



**Superintendencia de
Notariado y Registro**



INFORME DE SEGUIMIENTO

POLITICAS DE GOBIERNO DIGITAL Y SEGURIDAD DIGITAL

OFICINA DE CONTROL INTERNO

OCTUBRE DE 2025



Superintendencia de Notariado y Registro

INFORME DE SEGUIMIENTO A LAS POLÍTICAS DE GOBIERNO DIGITAL Y SEGURIDAD DIGITAL EN LA SUPERINTENDENCIA DE NOTARIADO Y REGISTRO

OBJETIVO

Verificar el grado de cumplimiento, efectividad y alineación de las políticas de Gobierno Digital y Seguridad Digital en la Superintendencia, conforme a los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), el DAFP y las normas nacionales vigentes.

ALCANCE

El seguimiento a las políticas de Gobierno Digital y Seguridad Digital se realizó para el periodo comprendido del 1 de julio de 2024 al 30 de septiembre de 2025, en los habilitadores de Arquitectura, Cultura y Apropiación, Seguridad y Privacidad de la Información, Servicios Ciudadanos Digitales y la línea de acción de Servicios y Procesos Inteligentes.

RESPONSABLE DEL PROCESO, PROCEDIMIENTO O ACTIVIDAD EVALUADA

El proceso de Gestión de Tecnologías de la Información, Ing. Jose Ricardo Acevedo Solarte

CRITERIOS

- 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.”*
- Modelo Integrado de Planeación y Gestión – MIPG.
- Decreto 767 de mayo 16 de 2022: *“Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.*
- Decreto 338 de 2022, *“Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones”.*
- CONPES 3854 de 2016, *Política Nacional de Seguridad Digital.*
- Decreto 1078 de 2015. *“Por medio del cual se expide el decreto único reglamentario del sector de Tecnologías de la Información y las comunicaciones”, ARTÍCULO 2.2.9.1.4.1. “Seguimiento y Evaluación. El Ministerio de Tecnologías de la Información y las Comunicaciones adelantará el seguimiento a la implementación de la Política de Gobierno Digital, con la periodicidad y criterios de medición definidos por el Consejo para la Gestión y Desempeño institucional, o quien haga sus veces, en el marco de la operación estadística de Medición del Desempeño Institucional, o la que se defina en su lugar, y cuya fuente de datos es el Formulario Único de Reporte de Avance en la Gestión – FURAG”.*
- Directiva Presidencial 02 de 2022, para garantizar la implementación segura de la Política de Gobierno Digital liderada por el MINTIC.
- Resolución 2710 de 2017 y Resolución 1126 de 2021 del MINTIC, sobre la implementación del protocolo IPv6 en Colombia.



Superintendencia de Notariado y Registro

- Resolución No.4905 del 13 de mayo de 2016, por medio de la cual se adopta el Sistema de Gestión de la Seguridad de la Información, para realizar el seguimiento de seguridad a nivel integral sobre procesos, procedimientos y sistemas de información.
- *Plan Estratégico de Tecnologías de la Información 2024 – 2026 de la SNR.*
- *Plan Estratégico de Seguridad y Privacidad de la Información 2024 – 2026 de la SNR.*
- *Manual Interno -Manual de Políticas de Seguridad y Privacidad de la Información de la SNR.*

METODOLOGÍA

Durante el desarrollo del proceso de seguimiento, se aplicaron de manera sistemática las técnicas de auditoría normalmente aceptadas, conforme a los lineamientos establecidos por las Normas Internacionales de Auditoría; las cuales permitieron obtener evidencias suficientes, competentes y pertinentes que respaldan los hallazgos y conclusiones del proceso.

Este seguimiento se desarrolló de la siguiente manera:

- Solicitud de información del avance alcanzado para el periodo de seguimiento.
- Análisis comparativo de la información relacionada con los componentes del alcance, con respecto a los lineamientos y guías de las Políticas de Gobierno Digital y Seguridad Digital.
- Revisión documental y de informes que permitieron soportar los avances alcanzados en las políticas.
- Verificación de la documentación existente en la página web y la intranet de la SNR.
- Revisión de los resultados de la entidad en el FURAG para la vigencia 2024, en las políticas de gobierno digital y seguridad digital.
- Revisiones documentales indirectas y análisis comparativos.
- Esta actividad se desarrolló a través del método de observación directa, entrevistas estructuradas, muestreo selectivo, verificación de la información de ejecución de las actividades evaluadas y las pruebas de cumplimiento y de control.

LIMITACIONES

Se presentaron limitaciones derivadas de la falta de respuesta oportuna por parte de algunas áreas o responsables institucionales.

DESARROLLO DEL SEGUIMIENTO

Con el seguimiento a las políticas de **Gobierno Digital y Seguridad Digital** la Oficina de Control Interno contribuye a fortalecer la gestión institucional, verificando el avance alcanzado por la SNR hacia una transformación digital segura, eficiente y transparente; A través de la evaluación continua del cumplimiento normativo y la verificación de la efectividad de las acciones implementadas, se consolidan prácticas que garantizan la protección de la información, la confianza ciudadana y la interoperabilidad entre entidades del Estado, fomentando una cultura de mejora continua, orientada a la sostenibilidad y al cumplimiento de los lineamientos establecidos por el MINTIC, el DAFP y el Marco de Referencia de Arquitectura Empresarial del Estado.

1. Contexto de las Políticas de Gobierno Digital y Seguridad Digital

[La Política de Gobierno Digital](#), es el instrumento gubernamental del orden nacional que propende por la transformación digital pública. Con esta política pública se busca fortalecer la relación Ciudadano - Estado, mejorando la prestación de servicios por parte de las entidades, y generando confianza en las instituciones que conforman la administración pública; a través del uso y aprovechamiento de las TIC. La PGD hace parte del



Superintendencia de Notariado y Registro

Modelo Integrado de Planeación y Gestión - MIPG y se integra con las políticas de gestión y desempeño institucional.

Objetivo Política, Impactar positivamente la calidad de vida de los ciudadanos y, en general, los habitantes del territorio nacional y la competitividad del país, promoviendo la generación de valor público a través de la transformación digital del Estado, de manera proactiva, confiable, articulada y colaborativa entre los Grupos de Interés y permitir el ejercicio de los derechos de los usuarios del ciberespacio.

La Política de Seguridad Digital, tiene como propósito fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, así como en la creación e implementación de instrumentos de resiliencia, recuperación y respuesta nacional en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país

El objetivo general de esta política es que los colombianos y las empresas conozcan e identifiquen los riesgos a los que están expuestos en el entorno digital y aprendan como protegerse, prevenir y reaccionar ante los delitos y ataques cibernéticos.

Lo anterior, según lo establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones.

Para la implementación de las Políticas de Gobierno Digital y de Seguridad Digital, se cuenta con documentos y herramientas del Ministerio de Tecnologías de la Información y las Comunicaciones y el Departamento Administrativo de la Función Pública.

La siguiente ilustración, representa los lineamientos del decreto 767 de 2022, para la implementación de la Política de Gobierno Digital y Seguridad Digital, la cual se estructura en Elementos Transversales, Habilitadores, líneas de acción e iniciativas dinamizadoras.

Figura 1 – Estructura de la Política de Gobierno Digital



Fuente: MINTIC - Fuente: <https://gobiernodigital.mintic.gov.co>



Superintendencia de Notariado y Registro

1.1. Elementos transversales: Los elementos transversales corresponden a la Gobernanza y la Innovación Pública Digital.

La Gobernanza, es un elemento transversal que busca desarrollar la implementación de la Política de Gobierno Digital bajo un modelo de gobernanza basado en el relacionamiento entre el orden nacional y territorial, y el nivel central y descentralizado involucrando a los grupos de interés en la toma de decisiones.

La Innovación Pública Digital, busca desarrollar la implementación de la Política de Gobierno Digital con un enfoque transversal basado en el relacionamiento de los grupos de interés, generando valor público a través de la introducción de soluciones novedosas, creativas y que hagan uso de las Tecnologías de la Información y las Comunicaciones.

1.1.2 Habilitadores: Las Políticas de Gobierno Digital y Seguridad Digital se ejecutan a través de cuatro (4) habilitadores transversales, como son:

Arquitectura: Desarrolla capacidades para el fortalecimiento institucional implementando el enfoque de arquitectura empresarial en la gestión, gobierno y desarrollo de los proyectos con componentes de tecnologías de la información.

Cultura y Apropiación: Busca desarrollar capacidades para el acceso, uso y aprovechamiento de Tecnologías de la Información y las Comunicaciones y busca promover el uso y apropiación de estas, entre las personas en situación de discapacidad y fomenta la inclusión con enfoque diferencial.

Seguridad y Privacidad de la Información: Busca desarrollar capacidades para la seguridad y privacidad de la información, en todos los activos de información con el fin de preservar la confidencialidad, integridad y disponibilidad de los datos.

Servicios Ciudadanos Digitales: Este habilitador busca desarrollar mediante soluciones tecnológicas, las capacidades para mejorar la interacción con la ciudadanía.

Servicios y procesos inteligentes: Esta es una línea de acción, que busca desarrollar servicios y procesos digitales, automatizados, accesibles, adaptativos y basados en criterios de calidad a partir del entendimiento de las necesidades del usuario y su experiencia, implementando esquemas de atención productiva y el uso de tecnologías emergentes. *Fuente: <https://gobiernodigital.mintic.gov.co>*

2. Resultados del Seguimiento

Con las definiciones descritas para el marco de las políticas de gobierno digital y seguridad digital, se abordarán los resultados de la revisión documental aportada por el proceso líder de las políticas y de las iniciativas de transformación digital en la Superintendencia.

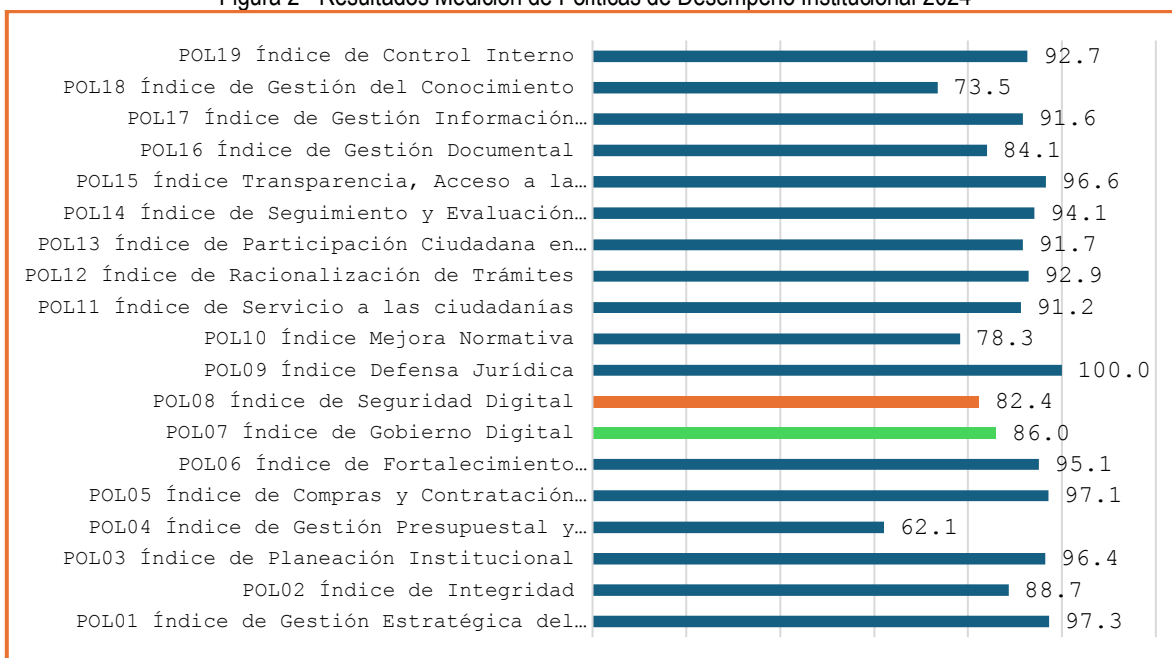
2.1. Verificación realizada a los resultados del Formulario Único Reporte de Avances de la Gestión SNR - FURAG 2024

En la siguiente gráfica se presentan los resultados del FURAG 2024, para la Superintendencia, en las políticas de Gobierno Digital con una calificación de 86.0 y Seguridad Digital con 82.4.



Superintendencia de Notariado y Registro

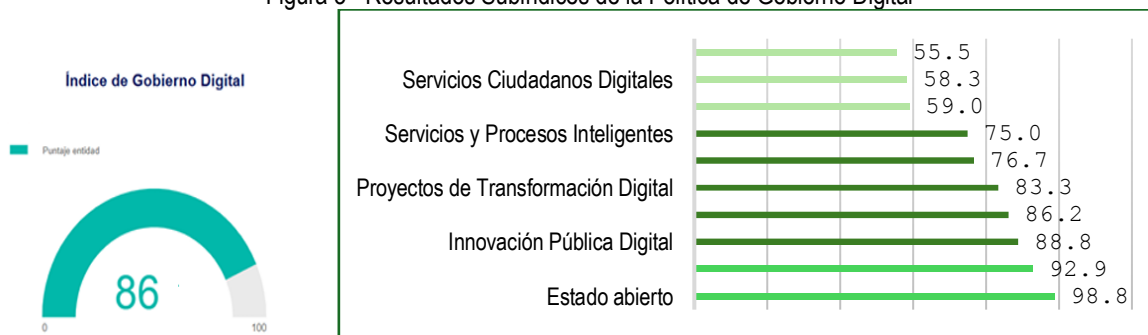
Figura 2 - Resultados Medición de Políticas de Desempeño Institucional 2024



Fuente. Elaboración propia con datos del FURAG 2024 – DAFP

A continuación, se presentan los resultados obtenidos por cada subíndice de la política de Gobierno Digital para la vigencia 2024:

Figura 3 - Resultados Subíndices de la Política de Gobierno Digital



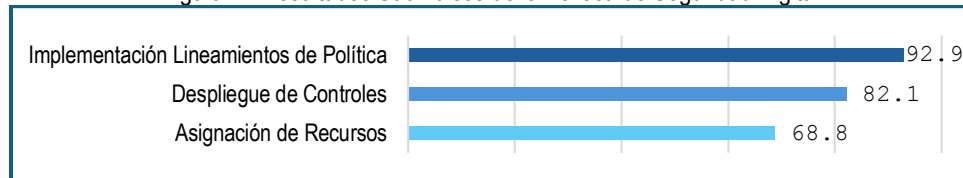
Fuente. Elaboración propia con datos del FURAG 2024 – DAFP -Mediciones Índice de Gobierno Digital

La medición de los subíndices de la Política de Gobierno Digital permite identificar que la Superintendencia obtuvo un puntaje de 86,0 en el índice de Gobierno Digital. Los índices que presentan un mayor puntaje corresponden a Estado Abierto y Cultura y Apropiación con 98,8 y 92,9 puntos respectivamente y los tres menores puntajes corresponden a Gobernanza (55,5); Servicios Ciudadanos Digitales (58,3) y Seguridad y Privacidad de la Información (59) puntos.



