar diagnóstico de seguridad de la información y establecer</td><td rowspan="2">Generar Plan Estratégico de Seguridad y Privacidad de la Información</td><td colspan="5">Mantener actualizado el diagnóstico de seguridad y privacidad de la información</td></tr>
<tr><td colspan="5">Ejecutar, actualizar y mantener informada a la alta dirección del avance de implementación del Plan Estratégico de Seguridad de la Información</td></tr>
<tr><td colspan="2">Actualizar la Política General de Seguridad de la Información y sus políticas.</td><td>Divulgación y apropiación de lineamientos y políticas de seguridad al personal de la entidad</td><td colspan="2">Mantenimiento y mejora continua de política general y especificas</td><td rowspan="4">Realizar preauditoria externa al SGSI</td><td rowspan="4">Implementación de planes de acción para preparación auditoria certificación.</td></tr>
<tr><td colspan="2">Establecer estructura de roles del SGSI enmarcado en las buenas prácticas para gestión de tecnología de la información</td><td colspan="3">Realizar apropiación de roles del Sistema de Gestión de Seguridad de la Información</td></tr>
<tr><td colspan="3">Iniciar el proceso de actualización de procedimientos y documentación del SGSI y documentos de TI con base a las buenas practicas</td><td>Divulgación y apropiación de documentos actualizados</td><td rowspan="3">Mantenimiento y mejora continua de los documentos del SGSI</td></tr>
<tr><td colspan="4">Establecer procedimientos o documentación faltante para dar cumplimiento a los dominios y controles del MSPI y norma ISO 27001</td></tr>
<tr><td colspan="4">Divulgación y apropiación de nuevos documentos</td><td colspan="2"></td></tr>
<tr><td colspan="2">Actualizar procedimiento y manual para gestión de activos de seguridad de la información.</td><td colspan="2" rowspan="2">Realizar capacitación y apropiación de metodología de riesgos y gestión de activos de seguridad digital</td><td colspan="3" rowspan="2">Realizar las actividades de apoyo para que los procesos puedan identificar, clasificar y valorar los activos y los riesgos de seguridad de la información.</td></tr>
<tr><td colspan="2">Crear procedimiento para gestión de riesgos de seguridad digital o integrar los mismos a la política integral de riesgos de la entidad de acuerdo con los lineamientos vigentes emitidos por el Departamento Administrativo de la Función Pública.</td></tr>
</table>