Superintendencia de Notariado y Registro

Figura 4 - Resultados Subíndices de la Política de Seguridad Digital



Fuente. Elaboración propia con datos del FURAG 2024 – DAFP -Mediciones Índice de Gobierno Digital

La entidad obtuvo un puntaje de 82,4 en el índice de Seguridad Digital. Los índices que presentan un mayor puntaje corresponden a Implementación Lineamientos de Política con 92,9 puntos y el menor puntaje corresponde a Asignación de Recursos con 68,8 puntos.

2.2. Verificación realizada al cumplimiento de elementos transversales de Gobernanza e Innovación Pública Digital, como referentes de las Políticas de Gobierno Digital y Seguridad Digital.

A continuación, se relacionan los principales resultados identificados en la evaluación y análisis de cada habilitador y línea de acción de las políticas de gobierno y seguridad digital, realizado por la Oficina de Control Interno para el periodo comprendido entre el 1 de julio de 2024 al 30 de septiembre de 2025, tomando como base los soportes documentales presentados por la Oficina de Tecnologías de la Información y los registros documentales existentes en el portal web.



a. PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI

El PETI es una herramienta estratégica que el Gobierno nacional, a través del Ministerio TIC, promueve para que las entidades públicas guíen sus esfuerzos tecnológicos.

Objetivo General PETI: “Formular y presentar el Plan Estratégico de Tecnologías de la Información (PETI) para el periodo 2024-2026 de la Superintendencia de Notariado y Registro (SNR), con una propuesta de proyectos de TI que contribuyan decisivamente a la Transformación Digital de la entidad. Este plan está orientado a impulsar el cumplimiento de su misión y la consecución de sus objetivos estratégicos, además de guiar a la entidad en la provisión de servicios digitales confiables y de alta calidad, fortaleciendo sus capacidades en el ámbito de Tecnologías de la Información.”

La gobernanza comprende los instrumentos, procesos y estructuras que orientan la gestión estratégica de las TI y el cumplimiento de los objetivos digitales del Estado; en este sentido, el PETI es precisamente el instrumento de planeación estratégica de TI que garantiza esa alineación institucional, definiendo inversiones, proyectos, capacidades y prioridades digitales. El MINTIC por su parte, ubica el PETI como parte del marco de gobernanza de las TI, bajo la subdimensión “Dirección estratégica de TI”, dentro del componente de Gobierno Digital.

Al verificar el acto administrativo de aprobación del PETI 2024- 2026, se pudo evidenciar el Acta No.4 jun- 2025 del Comité Institucional de Gestión y Desempeño de la SNR, donde fue presentado y aprobado dicho plan. También se evidenció la publicación del PETI en la página web de la entidad, a través del Link: portal-peti_v2.pdf (supernotariado.gov.co).



Superintendencia de Notariado y Registro

Se observa que el PETI fue definido teniendo en cuenta las principales normas relacionadas con el accionar misional de la Entidad, el Sector de la Justicia, el Sector de las Tecnologías de la Información y las Comunicaciones, asociada a los temas de la Política de Gobierno Digital, Arquitectura de Información, el Modelo de Gestión Estratégica de TI y el Modelo integrado de Planeación y Gestión (MIPG).

En la revisión de la planeación institucional registrada a través del PETI 2024-2026, publicado en la página web de la SNR se evidenció que fueron subsanadas las observaciones emitidas en el informe de Seguimiento a las Políticas de Gobierno Digital y Seguridad Digital de la vigencia 2021, emitido por la Oficina de Control Interno, y reiterado en el seguimiento realizado en la vigencia 2024, respecto a la falta de indicadores para cada una de las iniciativas de inversión y falta de un plan de comunicaciones.

Una vez solicitada la hoja de ruta del PETI, se indicó por parte de la Oficina de TI que *“esta hoja de ruta corresponde a la planeación estratégica de iniciativas de TI y constituye un instrumento dinámico y evolutivo, sujeto a ajustes según la disponibilidad presupuestal, las prioridades institucionales y las condiciones del entorno. Los proyectos definidos representan las iniciativas clave previstas para el año 2026 y han sido priorizados para fortalecer la gobernanza de datos, automatizar trámites y servicios, mejorar la experiencia del ciudadano, consolidar una infraestructura tecnológica resiliente y optimizar la gestión de proyectos de TI.*

Es importante señalar que el presupuesto estimado para cada iniciativa fue calculado con base en el juicio de expertos y entregado por la consultoría especializada, por lo cual constituye una referencia técnica que podrá ser refinada en las fases de estructuración y viabilización financiera. No obstante, algunas iniciativas ya han iniciado su ejecución de manera anticipada; por ejemplo, la herramienta de satisfacción de ciudadanos basada en inteligencia artificial, para la cual se está definiendo el alcance funcional y el modelo de IA a implementar, con el propósito de construir un Producto Mínimo Viable (PMV).”

Así mismo, manifestaron que las actividades están alineadas con la planeación institucional, a través del Plan Anual de Acción, que al ser revisado presentó el siguiente avance, durante el primer y segundo trimestre de 2025, acorde con el Informe Plan Anual de Acción 2025, que corresponde al seguimiento realizado por la Oficina Asesora de Planeación:

Tabla No. 1 – Resultados del seguimiento realizado a los Planes OTI

Primer Trimestre de 2025

Resultados Planes Decreto 612 (Primer trimestre 2025)

Código	Decreto 612	# Actividades I trimestre	% Ejecución
PH0	Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI	3	100% ●
PH1	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	N/A	N/A
PH2	Plan de Seguridad y Privacidad de la Información	N/A	N/A

Resultados Otros Planes (Primer trimestre 2025)

Otros planes	# Actividades I trimestre	% Ejecución
Plan de transformación digital	2	100% ●

Segundo Trimestre de 2025



Superintendencia de Notariado y Registro

Resultados Proyectos de Inversión (Segundo trimestre 2025)

Código	Proyecto	# Actividades II trimestre	% Ejecución
Pi_02	Fortalecimiento Tecnológico Hacia la Transformación Digital de la SNR a Nivel Nacional	6	100% ●

Resultados Planes Decreto 612 (Segundo trimestre 2025)

Código	Decreto 612	# Actividades II trimestre	% Ejecución
PI10	Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI	8	100% ●
PI11	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	1	100% ●
PI12	Plan de Seguridad y Privacidad de la Información	2	100% ●

Resultados Otros Planes (Segundo trimestre 2025)

Otros planes	# Actividades II trimestre	% Ejecución
Plan de transformación digital	5	100% ●

Fuente: OAP - SNR, Informe Plan Anual de Acción primer y segundo trimestre de 2025

Como se observa en la Tabla 1, La Oficina de Tecnologías de la Información de la SNR ha establecido acciones que han sido ejecutadas al 100% de enero a junio de 2025; la OTI planificó un total de 27 actividades, de las cuales 11 están asociadas al PETI; 1 actividad asociada al Plan de tratamiento de riesgos de seguridad y privacidad de la información; 2 actividades asociadas al Plan de seguridad y privacidad de la información; 7 actividades asociadas al Plan de Transformación Digital y 6 actividades asociadas al Fortalecimiento Tecnológico hacia la transformación digital de la SNR a nivel nacional.

El diseño y seguimiento de estos indicadores permiten a la SNR evaluar el progreso en la implementación de sus iniciativas tecnológicas, alineadas con las Políticas de Gobierno y Seguridad Digital. Así, los indicadores funcionan como mecanismos de control y gestión, reflejando la eficiencia, efectividad y calidad de las actividades vinculadas al PETI, y de manera general a todos los planes que desde la OTI se lideran.



b. DOMINIO ARQUITECTURA DE GESTIÓN DE TI

El PETI define un portafolio de proyectos estratégicos, una hoja de ruta clara para la implementación de los proyectos y unas metas organizadas a corto, mediano y largo plazo. Este plan, sigue los lineamientos y parámetros del Marco de Referencia de Arquitectura Empresarial de Gestión TI (MRAE) y en línea con la Política de Gobierno Digital propuesta por el Ministerio de Tecnologías de la Información y las Comunicaciones



Superintendencia de Notariado y Registro

(MINTIC), como un instrumento clave para impulsar la modernización y eficiencia de la SNR, contribuyendo significativamente al cumplimiento de los objetivos estratégicos institucionales.¹

Por su parte, la Oficina de Tecnologías de la Información de la SNR como respuesta a la solicitud realizada por la Oficina de Control Interno para este literal revisado, contestó lo siguiente:

“Se han venido adelantando ejercicios de Arquitectura Empresarial en el marco de la estrategia institucional de transformación digital. Dichos ejercicios se desarrollan con base en los lineamientos establecidos por la Política de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones, los cuales buscan garantizar la alineación entre los objetivos estratégicos de la entidad, sus procesos misionales y de apoyo, y el uso eficiente de las tecnologías de la información.

De manera particular, el habilitador de Arquitectura se integra con el Sistema de Gestión existente en la SNR mediante la articulación de los modelos de procesos, información, aplicaciones y tecnología con los componentes del Sistema, lo que permite:

- *Fortalecer la trazabilidad entre los objetivos institucionales, los proyectos de TI y los resultados de gestión.*
- *Incorporar prácticas de estandarización, interoperabilidad y seguridad digital dentro de los procedimientos del Sistema de Gestión.*
- *Asegurar que las iniciativas tecnológicas se evalúen y prioricen conforme a criterios de eficiencia, eficacia y cumplimiento normativo definidos en la Política de Gobierno Digital y en el Modelo Integrado de Planeación y Gestión – MIPG.*

De esta forma, la entidad garantiza que los avances en Arquitectura Empresarial no son esfuerzos aislados, sino que constituyen un habilitador transversal para la consolidación del Sistema de Gestión, en coherencia con la ruta definida por el Gobierno Digital.”

Así mismo, presentó como evidencias de avance la autoevaluación de madurez de la Arquitectura Empresarial realizada por la Oficina de Tecnologías de la Información en la SNR, para el segundo semestre del año 2024, según el Instrumento de Evaluación del Nivel de Madurez – MRAE enviado, cuyo objetivo de la herramienta consiste en *“brindar una herramienta para el desarrollo de ejercicios de evaluación de la madurez integral en del desarrollo de la AE, la gestión y gobierno de TI y la gestión de los proyectos de TI, teniendo en cuenta como criterios de evaluación las definiciones contenidas en los tres modelos del Marco de Referencia de Arquitectura Empresarial del Estado.”*

Al respecto se evidenció que el ejercicio de arquitectura realizado en la entidad y documentado a través del análisis de los diferentes elementos constituye un **insumo estratégico esencial para la gestión institucional**, al permitir comprender de manera integral la relación entre los procesos misionales, la información, las aplicaciones y la infraestructura tecnológica existente en la SNR.

Su debida implementación permitirá fortalecer la **eficiencia operativa**, el **cumplimiento normativo**, como el Decreto 767 de 2022, el Manual de Gobierno Digital, la Resolución 1519 de 2020 - resolución que establece lineamientos para el gobierno digital en Colombia y dentro de la cual se detallan aspectos como:

- Diseño de sedes electrónicas.
- Lineamientos de accesibilidad.
- Estándares de seguridad y divulgación.
- Requisitos mínimos para datos abiertos.

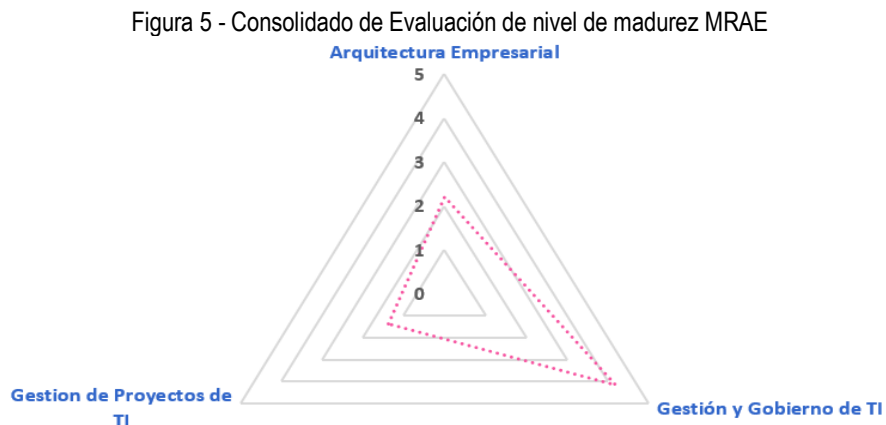
¹ PETI SNR 2024-2026



Superintendencia de Notariado y Registro

Este ejercicio realizado permitirá también la **toma de decisiones basadas en evidencia**, asegurando que los recursos tecnológicos se orienten al logro de los objetivos institucionales y a la mejora del servicio al ciudadano. En este sentido, proporciona una **visión articulada y actualizada del entorno tecnológico de la SNR**, que sirve como base para optimizar inversiones, garantizar la seguridad de la información y promover la interoperabilidad entre las entidades públicas.

A continuación, se presenta la gráfica de resultados de la autoevaluación realizada y consolidada, permitiendo conocer el nivel de madurez existente para los tres modelos: Arquitectura Empresarial, Gestión y Gobierno de TI, y Gestión de Proyectos de TI.



Fuente: Autodiagnóstico OTI, II sem.2024 - Presentación de resultados 0.MRAE

Según el análisis de evaluación de madurez presentado en la figura 5, la superintendencia obtuvo un puntaje de **2.21** para **Arquitectura Empresarial**; de **4,18** para **Gestión y Gobierno de TI**; y de **1.38** para **Gestión de Proyectos de TI**; por lo que la entidad presenta un total promedio del **nivel de madurez MRAE de 2,59**, lo que indica un avance moderado en la implementación de la arquitectura institucional, donde, si bien es cierto se han establecido prácticas y se cuenta con procesos en marcha, aún existen actividades que requieren un desarrollo más sistemático y formalizado para alcanzar un estado más robusto y estratégico; a continuación se presenta el análisis respectivo.

Análisis por componentes

Arquitectura Empresarial: Puntaje de 2,21

Este puntaje sugiere que la SNR ha comenzado a definir y documentar su arquitectura en un nivel inicial, donde se han identificado los componentes clave (arquitectura de negocio, de datos, de aplicaciones y de tecnología) y se han realizado algunos esfuerzos de estandarización, pero aún no se ha logrado una integración completa con la estrategia institucional.

Se recomienda fortalecer la articulación de la arquitectura con los objetivos de negocio y madurar los procesos de gestión del conocimiento relacionados con la misma.

Gestión y Gobierno de TI: Puntaje de 4,18

Este es el componente más sólido de la evaluación, lo que demuestra un alto grado de madurez en la gestión y el gobierno de TI. Según los rangos, un puntaje superior a 4 indica que la entidad no solo cuenta con políticas y procesos formales, sino que también realiza un seguimiento efectivo y utiliza la información para la toma de decisiones estratégicas. Con esta fortaleza la OTI se puede apalancar para impulsar la madurez de las otras



Superintendencia de Notariado y Registro

áreas, utilizando la sólida estructura de gobierno para formalizar y mejorar los procesos de arquitectura y gestión de proyectos.

Gestión de Proyectos de TI: Puntaje de 1,38

El puntaje obtenido indica una debilidad significativa. Una calificación tan baja sugiere que la gestión de proyectos de TI se encuentra en una etapa incipiente, es decir, con procesos poco formalizados o documentados. Esto puede generar ineficiencias, retrasos y una mayor probabilidad de que los proyectos no cumplan con los objetivos establecidos en la SNR.

Por lo anterior, se sugiere establecer como una prioridad crítica para mejorar este componente, donde se logre implementar y formalizar una metodología estándar para la gestión de proyectos de TI, asegurando que todos los proyectos de arquitectura empresarial se planifiquen, ejecuten y controlen de manera rigurosa.

De manera general la entidad tiene una base sólida en la Gestión y Gobierno de TI, lo cual debe ser el motor para impulsar la mejora en los demás componentes que obtuvieron una baja calificación. El principal desafío reside en la Gestión de Proyectos de TI, que requiere de una atención inmediata para estandarizar procedimientos y asegurar la correcta implementación de las iniciativas plasmadas a través del PETI. La Arquitectura Empresarial necesita un desarrollo continuo para pasar de una fase de “gestionado” a una plena integración estratégica con el negocio, de tal forma que se alcance la fase de “manejado” y/o “optimizado”.

Igualmente se presentó como evidencias el “Documento TOBE V0.1”, que contiene la “Arquitectura Objetivo para la transformación digital del proceso de Registro de instrumentos Públicos”, realizado con corte a noviembre de 2024, importante documento que proporciona un destino claro para la mejora del proceso y lo pone con una visión de futuro, traducido en un plan de acción concreto y ejecutable; esto permite pasar de la identificación de problemas, a la planificación de soluciones eficientes y rentables.

La Arquitectura Objetivo para alineación estratégica entre tecnología y el negocio de la SNR busca establecer una estructura sólida y coherente que permita la modernización de sus procesos y sistemas, alineándolos con los objetivos estratégicos de la entidad. Este plan incluye una serie de estrategias y cambios en diversos dominios clave, incluyendo el negocio, los datos, los sistemas de información, la infraestructura y la seguridad, así como el uso y la apropiación tecnológica. De esta manera, se pretende crear una base tecnológica robusta que soporte las iniciativas de transformación digital, mejorando la eficiencia operativa y la capacidad de respuesta de la SNR frente a los desafíos actuales y futuros.²

Con este documento se busca guiar la transformación; fomentar la colaboración y la alineación con las partes interesadas, asegurando que todos los involucrados entiendan y se comprometan con el mismo objetivo de mejora, facilitando así la gestión del cambio; se justifica la inversión facilitando la toma de decisiones informadas sobre la asignación de recursos necesarios para las iniciativas de mejora; este análisis proporciona una visión general de las brechas y sus posibles soluciones, las cuales se recomienda tener presentes para mejorar la eficiencia, seguridad y resiliencia de la infraestructura tecnológica de la entidad.

No obstante, los resultados obtenidos y como lo menciona la Oficina de Tecnologías de la Información, estos insumos constituyen soporte técnico y documental que reflejan el nivel de avance institucional en materia de Arquitectura en la SNR, y evidencian su aporte directo al habilitador de Arquitectura definido en la Política de Gobierno Digital. Se sugiere consolidar el equipo de apoyo de Arquitectura Empresarial, para desarrollar los proyectos o iniciativas que tienen previstos los procesos misionales, y realizar permanentes divulgaciones del apoyo que este equipo puede realizar a toda la entidad, y para los procesos que así lo requieran.

² Documento TOBEV0.1, numeral 2-Arquitectura Institucional



Superintendencia de Notariado y Registro

También se **recomienda** utilizar de manera activa el análisis y la documentación elaborada como herramienta de planificación y gestión continua, logrando su integración en:

- La formulación del Plan Estratégico de Tecnologías de la Información (PETI) y del Plan de Gobierno Digital.
- Los procesos de adquisición, desarrollo o actualización de sistemas de información.
- Las acciones de fortalecimiento institucional y de cumplimiento del Modelo Integrado de Planeación y Gestión (MIPG).

Asimismo, se **sugiere** mantener actualizado el repositorio documental de arquitectura, garantizando que cada nuevo proyecto tecnológico sea evaluado y alineado con los lineamientos definidos, promoviendo una gestión pública moderna, interoperable y centrada en el ciudadano.

Normas que se cumplen con los literales de PETI y Arquitectura

Al optimizar los procesos de una entidad, se mejora la prestación de servicios, lo que genera mayor valor público y satisfacción para los ciudadanos, en cumplimiento del MIPG. La arquitectura empresarial y el PETI son herramientas clave para planificar, ejecutar y evaluar estos avances, y su implementación requiere una planificación estratégica que se plasma en este plan, con un enfoque de mejoramiento continuo.

-Decreto 767 de 2022, Política De Gobierno Digital, Elementos de la Política de Gobierno Digital

ARTÍCULO 2.2.9.1.2.1. Estructura. *“La Política de Gobierno Digital se desarrollará a través de un esquema que articula los elementos que la componen, a saber: gobernanza, innovación pública digital, habilitadores, líneas de acción, e iniciativas dinamizadoras, con el fin de lograr su objetivo, entendidos así:*

*... 3. **Habilitadores:** Los sujetos obligados desarrollarán las capacidades que les permitan ejecutar las Líneas de Acción de la Política de Gobierno Digital, mediante la implementación de los siguientes habilitadores:*

3.1. Arquitectura: *Este habilitador busca que los sujetos obligados desarrollen capacidades para el fortalecimiento institucional implementando el enfoque de arquitectura empresarial en la gestión, gobierno y desarrollo de proyectos con componentes de Tecnologías de la Información.*

Los sujetos obligados deberán articular su orientación estratégica, su modelo de gestión, su plan de transformación digital, y su estrategia de Tecnologías de información y las Comunicaciones, con el objetivo de dar cumplimiento a la Política de Gobierno Digital.

5. Iniciativas Dinamizadoras: *Comprende los Proyectos de Transformación Digital y las Estrategias de Ciudades y Territorios Inteligentes, a través de las cuales se materializan las Líneas de Acción, que permiten dar cumplimiento al objetivo de la Política de Gobierno Digital con la implementación de mecanismos de compra pública que promuevan la innovación pública digital.*

5.1. Proyectos de Transformación Digital: *Comprende aquellos proyectos que implementarán los sujetos obligados para aportar a la generación de valor público mediante el aprovechamiento de las capacidades que brindan el uso y la apropiación de las Tecnologías de la Información y las Comunicaciones y así alcanzar los objetivos estratégicos institucionales. Los proyectos de Transformación Digital deberán estar integrados al Plan Estratégico de Tecnología y Sistemas de Información (PETI).”*

-Decreto 338 de 2022: Gobernanza de la Seguridad Digital; Señala que la política de Seguridad Digital es una de las políticas de Gestión y Desempeño Institucional, y reitera que la política de Seguridad Digital forma



Superintendencia de Notariado y Registro

parte de la Política de Gobierno Digital. El PETI, al incluir los componentes de seguridad, asegura el cumplimiento de esta política dentro de la estrategia de la entidad.

c. DOMINIO CULTURA Y APROPIACIÓN DE TI

El fortalecimiento de la **Cultura y Apropiación de las Tecnologías de la Información (TI)** es un pilar esencial para garantizar el éxito de la transformación digital en la entidad y teniendo en cuenta que no es suficiente con disponer de infraestructura y sistemas modernos, se hace necesario que cada una de las personas que laboran en la SNR **comprendan, valoren y apliquen las buenas prácticas tecnológicas** en su trabajo diario, teniendo en cuenta que una cultura digital sólida impulsa la eficiencia institucional, la transparencia, la innovación y la seguridad de la información, promoviendo servidores públicos más competentes, colaborativos y conscientes del impacto de la tecnología en la calidad del servicio al ciudadano.

Por tanto, la apropiación tecnológica es un **proceso continuo de aprendizaje, sensibilización y mejora**, que debe estar presente en la gestión estratégica, operativa y humana de la entidad.

En la revisión documental realizada a la definición de la estrategia de Uso y Apropiación de los servicios y soluciones de tecnologías de la información en la superintendencia, se evidenció que la OTI cuenta con el documento **“CRONOGRAMA CAPACITACIONES INVITACION MINJUSTICIA”**, el cual se encuentra en ejecución de Junio a Noviembre de 2025, para ser desarrolladas bajo la modalidad virtual, con diversas actividades programadas como son: Charla virtual sobre Gestión de cambio a través de la Transformación Digital; Taller de Inteligencia Artificial en el Sector Justicia; Inteligencia artificial aplicado a herramientas ofimáticas; Taller de Ciberseguridad integrando la inteligencia artificial; métodos de ciberataque (Pishing, sexting cyberbullying, grooming, sextorsion, ciberespionaje); entre otros.

Así mismo, se evidenció que éste cronograma se ha trabajado de manera conjunta con el Ministerio de Justicia y del Derecho, como cabeza de sector, buscando que en la entidad se perciban efectivamente los beneficios y el valor de estas capacitaciones para que estos servicios y soluciones de TI sean apropiados, usados e incorporados en las prácticas cotidianas de los funcionarios y colaboradores, así como en las interacciones con los usuarios que acceden a los servicios de la entidad; socializaciones que son notificadas y enviadas a los correos electrónicos de los servidores a nivel nacional.

Sin embargo, no se cuenta con una estrategia interna documentada, ante los diferentes cambios en las Tecnologías de la Información (DOCU /migración de folio a SIR, estrategia de analítica de datos con la herramienta Power Bi, entre otros); así como la actualización del Mapa de Procesos de la SNR, con cambios en los procedimientos TI, manuales, guías, políticas institucionales, etc, y que representan una oportunidad estratégica para fortalecer los procesos de transformación organizacional, que requieren capacitación y alineación con las políticas institucionales de seguridad de la información, de tal forma que garantice que las modificaciones a sistemas de información, infraestructuras y procedimientos de control de TI, se ejecuten de manera segura, controlada y documentada, minimizando riesgos operativos y fortaleciendo la confianza institucional.

Cabe señalar que este dominio de Uso y Apropiación de TI, busca generar las condiciones y prácticas necesarias para facilitar el proceso de adaptación de todas las partes involucradas en las transiciones que supone la incorporación de los servicios y soluciones de TI en la cultura organizacional de la entidad, por lo anterior, se considera necesario y se **recomienda**:



Superintendencia de Notariado y Registro

Implementar la estrategia de Uso y Apropiación de los Servicios y Soluciones de TI

- Documentar la estrategia de Uso y Apropiación, haciendo uso de la Guía “MGGTI.G.UA - USO Y APROPIACIÓN DE TI”, del MINTIC. Esta guía busca orientar a las entidades públicas para definir su estrategia de TI, y es desde la jefatura de la Oficina de Tecnologías de la Información o quien haga sus veces, la responsable de definir la estrategia de Uso y Apropiación de TI de los componentes de TI; la cual debe incorporar una matriz en la cual se caractericen todos los grupos de interés de la superintendencia; y se incorporen los siguientes lineamientos que aplican al dominio de Uso y Apropiación de TI:

Tabla No.1 - Lineamientos de Uso y Apropiación de TI

Código	Título	Descripción
MGGTI.LI.UA.01	Estrategia de Uso y Apropiación de TI	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces es la responsable de definir la estrategia de Uso y Apropiación de TI de los componentes de TI.
MGGTI.LI.UA.02	Gestión del cambio	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces es la responsable de elaborar una estrategia de gestión del cambio cada vez que se despliegue o adquiera un nuevo sistema de información, solución o aplicación de software en la Entidad.
MGGTI.LI.UA.03	Plan de Formación	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces es la responsable de articularse con los responsables de la entidad y asegurar que el plan de formación de la institución incorpore adecuadamente el desarrollo de las competencias internas requeridas en TI.
MGGTI.LI.UA.04	Evaluación del nivel de adopción de ti	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con indicadores de Uso y Apropiación para evaluar el nivel de adopción de la tecnología y la satisfacción en su uso, lo cual permitirá desarrollar acciones de mejora y transformación.
MGGTI.LI.UA.05	Plan de capacitación y entrenamiento sobre los sistemas de información	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe realizar constantemente capacitación y entrenamiento funcional y técnico a los grupos de interés, con el fin de fortalecer el uso y apropiación de los componentes de TI disponibles.

Fuente: MGGTI.G.UA - USO Y APROPIACIÓN DE TI, del “producto tipo” de MINTIC

Fortalecer las competencias digitales del talento humano

- Establecer programas de capacitación continua en seguridad digital, interoperabilidad, datos abiertos, servicios ciudadanos digitales e innovación pública.
- Incorporar indicadores de competencias digitales en los planes de desarrollo individual y evaluaciones de desempeño.

Promover el liderazgo digital interno

- Designar y capacitar líderes o embajadores digitales en cada dependencia, que impulsen el uso adecuado de las herramientas institucionales.
- Crear espacios de intercambio de experiencias exitosas entre equipos.

Fomentar el uso ético, seguro y responsable de la tecnología

- Divulgar campañas internas sobre ciberseguridad, protección de datos personales y buenas prácticas de uso institucional de TI.
- Socializar continuamente las políticas de SI y los protocolos sobre uso de equipos, contraseñas, correo, sistemas de información seguros.

Estimular la innovación y la co-creación

- Promover espacios de innovación pública, laboratorios digitales, retos internos y hackathons.



Superintendencia de Notariado y Registro

- Incentivar a los funcionarios a proponer soluciones tecnológicas para la mejora de los procesos misionales.

Monitorear y evaluar la apropiación tecnológica

- Definir indicadores que midan el grado de uso, apropiación, la funcionalidad, y percepción de la experiencia de uso de las herramientas tecnológicas adoptadas por la entidad.
- Incorporar los resultados en los informes de avance del Gobierno Digital y del MIPG.

Normas que se cumplen

-Decreto 767 de 2022, Política De Gobierno Digital, Elementos de la Política de Gobierno Digital ARTÍCULO 2.2.9.1.2.1. **Estructura.** “La Política de Gobierno Digital se desarrollará a través de un esquema que articula los elementos que la componen, a saber: gobernanza, innovación pública digital, habilitadores, líneas de acción, e iniciativas dinamizadoras, con el fin de lograr su objetivo, entendidos así:

... **3. Habilitadores:** Los sujetos obligados desarrollarán las capacidades que les permitan ejecutar las Líneas de Acción de la Política de Gobierno Digital, mediante la implementación de los siguientes habilitadores:

5. Iniciativas Dinamizadoras: Comprende los Proyectos de Transformación Digital y las Estrategias de Ciudades y Territorios Inteligentes, a través de las cuales se materializan las Líneas de Acción, que permiten dar cumplimiento al objetivo de la Política de Gobierno Digital con la implementación de mecanismos de compra pública que promuevan la innovación pública digital.

5.1. Proyectos de Transformación Digital: Comprende aquellos proyectos que implementarán los sujetos obligados para aportar a la generación de valor público mediante el aprovechamiento de las capacidades que brindan el uso y la apropiación de las Tecnologías de la Información y las Comunicaciones y así alcanzar los objetivos estratégicos institucionales. Los proyectos de Transformación Digital deberán estar integrados al Plan Estratégico de Tecnología y Sistemas de Información (PETI).”

d. DOMINIO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- Política de Seguridad de la Información

En el seguimiento se pudo evidenciar que la adopción de la Política de Seguridad de la Información, fue actualizada y formalizada mediante Comité Institucional de Gestión y Desempeño, Acta No.3 del 26 de junio de 2024, donde se definió la declaración de política a través de la Política del Sistema Integrado de Gestión - Código: SIG - PI - 01 Versión: 2 Fecha: 1/09/2025, para los aspectos que corresponde al aseguramiento de la confidencialidad, integridad y disponibilidad de los activos de seguridad de la información de la Entidad.