<table>
<tr><th colspan="2">AÑO 2024</th><th colspan="3">AÑO 2025</th><th colspan="2">AÑO 2026</th></tr>
<tr><th>SEMESTRE 1</th><th>SEMESTRE 2</th><th>SEMESTRE 1</th><th colspan="2">SEMESTRE 2</th><th>SEMESTRE 1</th><th>SEMESTRE 2</th></tr>
<tr><td rowspan="3">Actualizar procedimiento para gestión de copias de respaldo y manual de estrategias de recuperación</td><td rowspan="3">Ejecutar pruebas de restauración de servicios</td><td colspan="5">Ejecución periódica de pruebas de restauración de respaldos y servicios.</td></tr>
<tr><td colspan="5">Verificación de cumplimiento de lineamientos y pruebas de recuperación.</td></tr>
<tr><td>Realización de Análisis de riesgos de disponibilidad – Etapa 1 Continuidad de Negocio</td><td>Realización de Análisis BIA – Etapa 2 continuidad de negocio</td><td>Realización de Plan de Continuidad de TI (DRP) – Etapa 3 continuidad de negocio</td><td>Ejecución de pruebas de continuidad de negocio (DRP)</td><td>Establecimiento de actividades mejora del DRP</td></tr>
<tr><td colspan="7">ACTIVIDADES PERIÓDICAS</td></tr>
<tr><td>Eliminar documentos de comunicación del SGSI del 2022 y generar nuevo plan de comunicación y concientización del SGSI 2024</td><td>Ejecutar evaluación de seguridad de la información para medición de cultura de seguridad organizacional</td><td>Actualizar plan de comunicación del SGSI para la vigencia, de acuerdo con las necesidades y resultado de evaluación de seguridad.</td><td colspan="2">Ejecutar evaluación de seguridad de la información para medición de cultura de seguridad organizacional</td><td>Actualizar plan de comunicación del SGSI para la vigencia, de acuerdo con las necesidades y resultado de evaluación de seguridad.</td><td>Ejecutar evaluación de seguridad de la información para medición de cultura de seguridad organizacional</td></tr>
<tr><td>-</td><td>-</td><td>Actualizar el Plan Estratégico de Seguridad de la Información con base a los PTR encontrados.</td><td colspan="2"></td><td>Actualizar el Plan Estratégico de Seguridad de la Información con base a los PTR encontrados.</td><td></td></tr>
<tr><td>-</td><td>Realizar ejercicios de ingeniería social (ataques controlados) a los funcionarios y contratistas de la agencia.</td><td>-</td><td colspan="2">Realizar ejercicios de ingeniería social (ataques controlados) a los funcionarios y contratistas de la agencia.</td><td>-</td><td>Realizar ejercicios de ingeniería social (ataques controlados) a los funcionarios y contratistas de la agencia.</td></tr>
<tr><td>-</td><td>Renovación de servicios de mantenimiento, soporte y garantía de infraestructura de seguridad.</td><td>-</td><td colspan="2">Renovación de servicios de mantenimiento, soporte y garantía de infraestructura de seguridad.</td><td>-</td><td>Renovación de servicios de mantenimiento, soporte y garantía de infraestructura de seguridad.</td></tr>
<tr><td>-</td><td colspan="6">Realizar jornadas de sensibilización en seguridad de la información para los colaboradores</td></tr>
<tr><td>-</td><td>Generar plan de análisis de vulnerabilidades técnicas</td><td>Ejecutar pruebas de vulnerabilidades técnicas de los sistemas de información y acompañamiento de remediación</td><td>Actualizar plan de análisis de vulnerabilidades técnicas</td><td colspan="2">Ejecutar pruebas de vulnerabilidades técnicas de los sistemas de información y acompañamiento de remediación</td><td>Actualizar plan de análisis de vulnerabilidades técnicas
Ejecutar pruebas de vulnerabilidades técnicas de los sistemas de información y acompañamiento de remediación
Actualizar plan de análisis de vulnerabilidades técnicas</td></tr>
<tr><td colspan="7">Ejecución de monitoreo y seguimiento</td></tr>
</table>

7.3. ANÁLISIS PRESUPUESTAL

Con base a los proyectos definidos en el cronograma de actividades, se establece el siguiente presupuesto aproximado por cada vigencia según los proyectos establecidos:

AÑO 2024		AÑO 2025		AÑO 2026	
PROYECTO	**Inversión**	**PROYECTO**	**Inversión**	**PROYECTO**	**Inversión**
Diseño, implementación y/o mantenimiento del SGSI	$ 233.400.000	Diseño, implementación y mantenimiento del SGSI	$ 245.000.000	Diseño, implementación y mantenimiento del SGSI	$ 260.000.000
Renovación de mantenimiento garantía y soporte de infraestructura de seguridad Perimetral (Firewalls) (Centro Alterno y Principal)	$1.517.552.160	Renovación de mantenimiento garantía y soporte de infraestructura de seguridad Perimetral (Firewalls)	$ 1.593.429.768	Renovación de mantenimiento garantía y soporte de infraestructura de seguridad Perimetral (Firewalls)	$ 1.673.101.256
Adquisición de licencias o software de uso específico para VPN	Incluido Renovación Perimetral	Renovación de licencias o software de uso específico para VPN	Incluido Renovación Perimetral	Renovación de licencias o software de uso específico para VPN	Incluido Renovación Perimetral
Adquisición o reemplazo de firewall MPLS	Paso a Firewall principal	Renovación o remplazo de firewall MPLS	Paso a Firewall principal	Renovación o remplazo de firewall MPLS	Paso a Firewall principal
Renovación de mantenimiento garantía y soporte de equipos WAF (Firewalls de aplicaciones web)	$ 822.311.280	Renovación de mantenimiento garantía y soporte de equipos WAF (Firewalls de aplicaciones web)	$ 863.426.844	Renovación de mantenimiento garantía y soporte de equipos WAF (Firewalls de aplicaciones web)	$ 906.598.186,2
Adquisición y renovación de licenciamiento de EndPoint (Antivirus avanzado) renovar 3500 y adquirir 1000 licencias adicionales	$ 665.619.500,00	Renovación de licenciamiento de faltante de EndPoint (Antivirus avanzado) renovar 3000 y adquirir 1000 licencias adicionales	$ 698.900.475,00	Renovación de licenciamiento de faltante de EndPoint (Antivirus avanzado) renovar 3000 y adquirir 1000 licencias adicionales	$ 733.845.498,75
Adquisición de equipo o licenciamiento proxy (Filtrado de contenido WEB)	Incluido Renovación Perimetral	Renovación de equipo o licenciamiento proxy (Filtrado de contenido WEB)	Incluido Renovación Perimetral	Renovación de equipo o licenciamiento proxy (Filtrado de contenido WEB)	Incluido Renovación Perimetral
Renovación de mantenimiento garantía y soporte de infraestructura de seguridad NAC (Equipo de control de acceso a la red)	$40.000.000	Renovación de mantenimiento garantía y soporte de infraestructura de seguridad	$42.000.000	Renovación de mantenimiento garantía y soporte de infraestructura	$44.100.000