Así mismo, la SNR cuenta con la Resolución No.4905 del 13 de mayo de 2016, por medio de la cual se adopta el Sistema de Gestión de la Seguridad de la Información, para realizar el seguimiento de seguridad a nivel integral sobre procesos, procedimientos y sistemas de información.

Objetivo de la Política: “Gestionar de manera eficiente la información de la Superintendencia de Notariado y Registro a través de la implementación de planes, procedimientos y protocolos que den cumplimiento a las condiciones de confidencialidad, integridad y disponibilidad en el óptimo desarrollo de los procesos de la Entidad.”



Superintendencia de Notariado y Registro

Estos actos administrativos dotan de carácter vinculante y oficial a las políticas, transformándolas en directrices obligatorias para toda la entidad. Este proceso no solo responde a una necesidad interna, sino que también atiende a los mandatos legales, reforzando el compromiso con la gestión de riesgos y la mejora continua del sistema de gestión de seguridad de la información (SGSI). Se encuentran publicados en el link: [Política de Privacidad - Superintendencia de Notariado y Registro \(supernotariado.gov.co\)](http://supernotariado.gov.co)

- **Manual de Políticas del Sistema de Gestión de Seguridad de la Información**

Se evidenció que el Manual fue aprobado mediante Comité Institucional de Gestión y Desempeño, Acta No.6 del 29 de octubre de 2024, con lo cual no solo se formaliza un conjunto de políticas internas de seguridad de la información, sino que también asegura que la entidad se adhiera a un marco legal y estratégico más amplio, garantizando así la protección de la información, el cumplimiento normativo y el fortalecimiento de la confianza digital en sus operaciones.

Revisado el grado de cumplimiento del manual, frente a lo requerido en la plantilla del “producto tipo” de MINTIC, denominado Manual de Políticas del Sistema de Gestión de Seguridad de la Información, se encontraron las siguientes observaciones, cabe señalar que este es un insumo base o plantilla, para la elaboración del propio Manual de Políticas de Seguridad de la Información en cada entidad, tomando también la referencia de documentación de la política.

Tabla No.2 - cumplimiento del manual, frente a lo requerido en la plantilla del “producto tipo” de MINTIC

Elemento	Observación OCI
Objetivo del Manual	Cumple <i>“Establecer lineamientos claros, detallados para cada dominio de seguridad, basado en el Modelo de Seguridad y Privacidad de la Información (MSPI) y la norma ISO/IEC 27001, en articulación con todos los procesos de la Entidad, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información y el buen uso de los activos de información propiedad de la Superintendencia de Notariado y Registro.”</i>
Alcance del Manual	Cumple <i>“El Sistema de Gestión de Seguridad de la Información (SGSI), también denominado Modelo de Seguridad y Privacidad de la Información por el MINTIC y conforme a las disposiciones normativas de la política de Gobierno Digital y su implementación, establece que el alcance del sistema y aplicación de sus controles tenga alcance para todos los procesos de la entidad y partes interesadas identificadas que puedan afectar o ser afectadas por el SGSI de la Entidad.”</i>
Definiciones	Cumple GLOSARIO DE TÉRMINOS
Compromiso de la alta Dirección	Cumple <i>“La alta dirección establece los siguientes compromisos, con el fin de fijar el liderazgo y apoyo en la implementación, mantenimiento y logro de los objetivos del Sistema de Gestión de Seguridad de la Información:”</i>
Organización de la seguridad de la información (roles y responsabilidades)	Cumple; aunque se sugiere incluir al Grupo de Comunicaciones, por su rol de Comunicador al interior de la entidad sobre la información institucional y de interés, a través de los medios de comunicación internos, con el propósito de mantener un canal constante con los funcionarios. <i>“La Superintendencia, dentro de su organización establece dos niveles principales en la toma de decisiones de alto nivel, dentro estos dos niveles se encuentra la Alta Dirección y el Comité Institucional de Gestión y Desempeño. Así mismo, se establecen los roles y responsabilidades de cada uno de los actores y áreas involucrados que hacen parte y contribuyen en la construcción y mantenimiento del Sistema de Gestión de Seguridad de la Información. Tabla 1. Roles y responsabilidades del SGSI”</i>



Superintendencia de Notariado y Registro

Elemento	Observación OCI
Políticas	Cumple <i>CAPÍTULO II – Políticas Específicas del Sistema de Gestión de Seguridad de la Información (SGSI)</i> <i>CAPÍTULO III - Políticas de Seguridad para el Buen Uso de los Activos de Información</i>
Sensibilización y Comunicación en Seguridad de la Información	Cumple <i>“Concientización y Comunicación en Seguridad de la Información”; se cuenta con el Plan de comunicación y sensibilización en SI 2025, para divulgación y apropiación del cumplimiento de las políticas del SGSI.</i>
Sanciones	Cumple <i>“La falta de conocimiento de los presentes lineamientos no libera al personal de la Superintendencia de las responsabilidades establecidas en ellos por el mal uso que hagan de los recursos TIC, por lo tanto, las sanciones podrán ser las siguientes:</i> <i>a. Sanciones de acuerdo con el Código Único Disciplinario o sanciones penales según la gravedad.</i> <i>b. Ejecución de incumplimiento de contrato según aplique.</i> <i>La Oficina de Tecnologías de la Información apoyará a la Oficina de Control Disciplinario Interno en recopilar las evidencias de incumplimiento de los lineamientos, informes de impactos y consecuencias y cualquier otro insumo requerido para la determinación de la sanción, así mismo será el encargado de gestionar el Incidente de seguridad correspondiente.”</i>
Seguimiento, medición, análisis y evaluación del SGSI	Cumple parcialmente. Toda vez que a través de la Tabla 1. Roles y responsabilidades del SGSI, se designa al Oficial de Seguridad de la Información como el responsable de <i>“Proponer los objetivos de seguridad de la información, las métricas asociadas y las estrategias para conseguir el cumplimiento de estos.”</i> ; sin embargo, no se indica claramente como la entidad realizará seguimiento a la implementación del SGSI, si establecerá indicadores, a través de comités, revisiones por la dirección. Se recomienda establecer indicadores para el cumplimiento de las políticas del SGSI.
Aprobación y Revisión de las Políticas	Cumple <i>“La revisión y actualización (cuando aplique) del manual deberá ser realizada anualmente por el Oficial de Seguridad de la Información en coordinación con el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones, para posteriormente ser llevada al Comité Institucional de Gestión y Desempeño.”</i>

Fuente: Análisis revisión

Es importante mencionar que el Proceso de Tecnologías de la Información actualmente viene realizando la actualización de los procedimientos y formatos que permitirán la implementación y ejecución de las políticas establecidas a través del Manual. Para asegurar la pronta y efectiva implementación de los procedimientos derivados de las políticas de seguridad de la información, se **recomienda** gestionar prontamente los procedimientos más críticos, involucrar a las áreas clave y generar resultados visibles en un corto plazo para lograr priorizar la creación e implementación de aquellos procedimientos que mitiguen los riesgos con mayor impacto o probabilidad. Esto permitirá mostrar avances concretos y tangibles a la alta dirección, para ser implementados por todos los funcionarios y contratistas de la SNR.

Normas que cumplen al fortalecer estas políticas de seguridad de la información en la SNR:

-Decreto 1078 de 2015 y sus modificaciones (Decreto 338 de 2022): Este decreto reglamenta el sector de las Tecnologías de la Información y las Comunicaciones (TIC); al implementar políticas de seguridad, se cumple con las directrices de este decreto, que busca fortalecer la gobernanza de la seguridad digital y la identificación de infraestructuras cibernéticas críticas en el país. ARTÍCULO 2.2.21.1.4.3. *Obligaciones de seguridad de las autoridades titulares de infraestructura crítica, o que presten servicios esenciales.*



Superintendencia de Notariado y Registro

-CONPES 3995 de 2020: La Política Nacional de Confianza y Seguridad Digital, establece una estrategia nacional para fortalecer la seguridad digital. Las políticas adoptadas por la entidad se alinean con este CONPES, y su objetivo general de Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.

-La Resolución 2277 del 3 de junio de 2025, emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), actualiza el Anexo 1 de la Resolución 500 de 2021, incorporando una nueva versión del Modelo de Seguridad y Privacidad de la Información (MSPI), alineada con la norma internacional ISO/IEC 27001:2022. El acto administrativo de la SNR, al adoptar un marco de seguridad, se adhiere a los principios y estructura del MSPI, la cual es una guía para que las entidades públicas gestionen los riesgos de seguridad y privacidad.

-El "A5 del MSPI" se refiere al Dominio Gestión de la Seguridad de la Información, dentro del Modelo de Seguridad y Privacidad de la Información (MSPI) establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Este dominio establece la política de seguridad de la información, la cual es un documento de alto nivel que define el compromiso de la gerencia con la seguridad, junto con los procedimientos para gestionar y aplicar los controles de seguridad de la información.

-El Decreto 767 de 2022, ARTÍCULO 2.2.9.1.2.3.- Política De Gobierno Digital- Manual de Gobierno Digital. El conjunto de lineamientos, guías y estándares para la implementación y desarrollo de la Política de Gobierno Digital estarán contenidos en un único instrumento, centralizado, estandarizado y de fácil uso, denominado Manual de Gobierno Digital. PARÁGRAFO 3. El Manual de Gobierno Digital incorporará una Caja de Transformación Institucional Digital, herramienta técnica que permitirá a las entidades públicas fortalecer su institucionalidad, que contendrá herramientas prácticas para facilitar la aplicación de las guías, lineamientos y estándares de la Política de Gobierno Digital, para el desarrollo de sus capacidades internas.

ARTÍCULO 2.2.9.1.2.2. **Lineamientos, Guías y Estándares.** El Ministerio de Tecnologías de la Información y las Comunicaciones expedirá y publicará lineamientos, guías y estándares para facilitar la comprensión, sistematización e implementación integral de la Política de Gobierno Digital, los cuales harán parte integral de esta. La implementación de los lineamientos, guías y estándares se realizará en articulación con el Modelo integrado de Planeación y Gestión - MIPG.

-La Ley 1437 de 2011 (Código de Procedimiento Administrativo y de lo Contencioso Administrativo): Al regular la utilización de medios electrónicos por parte de las entidades públicas, esta ley exige el cumplimiento de estándares y protocolos que son precisamente los que se desarrollan y formalizan con la aprobación de los Actos Administrativos mencionados para la SNR.

La adopción de estas directrices ha permitido establecer lineamientos claros y responsabilidades para la protección de la información, garantizando la confidencialidad, integridad, disponibilidad y privacidad de la información en la entidad. En definitiva, la entidad demuestra la gestión de la seguridad digital al formalizar sus políticas, no solo para proteger sus propios activos, sino también para responder a las exigencias legales y generar confianza en el entorno digital. El reto a futuro será mantener esta alineación, actualizando constantemente las políticas para adaptarse a las nuevas amenazas y a las evoluciones del marco regulatorio, como lo demuestra la expedición de la Política y el Manual de políticas del Sistema de Gestión de Seguridad de la Información.



Superintendencia de Notariado y Registro

○ Plan Estratégico de Seguridad y Privacidad de la Información – PESI

En la revisión efectuada se evidenció que se cuenta con el Acta No.4, jun del 2025 del Comité Institucional de Gestión y Desempeño de la SNR, donde se observa que fue presentado el Plan Estratégico de Seguridad de la información 2024 - 2026, siendo aprobado por los miembros del Comité.

También se revisó el grado de cumplimiento del plan, frente a lo requerido en la plantilla del “producto tipo” de MINTIC, denominado Plan Estratégico de Seguridad y Privacidad de la Información, encontrando lo siguiente, cabe señalar que este es un insumo base o plantilla, para la elaboración propia del Plan.

Tabla No.3 - cumplimiento del plan, frente a lo requerido en la plantilla del “producto tipo” de MINTIC

Elemento	Observación OCI
Objetivo y objetivos Específicos del Plan	Cumple <i>“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.”</i>
Alcance del Plan	Cumple <i>“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.”</i>
Documentos de Referencia	Cumple <i>Se basa en el marco normativo – “El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento.”</i>
Estado actual de la entidad respecto al sistema de gestión de seguridad de la información	Cumple <i>Numeral 7 - ESTADO ACTUAL DE LA SUPERINTENDENCIA DE NOTARIADO Y REGISTRO RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN</i>
Estrategias	Cumple <i>Numeral 8 –“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...”</i>
Responsables	Cumple <i>Numeral 9 - Respecto al Plan Estratégico de Seguridad de la Información (PESI), se definen los siguientes responsables:</i>
Aprobación	Cumple <i>Numeral 10. 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).</i>

Fuente: Análisis revisión



Superintendencia de Notariado y Registro

La entidad cumple con el requisito de contar con un Plan Estratégico de Seguridad de la Información (PESI), consolidando un instrumento integral que orienta la protección de los activos digitales, la gestión de riesgos y la continuidad operativa conforme a los lineamientos del MinTIC, la Resolución 1519 de 2020 y las buenas prácticas internacionales en seguridad de la información.

No obstante, se identificó que el PESI carece de código, versión y fecha de aprobación, por lo cual se **recomienda** además codificar formalmente el documento PESI dentro del sistema institucional de gestión documental, con el fin de garantizar su trazabilidad, actualización, control de versiones y articulación con los demás instrumentos estratégicos de la entidad.

- **Autodiagnóstico MSPI 2025**

Se evidenció igualmente, que para gestionar este producto tipo, desde la Oficina de Tecnologías de la Información se ha venido aplicando el instrumento de autodiagnóstico sugerido por el MINTIC, el cual busca brindar un grado de avance evidenciado, de la implementación de lineamientos y controles exigidos por el Modelo de Seguridad y Privacidad de la Información de la Entidad. **El Modelo de Seguridad y Privacidad de la Información - MSPI**, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.

Al respecto, se presentó como evidencia, los resultados de la aplicación del instrumento con corte a agosto de 2025, donde se muestran los resultados obtenidos de la evaluación de efectividad de los controles según la ISO 27001:2022 del Anexo A. Igualmente, el avance obtenido del ciclo de funcionamiento del modelo de operación, según el PHVA. Así mismo, presentaron el **INFORME AUTODIAGNÓSTICO SGSI, AGOSTO 31 – 2025**, el cual contiene el porcentaje del análisis de avance obtenido (53%); donde entre otros, se indica que desde la OTI se viene trabajando en actividades de actualización, aprobación y publicación de procedimientos y manuales, que buscan fortalecer los diferentes controles por dominio, a fin de lograr asegurar la seguridad y privacidad de la información en línea, necesarios para alcanzar un nivel adecuado de protección de la confidencialidad, integridad y disponibilidad de la información en la entidad.

Al respecto, se evidenció un progreso significativo en la consolidación de las capacidades institucionales para la gestión de la seguridad y privacidad de la información, y el porcentaje refleja el cumplimiento parcial de los controles establecidos por el MinTIC; con avances sustanciales en los componentes de contexto de la organización, soporte, y liderazgo; Así mismo, se identifican brechas en aspectos relacionados con la planificación, operación, evaluación del desempeño y mejora.

El resultado demuestra que la entidad ha iniciado de manera efectiva la estructuración de su Sistema de Gestión de Seguridad de la Información (SGSI) conforme al MSPI, estableciendo bases sólidas para alcanzar el un cumplimiento sobresaliente; sin embargo, se requiere y se **recomienda** fortalecer la implementación operativa de las políticas de SI, procedimientos y controles técnicos, así como la documentación de evidencias y el seguimiento continuo de los indicadores de madurez. En términos generales, el avance obtenido permite concluir que la SNR se encuentra en una **etapa intermedia de madurez**, con capacidad para consolidar su estrategia de seguridad digital en el corto plazo, siempre que se mantenga el compromiso institucional, la asignación de recursos adecuados y la mejora continua de los procesos de seguridad y privacidad de la información.



Superintendencia de Notariado y Registro

Igualmente, se **recomienda** agilizar la etapa de aprobación, publicación, divulgación y adopción oportuna de los procedimientos, manuales y formatos de control pendientes del proceso de TI, realizando posteriormente una campaña de socialización o comunicación al interior de la Oficina de Tecnologías, para que los controles sean apropiados y usados oportunamente por todos los ingenieros en los diferentes aplicativos existentes al interior de la SNR, logrando así contar con controles efectivos y obteniendo un aumento considerable en la calificación de controles, al momento de documentarlos y/o evaluar el avance en el instrumento de identificación de la línea base de seguridad.

○ Designación del Oficial de Seguridad de la Información

La designación del Oficial de Seguridad de la Información se realiza en cumplimiento de las disposiciones del Decreto 767 de 2022, particularmente de su artículo 2.2.9.1.3.2, que asigna al representante legal de cada sujeto obligado, la responsabilidad de coordinar, adoptar, implementar y hacer seguimiento a la Política de Gobierno Digital, dentro de la cual se incluye el habilitador de Seguridad y Privacidad de la Información.

En este sentido, se presentó como evidencias memorando donde el Jefe de la Oficina de Tecnologías de la Información, mediante radicado número SNR2025IE-025277-3 del 8 de septiembre de 2025, remite al Jefe de la Oficina Asesora de Planeación, indica que la OTI informa que ha designado como oficial de seguridad de la información de la SNR al ing. Juan Carlos Valenzuela Buitrago, quien se encuentra vinculado a la entidad mediante contrato 438 de 2025. Así mismo, señaló que el ing. asumirá la responsabilidad de liderar y gestionar la seguridad de la información en la entidad. Sus funciones incluirán, las estipuladas en la Resolución No. 4905 del 13 de mayo de 2016 - artículo décimo primero, que relaciona las funciones del oficial de seguridad, además de las suscritas en la guía N. 4 del Ministerio de las Tecnologías de la Información - roles y responsabilidades – responsable de seguridad de la información.

La designación del Oficial de Seguridad de la Información constituye una acción fundamental para garantizar el cumplimiento de la Política de Gobierno Digital y del Modelo de Seguridad y Privacidad de la Información (MSPI). Con esta designación, la entidad asegura la existencia de un responsable técnico que oriente, supervise y coordine las estrategias y actividades relacionadas con la confidencialidad, integridad, disponibilidad y trazabilidad de la información, fortaleciendo así la gestión de riesgos digitales, la respuesta ante incidentes y la protección de los activos institucionales.

Con ello, la entidad demuestra su compromiso con el cumplimiento normativo establecido en el Decreto 767 de 2022, el Decreto 1083 de 2015 y la Resolución 4905 de 2016, contribuyendo al fortalecimiento de la Política de Gobierno Digital, la seguridad de la información y la confianza ciudadana en los servicios digitales del Estado; no obstante se **recomienda** que el Oficial de Seguridad de la Información pueda permanecer en el tiempo por las siguientes razones:

- Permanencia y continuidad: las funciones de seguridad de la información son de carácter permanente, y requieren seguimiento continuo, histórico y estratégico que no puede interrumpirse con los tiempos de contratación temporal;
- Confidencialidad y acceso privilegiado: el Oficial de Seguridad de la Información debe manejar información sensible, cuentas de administración, incidentes y registros críticos; esto requiere un vínculo de confianza institucional y estabilidad laboral;
- Responsabilidad disciplinaria y administrativa: como garante de la seguridad de la información, el Oficial de Seguridad de la Información debe tener responsabilidad directa ante los órganos de control interno y externos, lo cual solo puede garantizarse plenamente dando continuidad al Oficial de SI;
- Cumplimiento normativo y sostenibilidad: los lineamientos del MinTIC y las normas ISO/IEC 27001 y 27701 recomiendan que los roles de seguridad de la información sean institucionalizados, con designación formal y continuidad en el tiempo, para asegurar la madurez y sostenibilidad del MSPI.



Superintendencia de Notariado y Registro

○ Plan Institucional de Capacitación en Seguridad Digital

En la verificación realizada se evidenció la existencia del documento “*PLAN DE COMUNICACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACION – 2025*”; así mismo, se aportaron las evidencias de las distintas actividades realizadas en la vigencia 2025, según lo programado.

Dicho plan tiene como propósito fortalecer la cultura organizacional en materia de seguridad de la información, promoviendo la apropiación de buenas prácticas, la gestión del riesgo digital, la prevención de incidentes y la protección de los activos de información.

A través de este instrumento, la entidad garantiza la difusión permanente de lineamientos, campañas de sensibilización, formación al personal y comunicación efectiva sobre políticas, procedimientos y responsabilidades en seguridad digital, contribuyendo así al cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) y a la consolidación de una gestión institucional segura, confiable y alineada con los principios de la Política de Gobierno Digital del Estado colombiano.

Con ello, la entidad a través de su “Plan de Comunicación y Sensibilización en Seguridad de la Información – 2025”, da cumplimiento a lo establecido en el Decreto 767 de 2022, especialmente en su artículo 2.2.9.1.3.2, que dispone la responsabilidad de los sujetos obligados de adoptar, implementar y hacer seguimiento a la Política de Gobierno Digital, la cual integra el habilitador de Seguridad y Privacidad de la Información. Así mismo, al art. 2.2.9.1.2.3. Manual de Gobierno Digital, en relación con la Evaluación y planificación de la seguridad de la información, como indicador del Manual y a la Directiva Presidencial 02 de 2022, para garantizar la implementación segura de la Política de Gobierno Digital liderada por el MINTIC.

- Gestión de Activos de la Información en la SNR
- Riesgos de Seguridad Digital /
- Plan de Tratamiento de Riesgos de Seguridad de la Información

Este ítem se considera prioritario revisar, teniendo en cuenta que **la gestión de activos de información constituye un pilar fundamental dentro del Modelo de Seguridad y Privacidad de la Información (MSPI)**, al permitir identificar, clasificar y proteger los recursos que soportan los procesos misionales y de apoyo de la entidad. Su implementación garantiza una visión integral de la información, facilitando la administración de riesgos, la definición de responsabilidades y la aplicación de controles de seguridad, acordes con el valor y la criticidad de cada activo. El levantamiento y mantenimiento actualizado del inventario de activos posibilita tomar decisiones basadas en evidencia, optimizar recursos tecnológicos y fortalecer la continuidad del negocio ante incidentes o contingencias. Además, permite dar cumplimiento a los requerimientos normativos del MinTIC, la ISO/IEC 27001 y las políticas institucionales de seguridad digital.

En la revisión realizada se encontró que la Oficina de TI presentó como evidencias el “*INFORME IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN VIGENCIA 2025*”, en el cual se indicó que con base en la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) y su Plan Estratégico de Seguridad de la Información, la Oficina de Tecnologías de la Información viene realizando actividades de identificación, clasificación y valoración de activos de la información, donde se ha logrado avanzar en la identificación de activos para 9 de los 15 procesos que actualmente se encuentran caracterizados; este avance se presenta tomando como referencia la actualización del mapa de procesos de la SNR que fue publicado el pasado 1ro. de octubre de 2025 a través de la página web de la entidad. Así mismo, informaron que las matrices de activos reposan en el repositorio de teams correspondiente al grupo de seguridad de la información.



Superintendencia de Notariado y Registro

También presentaron como evidencias el Acta de Comité Institucional de Gestión y Desempeño No. 4 de jun.2025, donde fue aprobado el plan, y se anexo el documento “*PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – (PTR) 2025*”, cuyo **Objetivo** indica: “*Contextualizar el estado de los riesgos de seguridad de la información en la Superintendencia de Notariado y Registro (SNR), así como las medidas adoptadas para gestionar y mitigar los riesgos identificados, asegurando el cumplimiento de la normativa aplicable y la implementación de controles operacionales eficaces para proteger la información.*”; sin embargo, este documento tan solo incluyó el análisis para el proceso de Gestión de Tecnologías de la Información, quedando pendiente por tratamiento los activos de información de los demás procesos de la SNR.

Teniendo en cuenta que no se ha culminado el proceso de identificación, clasificación y valoración de activos de la información para el 100% de los procesos existentes, toda vez que esta culminación es prioritaria para consolidar el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI), con el fin de garantizar una protección efectiva a los recursos existentes. La identificación de activos de información es la primera etapa del componente de Gestión del Riesgo de Seguridad y Privacidad, dado que permite reconocer los recursos críticos (tecnológicos, humanos, físicos y de información) sobre los cuales se deben aplicar controles y salvaguardas. Por tanto, es necesario consolidar el inventario institucional de activos de información para todos los procesos de la entidad, como insumo prioritario para la actualización del Plan de Tratamiento de Riesgos, la gestión de incidentes y el seguimiento a la Política de Seguridad de la Información, garantizando así la confidencialidad, integridad, disponibilidad y trazabilidad de los datos institucionales.

Por lo anterior, se **recomienda** dar prioridad y completar este levantamiento de información, que le permitirá asociar los riesgos a los activos reales, establecer controles proporcionales a su criticidad, y asegurar el cumplimiento de los lineamientos del MSPI, la ISO/IEC 27001 y las políticas de Gobierno Digital. Además, es una condición indispensable para avanzar hacia un modelo de madurez superior en seguridad de la información, donde las decisiones se fundamenten en datos y evidencias. En este sentido, se hace necesario insistir en la culminación oportuna y completa del inventario y valoración de activos, garantizando su validación por las áreas responsables y su actualización periódica. Este esfuerzo no solo cumple con un requerimiento normativo, sino que fortalece la confianza, la transparencia y la capacidad de respuesta de la entidad frente a los desafíos de seguridad y privacidad de la información.

También la Oficina de Control Interno **recomienda** priorizar a corto plazo:

- Elaborar un procedimiento para la Identificación y Clasificación de Activos, que permita establecer una base estructurada y controlada para proteger, administrar y optimizar los recursos que tiene la entidad.
- Para el Plan de Tratamiento de Riesgos, contemplar la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos identificados en la entidad, donde para cada una de las actividades se establezcan responsables y fechas de ejecución; en todo caso siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información del MINTIC, y/o las señaladas por Función Pública a través de la última versión de la Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7, Agosto de 2025.
- La conformación de un equipo de trabajo liderado por el Oficial de Seguridad de la Información, con participación de las áreas TIC, planeación y procesos misionales, para continuar el levantamiento de información en la plantilla oficial del MINTIC para el levantamiento de los activos de información.
- Priorizar sistemas de información, bases de datos y procesos críticos.
- Clasificar los activos identificados según su nivel de confidencialidad, integridad y disponibilidad, para definir prioridades de protección.
- Validar y aprobar el inventario ante el Comité Institucional de Gestión y Desempeño o el Comité de Seguridad de la Información.



Superintendencia de Notariado y Registro

-Actualizar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad con base en los activos priorizados.

Estas medidas permitirán culminar en el corto plazo la identificación institucional de activos, fortalecer la gestión del riesgo de seguridad y evidenciar el cumplimiento progresivo de la normativa vigente, contribuyendo a la consolidación de una entidad segura, confiable y alineada con los principios de la Política de Gobierno Digital.

Lo anterior, en cumplimiento de lo dispuesto en el **Decreto 767 de 2022**, artículo 2.2.9.1.3.2, -los sujetos obligados deben coordinar, adoptar e implementar la Política de Gobierno Digital, la cual incorpora el Modelo de Seguridad y Privacidad de la Información (MSPI) como uno de sus habilitadores esenciales.

-El **Decreto 1083 de 2015**, artículo 2.2.22.2.1, que establece la Seguridad Digital como parte de las políticas de gestión y desempeño institucional, las cuales deben garantizar la protección de los activos de información y el tratamiento seguro de los datos.

-El **Documento Maestro del MSPI del MINTIC** que complementa estas disposiciones, señalando que la identificación y valoración de activos de la información constituyen la base del proceso de gestión del riesgo de seguridad y privacidad de la información.

o Gestión de Control de Accesos y Autenticación

Se revisó la adecuada gestión de accesos y autenticación teniendo en cuenta que es un componente esencial dentro del Modelo de Seguridad y Privacidad de la Información (MSPI), ya que garantiza que únicamente las personas autorizadas puedan acceder a los recursos, sistemas y datos de la Superintendencia conforme a sus funciones y responsabilidades. Este control permite **proteger la confidencialidad, integridad y disponibilidad de la información**, reduciendo significativamente los riesgos de accesos indebidos, fugas de datos o manipulación no autorizada.

Verificado este aspecto la Oficina de TI informó que la Superintendencia de Notariado y Registro gestiona los accesos a sus sistemas de información a través de un sistema centralizado de gestión de identidades (IGA), que permite la creación, modificación e inactivación de usuarios en los diferentes sistemas de información como: SIR, VUR, SIDT y el Directorio Activo.

Igualmente indicó que se realiza la asignación de roles mínimos requeridos según el tipo de usuario (funcionario, contratista, pasante, cliente, etc.); y que se permite la autenticación mediante usuario y contraseña, con segundo factor obligatorio (OTP, tokens). Se cuenta con la trazabilidad de accesos y actividades (adiciones, eliminaciones, modificaciones); se realiza la entrega de credenciales solo si están debidamente solicitadas y autorizadas, a través de la documentación requerida según el tipo de vinculación del personal de la SNR.

Igualmente se verificó el mapa de procesos de la entidad, donde se evidenció que existen los siguientes documentos, actualizados recientemente al 03/Oct/2025:

- Manual de *GESTION DE USUARIOS Y CONTRASEÑAS*, código: GTI-MN-006,
- Procedimiento *ADMINISTRACION DE USUARIOS Y CONTRASEÑAS*, código: GTI-PR-007;
- Formato *ADMINISTRACION DE USUARIOS*
- Formato *MATRIZ DE REGISTRO DE USUARIOS PRIVILEGIADOS Y DE SERVICIO*

Cuyo objetivo se basa en controlar la creación, modificación e inactivación de usuarios en los sistemas de información de la Superintendencia de Notariado y Registro mediante la implementación de controles



Superintendencia de Notariado y Registro

adecuados durante el ciclo de vida de los usuarios y el uso de contraseñas seguras, para proteger la confidencialidad, integridad y disponibilidad de los servicios tecnológicos de la entidad.