AÑO 2024		AÑO 2025		AÑO 2026	
PROYECTO	**Inversión**	**PROYECTO**	**Inversión**	**PROYECTO**	**Inversión**
		NAC (Equipo de control de acceso a la red)		de seguridad NAC (Equipo de control de acceso a la red)	
Adquisición de licenciamiento para doble factor de autenticación Office 365	Inmerso en licenciamiento Microsoft	Renovación de licenciamiento para doble factor de autenticación Office 365	Inmerso en licenciamiento Microsoft	Adquisición de licenciamiento para doble factor de autenticación Office 365	Inmerso en licenciamiento Microsoft
Adquisición de licenciamiento Defender Office365 (950 buzones)	$142.832.880	Adquisición de licenciamiento Defender Office365 (4585 buzones)	$ 751.398.677	Adquisición de licenciamiento Defender Office365 (4585 buzones)	$ 751.398.677
Adquisición de servicio de prueba de ethical hacking y remediación	$220.000.000	Adquisición de servicio de prueba de ethical hacking y remediación	$231.000.000	Adquisición de servicio de prueba de ethical hacking y remediación	$242.550.000
Adquisición de servicios para fortalecimiento de seguridad nube	$40.000.000	Renovación de servicios para fortalecimiento de seguridad nube	Proyección de puesta en producción	Renovación de servicios para fortalecimiento de seguridad nube	Proyección de puesta en producción
Adquisición de escáner de vulnerabilidades	$50.000.000	Renovación de escáner de vulnerabilidades	$52.500.000	Renovación de escáner de vulnerabilidades y análisis de código estático	$55.125.000
		Adquisición de servicio análisis avanzado de amenazas	$350.000.000	Renovación de servicio análisis avanzado de amenazas	$350.000.000
		Adquisición e Implementación de sistema detección y respuesta de la red (NDR)	$350.000.000	Renovación de sistema detección y respuesta de la red (NDR)	$94.000.000
		Adquisición de servicio AntiDDoS (Sistema contra denegación de servicio)	$450.000.000	Renovación de servicio AntiDDoS (Sistema contra denegación de servicio)	$ 112.500.000
		Adquisición de servicio SOC/NOC (Servicio de monitoreo y respuesta	$250.000.000	Renovación de servicio SOC/NOC (Servicio de monitoreo y respuesta	$262.500.000
		Adquisición herramienta de análisis de código estático	$80.000.000	Renovación herramienta de análisis de código estático	$84.000.000
		Adquisición de firewall de base de datos	$600.000.000	Renovación de firewall de base de datos	$ 180.000.000,00
Presupuesto Aprox. Vigencia 2024	$3.805.715.820	**Presupuesto Aprox. Vigencia 2025**	$6.557.655.764	**Presupuesto Aprox. Vigencia 2026**	$5.748.718.617

Los controles de seguridad relacionados con productos de Azure o Microsoft (doble factor de autenticación, geolocalización y otros), vienen inmersos dentro del licenciamiento adquirido para el funcionamiento de la Oficina de Tecnologías de la Información, los aspectos de seguridad están incluidos en dichas suscripciones o licencias.