Igualmente, presentan evidencias del Formato -Creación, modificación o eliminación de VPN site to Site, del proceso Sistema de Gestión de Seguridad de la Información, versión 01 del 28 abril de 2023. Se cuenta con el MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, Código: SIG-SSI-PO-04-MN-01, versión: 01 de Fecha: 29 de Oct. de 2024, al numeral 6.3. se establece que para el Control de Acceso la entidad establece lineamientos, procedimientos y controles de acceso a la red y sistemas de información con el fin de mitigar riesgos asociados al acceso no autorizado tanto a la información como a la infraestructura tecnológica.

El procedimiento de administración de usuarios y contraseñas, como control de acceso a los sistemas de información es un pilar fundamental en la gestión de la seguridad digital de la entidad. Su correcta aplicación garantiza que solo las personas autorizadas puedan acceder a los recursos, datos y aplicaciones necesarias para el cumplimiento de sus funciones, reduciendo significativamente el riesgo de accesos indebidos, fugas de información, fraudes o sabotajes.

Además, este procedimiento permitirá mantener la trazabilidad de las acciones realizadas dentro de los sistemas, fortaleciendo la rendición de cuentas y facilitando auditorías o investigaciones cuando sea necesario. Al implementar políticas claras de autenticación, perfiles de usuario, control de privilegios y registro de actividades, se promueve la protección de la confidencialidad, integridad y disponibilidad de la información, pilares esenciales de la seguridad de la información.

Un adecuado control de acceso no solo protege los activos digitales de la entidad, sino que también contribuye al cumplimiento normativo, como las políticas de seguridad digital o la Ley de Protección de Datos Personales y fortalece la confianza de los usuarios en el manejo responsable de la información.

o Políticas de Cifrados

Este es un elemento esencial dentro del MSPI, al garantizar que los datos institucionales tanto en tránsito, como en reposo se mantengan protegidos frente a accesos no autorizados, pérdida o manipulación indebida. El cifrado asegura la **confidencialidad y la integridad de la información**, incluso cuando los sistemas son comprometidos o los medios de almacenamiento resultan vulnerados.

En la revisión realizada la Oficina de TI informó que la Superintendencia de Notariado y Registro cuenta con la aplicación de controles criptográficos a los activos que, por su exposición, así lo requieran. Así mismo, presentaron evidencias del listado de controles criptográficos 2025 existentes, a través del cual se realizará el seguimiento y gestión de los controles criptográficos implementados.

Igualmente se verificó el mapa de procesos de la entidad, donde se evidenció que recientemente fueron creados los siguientes documentos:

- El Manual de GESTION DE CONTROLES CRIPTOGRAFICOS, código GTI-MN-005;
- El Procedimiento GESTION DE CONTROLES CRIPTOGRAFICOS, código GTI-PR-006;
- El formato LISTADO DE CONTROLES CRIPTOGRAFICOS, código GTI-FR-005 y
- El MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, Código: SIG-SSI-PO-04-MN-01 Versión: 01, de Fecha: 29 de Octubre de 2024

El establecimiento de procedimientos y políticas de cifrado constituye un componente esencial dentro del marco de seguridad de la información de la SNR. Su principal objetivo es proteger la confidencialidad, integridad y



Superintendencia de Notariado y Registro

autenticidad de la información durante su almacenamiento, procesamiento y transmisión, evitando el acceso no autorizado y la exposición de datos sensibles o estratégicos.

Contar con políticas de cifrado formalizadas permite definir estándares, responsabilidades y mecanismos técnicos para el uso de algoritmos criptográficos seguros, la gestión de claves, la protección de dispositivos y medios de almacenamiento, así como la comunicación segura entre sistemas y usuarios. Esto contribuye a la mitigación de riesgos tecnológicos, el cumplimiento normativo y la confianza en los servicios digitales.

En conclusión, las políticas y procedimientos de cifrado no son opcionales sino estratégicos, pues permiten garantizar la protección de la información institucional frente a las amenazas digitales, fortaleciendo la ciberseguridad organizacional.

o Seguridad de las Operaciones de TI

La seguridad de las operaciones de TI es un componente crítico para garantizar la **estabilidad, disponibilidad y confiabilidad de los servicios tecnológicos** que soportan los procesos misionales y administrativos de la entidad. Su adecuada gestión permite **prevenir incidentes, minimizar interrupciones, y asegurar la integridad de los sistemas y datos institucionales** frente a amenazas internas o externas.

En esta revisión que fue realizada a la seguridad de las operaciones que diariamente se desarrollan al interior de la entidad, y en especial a la relacionada con la expedición de los Certificados de Tradición y Libertad - CTL, para ello la Oficina de TI presentó como evidencias el documento de “*CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN*” y “*EVIDENCIAS INFORMACION CERTIFICADA DE CTL - BANCARZACION (CTL)*”; en estos documentos se evidenció que existen diversos mecanismos de seguridad que permiten garantizar la confidencialidad, la integridad y salvaguarda de la información, como son:

- Se gestionan los accesos a los sistemas de información a través de un sistema centralizado de gestión de identidades (IGA), que permite la creación, modificación e inactivación de usuarios en los diferentes sistemas de información como: SIR, VUR, SIDT y el Directorio Activo.

- Se realiza la asignación de roles mínimos requeridos según el tipo de usuario (funcionario, contratista, pasante, cliente, etc.); y que se permite la autenticación mediante usuario y contraseña, con segundo factor obligatorio (OTP, tokens).

- Se cuenta con la trazabilidad de accesos y actividades (adiciones, eliminaciones, modificaciones); se realiza la entrega de credenciales solo si están debidamente solicitadas y autorizadas, a través de la documentación requerida según el tipo de vinculación del personal de la SNR.

- La firma digital en un certificado CTL representa un pilar fundamental dentro del ecosistema de Gobierno Digital, al garantizar la autenticidad, integridad y no repudio de los documentos, según las transacciones electrónicas que son realizadas. Este mecanismo fortalece la confianza ciudadana en los servicios digitales, asegurando que las actuaciones administrativas sean verificables y seguras.

- El proceso de asignación de privilegios según los roles autorizados, que constituye una práctica esencial para la seguridad de la información y la gestión eficiente de los sistemas digitales del Estado. Este enfoque, basado en el principio de mínimo privilegio, garantiza que cada usuario acceda únicamente a los recursos necesarios para el desempeño de sus funciones, reduciendo los riesgos de uso indebido o fuga de información.



Superintendencia de Notariado y Registro

- La aplicación de Bancarización que cuenta con un sistema de registro de eventos (logging) integral, diseñado para garantizar la trazabilidad completa, facilitar las auditorías de sistema y permitir el análisis forense ante cualquier incidente de seguridad o de negocio, según las transacciones ejecutadas en la plataforma.
- La aplicación de controles rigurosos, en múltiples capas para proteger la Confidencialidad, Integridad y Disponibilidad de la Información.
- La aplicación de políticas de respaldo y recuperación de datos, que se convierte en un componente crítico dentro de la seguridad y continuidad operativa de los procesos en el marco del Gobierno Digital. Estas políticas aseguran la disponibilidad, integridad y recuperación oportuna de la información ante incidentes, fallas técnicas o ciberataques, garantizando la prestación ininterrumpida de los servicios digitales del Estado.

Al implementar procedimientos estandarizados de operación, monitoreo, respaldo, actualización y control de cambios se contribuye a mantener un entorno tecnológico seguro, trazable y resiliente. Además, asegura el cumplimiento de los lineamientos del MSPI, la ISO/IEC 27001 y las políticas nacionales de Gobierno Digital, que exigen prácticas de operación seguras, documentadas y auditables.

- **Seguridad en las Comunicaciones de TI**

Este es un elemento esencial para garantizar la confidencialidad, integridad y disponibilidad de la información que se transmite dentro y fuera de la entidad. Su adecuada gestión permite **prevenir accesos no autorizados, interceptaciones, alteraciones o pérdidas de datos**, protegiendo tanto la información institucional como la confianza de los ciudadanos y aliados estratégicos.

La Oficina de TI presentó como soporte, dos informes técnicos de la gestión adelantada por el proveedor de telecomunicaciones, uno de octubre de 2024 y el otro, con seguimientos realizados en el primer semestre de 2025; igualmente se indicó que la entidad cumple con los lineamientos y buenas prácticas de seguridad en las comunicaciones, garantizando la confidencialidad, integridad y disponibilidad de la información que se transmite entre sus sistemas, funcionarios y ciudadanos, a través de la implementación de mecanismos de cifrado, autenticación y control de acceso, de tal forma que asegura que los datos sean protegidos frente a interceptaciones o manipulaciones no autorizadas.

Este cumplimiento se enmarca en las directrices del Modelo de Seguridad y Privacidad de la Información (MSPI) y la Política de Gobierno Digital del MinTIC.













- **Seguridad Integrada en el Ciclo de Vida de los Sistemas de Información**

Integrar la seguridad al ciclo de vida de los sistemas de información es una práctica esencial para **garantizar que la protección de la información se considere desde la concepción, hasta el retiro de cada sistema de información**. Este enfoque preventivo permite identificar y mitigar riesgos desde las etapas iniciales de análisis, diseño, desarrollo y mantenimiento del software y sistemas de información en general, evitando vulnerabilidades que podrían comprometer la **confidencialidad, integridad y disponibilidad** de los datos de la entidad.

En la revisión realizada, la Oficina de TI presentó como evidencias los siguientes lineamientos del procedimiento de adquisición, mantenimiento o desarrollo de software; para la separación de ambientes; control de versiones; y liberación de sistemas de información:



Superintendencia de Notariado y Registro

-  8. Procedimiento adquisición, mantenimiento y desarrollo de software
-  12. Separación de Ambientes
-  13. Control de Versiones de Software
-  14. Liberación de Sistemas
-  1. Manual para adquisición, desarrollo y mantenimiento seguro de sistemas de información
-  2. Procedimiento adquisición, desarrollo y mantenimiento seguro de sistemas de información
-  3. Manual de Desarrollo Seguro de Sistemas de Información
-  4. Estándar para Codificación Segura
-  1. Manual de Separación de Ambientes
-  1. Procedimiento - Control de Versiones de Software
-  2. Formato - Control de versiones de software
-  1. Procedimiento de Liberación de Sistemas de Información

Durante la revisión del ítem se evidenció que los documentos correspondientes se encuentran en versión borrador, sin aprobación formal, ni publicación oficial. Esta situación refleja un avance parcial en la implementación del control, dado que los lineamientos, procedimientos o políticas aún no cuentan con validez institucional ni aplicabilidad operativa. Por lo tanto, la ausencia de los documentos aprobados y vigentes representa un riesgo significativo para la gestión de seguridad y privacidad de la información, ya que impide garantizar la uniformidad en la aplicación de controles, la responsabilidad institucional, y la trazabilidad en la gestión de cambios. Además, expone a la entidad ante posibles brechas normativas, inconsistencias en los procedimientos de desarrollo o mantenimiento del software y debilidades de cumplimiento de requerimientos del MSPI.

Por lo anterior, **se recomienda** agilizar su implementación y formalización, con el fin de mitigar posibles riesgos asociados a vulnerabilidades en el software, garantizar la protección de la información desde su diseño y fortalecer el cumplimiento normativo y regulatorio aplicable, como son los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y en cumplimiento con los requisitos establecidos por la norma ISO/IEC 27001, particularmente los controles relacionados con la adquisición, desarrollo y mantenimiento de los sistemas; de tal forma que se logre cubrir los controles del desarrollo de software y su ciclo de vida, en atención a la necesidad de adoptar estrategias de seguridad digital que integre “principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital”, documentación que es esencial para asegurar la implementación de prácticas seguras, trazables y controladas en el desarrollo de soluciones tecnológicas de la entidad, por lo cual es necesaria su inclusión al SIGI.

Ahora bien, una vez revisado el Mapa de Procesos actualizado y vigente desde el 1ro de octubre de 2025, se encontró el procedimiento denominado “*Gestión de Cambios TI*”, identificado con código: GTI-PR-005 del 3 de octubre de 2025, y el “*MANUAL DE CONTROL DE CAMBIOS DE TI - Gestión de Tecnologías de la Información*”, donde se establecen distintas actividades con el fin de controlar adecuadamente los cambios en los sistemas de información productivos, mediante la planificación de actividades, análisis de riesgos asociados, y validación de pruebas previas a la implementación, esto con el propósito de minimizar posibles afectaciones a la continuidad e integridad de los servicios tecnológicos de la SNR.

Para ello, se establece en este procedimiento la necesidad de “*crear la solicitud de cambio a través de la plataforma definida para la gestión de cambios y posteriormente incluir el formato de solicitud de cambios totalmente diligenciado y que para la apertura de los cambios, se debe tener en cuenta las actividades planificadas en los sistemas de información como lo son los Planes de Mantenimiento Preventivo, conforme con los lineamientos vigentes para Mantenimiento...*” Así mismo se evidencia que, en estas situaciones, debe



Superintendencia de Notariado y Registro

existir aprobación del cambio por parte de la mesa de control de cambios de TI o del Comité Institucional de Gestión y Desempeño, para solicitar el cambio.

Ante este procedimiento y dada su reciente publicación oficial, resulta fundamental y se **recomienda** garantizar su divulgación efectiva dentro de la Oficina de TI, a fin de que todos los funcionarios y contratistas conozcan, comprendan y apliquen los lineamientos allí establecidos. La divulgación oportuna permite fortalecer la cultura de seguridad de la información, asegurar la adopción homogénea de las políticas y minimizar los riesgos asociados al desconocimiento o la aplicación incorrecta del procedimiento, conllevando a la materialización de los riesgos anteriormente mencionados.

De otra parte, la Oficina de TI presentó como evidencias los informes técnicos de “Análisis de Vulnerabilidades” realizados a diferentes aplicativos de la entidad en la vigencia 2025, con el objetivo de analizar, identificar evaluar y mapear sus vulnerabilidades utilizando la técnica de escaneo y priorizando las debilidades o fallas de seguridad en un sistema, red, aplicación o infraestructura tecnológica, para preservar la confidencialidad, integridad o disponibilidad de la información. En estos informes se estableció, entre otros, las **recomendaciones** que se presentan con el fin de corregir las diferentes vulnerabilidades identificadas en los dispositivos evaluados, o para la aplicación de las Políticas establecidas.

La realización periódica de análisis de vulnerabilidades constituye una práctica fundamental para la gestión proactiva de la seguridad de la información en la entidad, al permitir la identificación temprana de debilidades técnicas que podrían ser explotadas por actores maliciosos. En este sentido, **se recomienda** dar continuidad a estas actividades, fortaleciendo su alcance y frecuencia, con el fin de mantener un nivel adecuado de protección en la infraestructura tecnológica de la entidad.

Igualmente, se hace necesario y se **recomienda** atender oportunamente las recomendaciones derivadas de dichos análisis, implementando las acciones correctivas y/o preventivas necesarias para mitigar los riesgos identificados, dejando documentación de lo actuado. El No abordar estas observaciones puede dejar expuesta a la entidad frente a amenazas reales y comprometer la eficacia del sistema de gestión de seguridad de la información.

Este proceso contribuye al cumplimiento de los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI), así como a los principios y controles definidos en la norma técnica ISO/IEC 27001 -específicamente en el dominio -Seguridad en las operaciones y Cumplimiento. Adicionalmente, respalda la conformidad con otras disposiciones nacionales sobre protección de datos personales y gestión de riesgos tecnológicos.

- **Protocolos para la Gestión de incidentes - Interacción con CSIRT**

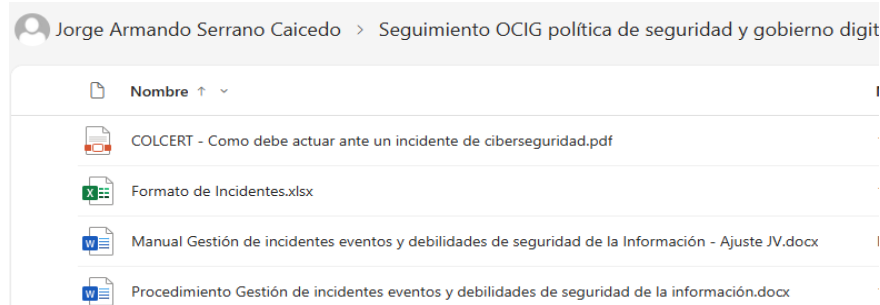
Contar con protocolos definidos para la gestión de incidentes de seguridad de la información es fundamental para garantizar una respuesta oportuna, coordinada y eficaz ante eventos que puedan afectar la confidencialidad, integridad o disponibilidad de los activos de información de la SNR. Estos protocolos permiten establecer procedimientos claros para la detección, reporte, análisis, contención, recuperación y documentación de los incidentes, minimizando su impacto operativo y reputacional.

En la revisión realizada, la Oficina de TI presentó como evidencias un brochure de COLCERT que contiene las instrucciones de como actuar ante un incidente de ciberseguridad; no obstante, no se presentaron evidencias de la interacción realizada con ellos para el recibo de capacitaciones u otras actividades.



Superintendencia de Notariado y Registro

Igualmente, la OTI presentó como evidencias para esta revisión los siguientes lineamientos para la gestión de incidentes, los cuales se observó que están en una versión preliminar y pendientes de aprobación, codificación:



El principal objetivo de estos lineamientos refiere: “*establecer las actividades para la gestión eficaz de eventos, incidentes y debilidades de seguridad de la información en la Superintendencia de Notariado y Registro (SNR). Propendiendo por la protección de los activos de información, y minimizando los posibles impactos que puedan afectar la operación de la entidad.*”, sin embargo, y teniendo en cuenta que los soportes documentales presentados están sin aprobación formal, ni publicación oficial, se identifica un avance parcial en la implementación del control, dado que los lineamientos, procedimientos o políticas aún no cuentan con validez institucional, ni aplicabilidad operativa.

Por lo anterior, **se recomienda** priorizar y agilizar la elaboración, revisión y aprobación de los protocolos de gestión de incidentes de seguridad de la información, que abarque todas las fases, desde la detección inicial hasta el cierre y análisis posterior del incidente, con el fin de asegurar una respuesta institucional oportuna ante eventos que puedan comprometer los activos de información o la continuidad de los servicios de la SNR.

Para lograrlo, se **sugiere** conformar un equipo técnico multidisciplinario que integre representantes de las distintas áreas de tecnología, seguridad digital y procesos, a fin de coordinar la construcción de los procedimientos de manera colaborativa y coherente con los lineamientos del MSPI, la ISO/IEC 27035 y la Política de Seguridad y Privacidad de la Información. Asimismo, se **recomienda** utilizar formatos estandarizados, plantillas y/o ejemplos de referencia, que ya estén definidos como los del MINTIC, lo que permitirá reducir tiempos de redacción y facilitará la validación técnica y jurídica, con el fin de mitigar posibles riesgos asociados a la materialización de los riesgos existentes y fortalecer el cumplimiento normativo y regulatorio aplicable, como son los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y en cumplimiento con los requisitos establecidos por la norma ISO/IEC 27001, particularmente los controles relacionados con la gestión de incidentes.

○ Plan de Recuperación Ante Desastres -DRP

Contar con un Plan de Recuperación ante Desastres (Disaster Recovery Plan – DRP), es fundamental para garantizar la continuidad operativa, la protección de la información y la resiliencia tecnológica de la entidad frente a incidentes que puedan interrumpir sus servicios.

Un DRP permitirá reaccionar de manera rápida, ordenada y efectiva ante eventos como ciberataques, fallas de infraestructura, desastres naturales o errores humanos, minimizando el impacto sobre los procesos críticos y reduciendo pérdidas económicas y reputacionales. Además, disponer de un DRP fortalece la confianza de los ciudadanos, al demostrar que la entidad está preparada para mantener la disponibilidad de sus sistemas y proteger los datos bajo cualquier circunstancia.



Superintendencia de Notariado y Registro

En la revisión efectuada a este elemento, la Oficina de Tecnologías indicó que: “*Para el mes de Julio de 2026 la Oficina de Tecnologías de la información estableció actividades para la definición de la primera versión del Plan de Recuperación de Desastres TI-DRP, para los cuales se tiene el siguiente avance*”

ACTIVIDADES	Estado
<i>Levantamiento de información procesos de la entidad</i>	<i>Terminado</i>
<i>Levantamiento Estado de la infraestructura TI de Superintendencia de Notariado y Registro</i>	<i>En Curso</i>
<i>Identificación y Definición de Procesos críticos de la Entidad</i>	<i>En curso</i>
<i>Definición de Proveedores Críticos para la Operación y análisis de ANS</i>	<i>Terminado</i>
<i>Análisis de Impacto al Negocio (BIA) de procesos, determinando los tiempos de recuperación críticos (RTO, RPO).</i>	<i>En Construcción de matrices de evaluación</i>

Ante la falta de un Plan de Recuperación ante Desastres (DRP) en Tecnologías de la Información en la entidad, representa un riesgo crítico para la continuidad de los servicios y la protección de la información. Si bien esta actividad ha sido reprogramada en diferentes vigencias, es imprescindible y se **recomienda** priorizar su elaboración e implementación en el corto plazo para mitigar posibles vulnerabilidades y cumplir con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y otras normativas aplicables.

Se recomienda acelerar este proceso, conformando un equipo responsable con roles claros, establecer un cronograma con prioridades, realizar un análisis de impacto al negocio que permita focalizar los esfuerzos, y apoyarse en marcos normativos y metodologías del MINTIC. Asimismo, es fundamental contar con el compromiso de la alta dirección, capacitar al personal involucrado, ejecutar pruebas periódicas para validar el plan y mantener una comunicación constante sobre los avances del proyecto. Adoptar estas acciones garantizará la formalización de un DRP robusto y efectivo, fortaleciendo la resiliencia institucional y asegurando la continuidad operativa ante eventuales incidentes o desastres.

En conclusión el DRP no solo es un requisito técnico o normativo, sino una estrategia esencial de gestión de riesgos y seguridad de la información, que permite a las entidades asegurar la continuidad del negocio, proteger sus activos digitales y cumplir con los principios de disponibilidad, integridad y confiabilidad establecidos como buenas prácticas, en marcos como ISO 22301 y la norma ISO 27031.

- **Plan de Continuidad del Negocio**

Disponer de un Plan de Continuidad del Negocio (BCP), no es solo un requisito normativo, sino una decisión estratégica de la alta dirección, que demuestra liderazgo en gobernanza digital, garantiza la resiliencia organizacional y protege la continuidad de la misión institucional frente a cualquier contingencia, lo que lo constituye en un componente crítico del Sistema de Gestión de Seguridad de la Información (SGSI) y del cumplimiento de la Política de Seguridad Digital del Estado colombiano.

Su implementación garantiza que la entidad mantenga la disponibilidad operativa de sus servicios misionales y tecnológicos ante eventos de interrupción, ya sean de origen físico, lógico o humano. El BCP permite identificar procesos críticos, evaluar dependencias tecnológicas y establecer estrategias de recuperación medibles y verificables. De esta manera, se optimiza la capacidad de respuesta ante incidentes, se asegura la continuidad de los servicios digitales y se minimiza el impacto económico, reputacional y de cumplimiento normativo.



Superintendencia de Notariado y Registro

Contar con un BCP vigente y probado también fortalece la madurez institucional en gestión del riesgo operativo y cibernético, articulándose con el Plan de Recuperación ante Desastres (DRP), el MIPG, y los lineamientos de ISO 22301 e ISO 27031.

Para esta revisión desde Control Interno se solicitó a la Oficina Asesora de Planeación mediante correo electrónico del 26 de septiembre de 2025, y a la Oficina de Tecnologías de la Información, informar el avance alcanzado, del cual, a la fecha de cierre del presente informe, no se había dado respuesta. Por lo que se recomienda que la entidad diseñe e implemente un Plan de Continuidad del Negocio (BCP) alineado con la Política de Seguridad Digital (Decreto 767/2022), la Resolución 1519/2020 y las normas ISO, garantizando la continuidad operativa y tecnológica ante posibles incidentes, fortaleciendo la capacidad de respuesta y continuidad del servicio público. Esta acción técnica fortalece la madurez institucional en gestión del riesgo digital, garantiza la continuidad de los servicios misionales y demuestra liderazgo en gobernanza y seguridad de la información dentro del marco del Gobierno Digital.

De manera general es necesario y se **recomienda** agilizar la documentación de los diferentes protocolos y lineamientos pendientes de ajustes y aprobación, lo cual no solo permitirá fortalecer la capacidad de respuesta ante incidentes, garantizar la trazabilidad de las acciones y avanzar en la madurez del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI), sino que también permitirá dar cumplimiento a los requerimientos normativos, como son:

-Decreto 767 de 2022 (MinTIC) – reglamenta aspectos de la Política de Seguridad Digital del Estado Colombiano. Artículo 2.2.9.1.1.3. Principios. Numeral 12. **“Resiliencia Tecnológica:** *Los sujetos obligados a la aplicación de la presente Política tomarán acciones respecto de la prevención de riesgos que puedan afectar la seguridad digital y con ello propenderán por la disponibilidad de los activos, la recuperación y continuidad de la prestación del servicio ante interrupciones o incidentes”*. Artículo 2.2.9.1.3.2, -los sujetos obligados deben coordinar, adoptar e implementar la Política de Gobierno Digital, la cual incorpora el Modelo de Seguridad y Privacidad de la Información (MSPI) como uno de sus habilitadores esenciales.

-El Decreto 1083 de 2015, artículo 2.2.22.2.1, que establece la Seguridad Digital como parte de las políticas de gestión y desempeño institucional, las cuales deben garantizar la protección de los activos de información y el tratamiento seguro de los datos.

-El Documento Maestro del MSPI del MINTIC que complementa estas disposiciones, señalando que la identificación y valoración de activos de la información constituyen la base del proceso de gestión del riesgo de seguridad y privacidad de la información.

-Ley 1581 de 2012 y su Decreto Reglamentario 1377 de 2013, sobre protección de datos personales, donde se exige adoptar medidas de seguridad apropiadas para impedir el acceso, pérdida o uso no autorizado de los datos.

-Resolución 1519 de 2020, Artículo 6. Condiciones mínimas técnicas y de seguridad digital. Los sujetos obligados deberán observar las condiciones mínimas técnicas y de seguridad digital que se definen en el Anexo 3 de la presente resolución. -3.2 CONDICIONES DE SEGURIDAD DIGITAL: Establecer los planes de contingencia, DRP y BCP, que permita garantizar la continuidad de la sede electrónica o del sitio web 7/24 los 365 días del año.

-ISO/IEC 27001:2022, que recomiendan el uso de controles como respuesta a incidentes de seguridad de la información; centrándose en la gestión de incidentes de seguridad de la información a través de procesos



Superintendencia de Notariado y Registro

efectivos, que incluyen contención, mitigación y manejo de evidencia, con la responsabilidad asignada a la alta dirección para su supervisión.

-Directiva Presidencial 02 de 2022, que promueve la adopción de estándares de seguridad y gobierno digital en entidades públicas.

e. DOMINIO SERVICIOS CIUDADANOS DIGITALES

Los Servicios Ciudadanos Digitales representan un pilar fundamental en la transformación digital del Estado colombiano, ya que permiten ofrecer trámites y servicios en línea de manera segura, accesible e interoperable, fortaleciendo la relación entre la ciudadanía y las entidades públicas.

Su implementación contribuye a la eficiencia administrativa, reduce tiempos y costos, mejora la transparencia y promueve una atención más cercana, personalizada e inclusiva. Además, facilitan el uso de la identidad digital, la interoperabilidad y la carpeta ciudadana, elementos que aseguran que los servicios públicos estén centrados en el ciudadano y no en la entidad.

En cumplimiento a este dominio la SNR cuenta con la Ventanilla Única de Servicios – VUR que es el modelo de simplificación de trámites de registro, articula las diferentes entidades facilitando el registro inmobiliario y garantizando seguridad jurídica al ciudadano y las entidades que lo integran.

Su principal objetivo es reducir los trámites, plazos, costos y requisitos necesarios para formalizar los procesos de escrituración y registro de la propiedad inmueble, principalmente para los actos de transferencia de dominio. Fomentar la formalidad y el cumplimiento de las obligaciones legales del ciudadano frente a las transacciones de transferencia de inmuebles. Garantizar la transparencia y evitar riesgo de fraude alrededor de transacciones de compraventa entre particulares. Mejorar los procesos de información e inducir a una cultura de legalidad en torno a la propiedad inmueble. Acercar las gestiones asociadas al registro inmueble ante la ciudadanía, a partir de la ampliación y cualificación de canales de atención y el mejoramiento de la calidad del servicio. Articular a las entidades públicas y privadas relacionadas con el registro de la propiedad inmueble en torno a un proceso eficiente y expedito.

Los principales beneficios para los ciudadanos con el servicio de la VUR, son:

Reducción de plazos, costos y requisitos necesarios para formalizar los procesos de escrituración y registro de la propiedad inmueble, dado que el trámite se realiza desde la notaría; a través del REL.

Evitar riesgos de fraude y corrupción.

Al articular entidades públicas y privadas que forman parte de la cadena de registro inmobiliario, mejora la calidad del servicio registral.

Los servicios a los que puede acceder un ciudadano en esta Ventanilla son:

-PSE Derechos: Realizar el pago de los derechos de registro a través del botón PSE.

-Certificados: Acceder a la compra en línea de certificados de tradición y libertad.

-Estado del trámite: Mediante esta opción el ciudadano podrá realizar el seguimiento al estado de su trámite, solo debe indicar la Oficina de Registro (ORIP) donde lo está realizando y el número de turno de radicación.

-Radicación Electrónica: A finales de abril del 2019 se inició en las notarías de la ciudad de Bogotá la prueba piloto de la Radicación Electrónica, a la fecha se encuentra operando en más de 100 notarías.

Así mismo, existen otros servicios complementarios que se obtienen a través de la Ventanilla Única de Registro, como son:



Superintendencia de Notariado y Registro

- Repositorio de poderes.
- Acceso de entidades a la información registral.
- Registro Único Empresarial y Social.

Igualmente se evidenció que la entidad cuenta con los protocolos técnicos de servicio web, suscritos con diferentes entidades del estado, a través de la plataforma X-ROAD, de intercambio seguro y estandarizado de datos entre sistemas de información para la “CONSULTA ÚLTIMO PROPIETARIO Y SEGREGADOS”; y CONSULTA INDICE DOCUMENTO”, los cuales fueron presentados por la Oficina de TI al equipo auditor.