8. RESPONSABLES

Respecto al Plan Estratégico de Seguridad de la Información (PESI), se definen los siguientes responsables:

ROL	RESPONSABILIDADES
Comité Institucional de Gestión de Desempeño	• Revisar y aprobar el Plan Estratégico de Seguridad de la Información. • Hacer seguimiento a las actividades del PESI • Asegurar los recursos necesarios para implementar los controles o proyectos aprobados en el PESI
Oficial de Seguridad de la Información	• Realizar la implementación de las actividades de su pertinencia y hacer seguimiento a las actividades del PESI a cargo de otras áreas. • Informar al Jefe de la Oficina de Tecnología de la información y al CIGD respecto al avance en la ejecución del PESI.
Oficina de Tecnologías de la Información	• Realizar la implementación de las actividades/controles de su pertinencia. • Apoyar al Oficial de Seguridad de la Información en el despliegue y administración de las soluciones tecnológicas de seguridad para la protección de los activos de la entidad.

9. APROBACIÓN

El presente plan ha sido sometido a consideración y conocimiento de la alta dirección y el comité de gestión y desempeño institucional con el objetivo de ser aprobado y aplicado conforme a lo que aquí se define. (*La aprobación se dará por medio del acta de comité correspondiente*).

10. GLOSARIO DE TÉRMINOS

Activos de Seguridad de la Información: se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, documentos, soportes, edificios, personas...) que tenga valor para la organización.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Debilidad: Vulnerabilidad de un activo o control que puede ser explotada por una o más amenazas

Disponibilidad: Es uno de los pilares de la seguridad de la información y este indica que la información pueda estar accesible y utilizable cuando lo requiera un usuario autorizado.

Evento de seguridad de la información: Acontecimiento identificado en el estado de un sistema, servicio o red que indica un posible incumplimiento o falla en las políticas o controles de seguridad de la información o de una situación desconocida que puede ser relevante para la seguridad.

Integridad: Es uno de los pilares de la seguridad de la información y este conlleva el mantenimiento de la exactitud, completitud y confiabilidad de la información.

Incidente de seguridad de la información: Uno o una serie de eventos de seguridad de la información inesperados o no deseados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

VPN (Virtual Private Network): Conexión cifrada a través de Internet desde un dispositivo a una red. La conexión cifrada ayuda a garantizar que los datos confidenciales se transmitan de forma segura. Evita que personas no autorizadas espíen el tráfico y permite al usuario realizar el trabajo de forma remota.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

11. BIBLIOGRAFÍA

- Ministerio de Tecnologías de la Información y las Comunicaciones - Documento Maestro del Modelo de Seguridad y Privacidad de la Información - octubre 2021.
- Ministerio de Tecnologías de la Información y las Comunicaciones - Modelo Nacional de Gestión de Riesgos de Seguridad de la Información en Entidades – octubre 2021.

- Ministerio de Tecnologías de la Información y las Comunicaciones - Producto tipo: PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.
- Ministerio de Tecnologías de la Información y las Comunicaciones - Instrumento de Evaluación MSPI
- ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls

ELABORACIÓN Y APROBACIÓN			
ELABORÓ	**REVISIÓN METODOLOGICA**	**APROBÓ**	**Vo.Bo Oficina Asesora de Planeación**
Juan Carlos Valenzuela Buitrago Hugo Alejandro Casallas Larrota	Juan Camilo Guiran Sánchez	José Ricardo Acevedo Solarte Jefe Oficina de Tecnología de la Información Comité de Gestión y Desempeño Institucional	Mónica Yaneth Galvis García Coordinadora Grupo Arquitectura Organizacional y Mejoramiento Continuo de la Oficina Asesora De Planeación
Oficina de tecnología de la Información y las Comunicaciones	Oficina Asesora de Planeación		
Fecha: 10/05/2024	Fecha:10/05/2024	Fecha:26/06/2024	Fecha Aprobación: 26/06/2024