De manera general, los Servicios Ciudadanos Digitales, apoyados en tecnologías como X-Road, impulsan un Estado más conectado, confiable e inclusivo, donde la información fluye de manera ágil entre entidades y el ciudadano se beneficia de servicios simples, digitales y centrados en sus necesidades, en cumplimiento de la Resolución 1519 de 2020 y las directrices del Gobierno Digital colombiano.



f. LÍNEA DE ACCIÓN - SERVICIOS Y PROCESOS INTELIGENTES

La importancia de los servicios y procesos inteligentes radica en su capacidad de convertir la información existente, en un conocimiento útil y en acciones automatizadas, potenciando la productividad, la sostenibilidad y la innovación institucional. Son la base para construir entidades más ágiles, resilientes y centradas en el valor público. Su relevancia radica en la **capacidad de integrar tecnologías como la inteligencia artificial**, el análisis de datos, la automatización y el Internet de las Cosas (IoT) para optimizar la toma de decisiones, reducir costos operativos y mejorar la experiencia de los ciudadanos.

Para esta revisión la Oficina de Tecnologías de la Información indicó que se está trabajando en el proyecto piloto para un asistente de Inteligencia Artificial denominado “Vicky”.

Así mismo, señaló que “La entidad avanza en el desarrollo de un modelo conversacional basado en Inteligencia Artificial Generativa, orientado a fortalecer las capacidades del asistente virtual Vicky.

El objetivo de esta iniciativa es alcanzar un Producto Mínimo Viable (MVP) que permita evolucionar el asistente actual hacia una versión que ofrezca respuestas precisas, contextuales y alineadas con la normativa, los procedimientos y los servicios institucionales.

Durante la fase inicial, el equipo técnico trabaja en la modernización del frontend y backend del asistente, habilitando la integración con modelos de IA generativa. Esta evolución permitirá incorporar capacidades de comprensión del lenguaje natural, contextualización avanzada y generación dinámica de respuestas, contribuyendo a una atención más eficiente, personalizada y coherente con los lineamientos de la entidad.

La iniciativa se enmarca dentro de la estrategia de transformación digital y busca fortalecer los mecanismos de atención ciudadana mediante el uso ético y responsable de tecnologías de inteligencia artificial, en cumplimiento de las directrices de la Política de Gobierno Digital.”

Al respecto, se resalta la importancia de contemplar servicios y procesos inteligentes en la SNR, basados en la capacidad de convertir la información en conocimiento útil y en acciones automatizadas, potenciando la productividad, la sostenibilidad y la innovación institucional, los cuales son la base para construir entidades más



Superintendencia de Notariado y Registro

ágiles, resilientes y centradas en el valor público. No obstante, y teniendo en cuenta que el uso de la inteligencia artificial en los servicios y procesos inteligentes, aunque puede ofrecer grandes beneficios, también plantea nuevos riesgos para la seguridad de la información; por este motivo se **recomienda** implementar un enfoque integral de ciberseguridad y gobernanza de datos, de tal forma que combine las políticas, la tecnología y la cultura organizacional, como las siguientes (entre otras):

Gobernanza y clasificación de la información:

Establecer un marco claro de clasificación de datos (públicos, internos, confidenciales y sensibles) antes de su procesamiento con IA, garantizando que los modelos no accedan ni almacenen información sin los permisos adecuados.

Gestión de riesgos en IA:

Incorporar evaluaciones de riesgo específicas para sistemas basados en IA, considerando vulnerabilidades como manipulación de datos de entrenamiento, sesgos algorítmicos y posibles ataques.

Seguridad en el ciclo de vida del modelo:

Proteger las etapas de diseño, entrenamiento, despliegue y mantenimiento de los modelos de IA mediante controles de acceso, auditorías continuas y monitoreo de comportamiento anómalo.

Uso ético y transparente:

Asegurar la trazabilidad y explicabilidad de las decisiones automatizadas, manteniendo registros de auditoría y mecanismos de revisión humana, cuando se traten datos personales o decisiones críticas.

Capacitación y cultura de ciberseguridad:

Fortalecer la conciencia del personal en el manejo de herramientas inteligentes, promoviendo prácticas seguras en el intercambio y almacenamiento de información.

Cumplimiento normativo:

Garantizar la alineación con normas nacionales e internacionales como la Ley 1581 de 2012 (protección de datos personales), la Resolución MinTIC 1519 de 2020, y estándares como ISO/IEC 27001 y 27701, asegurando la protección integral de la información.

Estas acciones permitirán aprovechar el potencial de la IA sin comprometer la confidencialidad, integridad y disponibilidad de los datos, reforzando la confianza institucional y ciudadana en los servicios digitales inteligentes.

g. ADOPCIÓN DEL PROTOCOLO IPv6 EN LA SNR

Descripción: En respuesta a la masiva conexión de dispositivos a Internet y el agotamiento de las direcciones IPv4, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) expidió la Resolución 2710 de 2017, "Por la cual se establecen lineamientos para la adopción del protocolo IPv6" en el país. Así mismo, expidió la Resolución 1126 de 2021, Por la cual se modifica la Resolución 2710 de 2017; con estas resoluciones se busca básicamente que las entidades del Estado adopten el IPv6 en sus infraestructuras tecnológicas, lo cual permite que más dispositivos puedan ser conectados a Internet, abonando el camino para la implementación de redes de nueva generación.

En la verificación realizada a este aspecto la Oficina de TI presentó como evidencias de avance, el documento denominado -Plan de Diagnóstico IPv4 a IPv6, para la Superintendencia de Notariado y Registro, elaborado en



Superintendencia de Notariado y Registro

Noviembre de 2024, que contiene entre otros, el inventario realizado para el proceso de transición de IPv4 a IPv6, en el numeral 5 del documento. El inventario contiene el detalle de la infraestructura tecnológica de la SNR, abarcando tanto hardware como software crítico para la operación de la entidad.

El inventario se centra en identificar la compatibilidad de cada componente con el protocolo IPv6, con el objetivo de facilitar la planificación de la transición. Los detalles completos del inventario están documentados en el Anexo 1: Inventario General de TI, que incluye un análisis detallado de cada equipo y sistema evaluado, quedando reportados en el plan de diagnóstico, y donde se indica que actividades se deberían ejecutar en el corto plazo para su cumplimiento, o si es necesario declarar en estado de obsolescencia por no cumplimiento del protocolo.

Así mismo, el documento contempla los diferentes riesgos y **recomendaciones** para el aseguramiento de los dispositivos de seguridad, proponiendo acciones para mitigar cualquier riesgo asociado con la transición, limitando la posibilidad de ataques relacionados con la asignación de direcciones, garantizando así la continuidad operativa de los servicios de la SNR y cumplimiento con las normativas nacionales e internacionales; por lo anterior, se considera necesario y se **recomienda** acatar su cumplimiento a fin de proteger la confidencialidad, integridad y disponibilidad de la información de la entidad.

Con base en la documentación presentada se evidenció que el personal de la OTI realizó las pruebas para configurar el direccionamiento IPv6 sugerido en el documento “Plan de Direccionamiento” y donde se usaron los dispositivos que se definen con soporte IPv6 en el apartado de inventario del documento “Plan de Diagnostico IPv6”; pruebas que fueron realizadas en la vigencia 2025 y fueron documentadas en el “Plan de Pruebas Piloto”, el cual fue compartido al equipo auditor; esta transición permitirá asegurar la modernización y compatibilidad de las redes de la SNR.

No obstante, se **recomienda** agilizar su implementación de tal forma que permita las conexiones a IPv4 e IPv6 desde cualquier usuario, teniendo en cuenta que el Art.3. de la **Resolución No.01126 de 2021**, indica que: **“Plazo de adopción. Las entidades estatales del orden nacional que trata el artículo segundo de la presente resolución, deberán culminar el proceso de transición al protocolo IPv6 en convivencia con el protocolo IPv4 a más tardar el 30 de junio de 2022.”** (Resaltado y subrayado fuera de texto).

Así mismo, en el art.2. se indica: Modificación del párrafo del artículo 4 de la Resolución 2710 de 2017. Modifíquese el párrafo del artículo 4 de la Resolución MinTIC 2710 de 2017, el cual quedará de la siguiente manera: **“Parágrafo. Los sujetos obligados de que trata el Artículo 2 de la presente Resolución, en el proceso de transición al protocolo IPV6 deberán adoptar los documentos denominados: “Guía de transición de IPv4 a IPv6 para Colombia” y “Guía para el aseguramiento del Protocolo IPv6”, guías que no fueron presentadas como soportes documentales del avance alcanzado en la SNR.**

Así mismo, se **recomienda** tener presente lo señalado en el Artículo 6 de la **Resolución 2710 de 2017** del MinTIC, donde se ha establecido que *“el incumplimiento de las disposiciones de la norma dará lugar a las sanciones establecidas en el marco de la Ley 1341 de 2009. En todo caso, las entidades tendrán la posibilidad de continuar el proceso de adopción de IPv6, de conformidad con el plan de diagnóstico de las infraestructuras de TI que se hayan realizado y, por otro lado, iniciar el registro del avance en la herramienta de seguimiento para tal fin establecida por el MinTIC en el siguiente enlace: <https://ipvseis.mintic.gov.co/login/>.”*



Superintendencia de Notariado y Registro

h. IMPLEMENTACIÓN RESOLUCIÓN No.1519 DE 2020 - Anexo No.1 - Directrices de accesibilidad web

Implementar las Directrices de Accesibilidad para el Contenido Web es fundamental para garantizar que los sitios y servicios digitales sean inclusivos, usables y accesibles para todas las personas, incluyendo aquellas con discapacidad visual, auditiva, motriz o cognitiva. Desde una perspectiva técnica y de cumplimiento, aplicar estas directrices —alineadas con la Política de Gobierno Digital (Resolución MinTIC 1519 de 2020) permite que las entidades públicas cumplan con los estándares internacionales del W3C y con los principios de accesibilidad, interoperabilidad y transparencia exigidos por el Estado colombiano.

Para esta revisión la Oficina de TI presentó como evidencia el documento .pdf denominado “Portal-Política de Términos y condiciones de uso página web.”; donde se relacionaron los Términos y condiciones de uso de la página web; la Aceptación de Términos; el Aviso de privacidad; las Condiciones de uso de la Página Web; las Páginas web de terceros; la Política de Seguridad de la Información y Protección de Datos Personales; y el enlace de contacto.

Así mismo, aportaron el documento .pdf “Portal-certificados_ita_2025”, donde el jefe de la Oficina de Tecnología de la Información de la Superintendencia de Notariado y Registro, certifica el cumplimiento de los criterios de accesibilidad web descritos en el Anexo 1 de la Resolución 1519 de 2020, para 7 requisitos.

Tras la verificación realizada a los criterios establecidos en el Anexo 1 de la Resolución 1519 de 2020 del MINTIC, se concluye que la entidad ha alcanzado un nivel de cumplimiento adecuado respecto a los lineamientos de accesibilidad digital exigidos para sus portales y sedes electrónicas, en concordancia con los estándares WCAG, donde se evidenció la implementación de prácticas que facilitan la navegación, comprensión y acceso equitativo a la información, tales como la estandarización de contenidos, donde se cuenta con información de acceso a la misión, visión, funciones y normativa; el uso de textos alternativos en imágenes; estructuras semánticas correctas; videos publicados con subtítulos; disposición de un mapa del sitio de forma que se facilita la accesibilidad a los usuarios; permite la navegación mediante teclado; el contraste visual es apropiado; para la identificación de la entidad se observa el nombre de la entidad completo tanto en el encabezado, como en el pie de página; cuenta con el vínculo a redes sociales para ser redireccionado en los botones respectivos; maneja un lenguaje claro; se observa en página, que las noticias tienen la fecha de publicación; Se cuenta con la sección Página de Ley de Transparencia; elementos que permiten contribuir al cumplimiento de las políticas de Gobierno Digital y de la Ley 1712 de 2014.

Por lo anterior, se determina que el Anexo 1 presenta cumplimiento satisfactorio, dejando como **recomendación** mantener una estrategia continua de mejora en accesibilidad inclusiva, con revisiones técnicas y seguimientos periódicos que aseguren la sostenibilidad del cumplimiento normativo, teniendo en cuenta que aún es posible seguir fortaleciendo los mecanismos de accesibilidad para personas con discapacidad, mediante la incorporación de herramientas adicionales de asistencia (como transcripciones de audio, lenguaje de señas, entre otras), así como la actualización permanente de los contenidos digitales conforme a la evolución de los estándares internacionales.

3. EVALUACIÓN DE RIESGOS Y CONTROLES

De acuerdo con la verificación realizada al mapa de riesgos de gestión de TI actualizado y suministrado por la Oficina Asesora de Planeación, se observa que han sido identificado cuatro riesgos de gestión al proceso GESTION TICS, para los cuales se han diseñado los respectivos controles, siguiendo los lineamientos del



Superintendencia de Notariado y Registro

Departamento Administrativo de la Función Pública - DAFP, descritos en la Guía para la Gestión Integral del Riesgo en Entidades Públicas V7 del 2025.

En cuanto a las actividades de control, las cuales deben atender las causas raíz identificadas y enfocarse en la gestión de los factores de riesgo previamente identificados, cuentan con los atributos, de responsable de la ejecución y nivel de autoridad apropiado, la acción y los atributos informativos o de formalización del control.

En cuanto a los atributos informativos, cuentan con el aspecto de documentación, frecuencia, evidencia y ejecución; no obstante, se sugiere revisar en el atributo *ejecución*, que se describa además de cómo se ejecuta el control, las acciones que se implementarán o se tomarán en caso de desviaciones o situaciones que se tecten, tema que no se identifica con claridad en los controles establecidos, como es el caso del control 1 riesgo 2 el cual describe: *"El Coordinador de Servicios Tecnológicos anualmente solicita, consolida y valida las necesidades de contratación de adquisición, renovación y/o mantenimiento de la infraestructura tecnológica de SNR, como evidencia queda el reporte de las necesidades al Jefe de la OTI y/o la persona encargada de la consolidación y gestión del Plan de Adquisiciones de la oficina para cada vigencia"*.

Al respecto, se observa que efectivamente se consolidarán y validarán las necesidades del proceso, dejando el reporte correspondiente; sin embargo, no se tiene en cuenta, para el no cubrimiento de esas necesidades cual podría ser la alternativa para que se cumpla con el objetivo del control, evitando así la materialización del riesgo, teniendo en cuenta que es un control de tipo preventivo.

De manera general se evidencia un trabajo significativo en la actualización y mejora de los riesgos identificados por el proceso, así como en el establecimiento de los controles, lo cual refleja una comprensión adecuada de las áreas críticas y los factores que pueden afectar el cumplimiento de los objetivos institucionales; No obstante, a la fecha del presente informe no se cuenta con actividades de control ejecutadas, toda vez que su salida a producción fue el pasado 1ro. de octubre de 2025, con el nuevo Mapa de Procesos, por lo cual se sugiere fortalecer la fase de ejecución mediante la implementación y seguimiento de los controles definidos, garantizando su eficacia y trazabilidad.

Lo anterior, teniendo en cuenta que la ejecución de los controles de riesgos de gestión constituye un componente esencial para garantizar la efectividad del sistema de control interno y la sostenibilidad de la gestión institucional. Su adecuada aplicación permitirá **anticipar, mitigar y monitorear** los riesgos que pueden afectar el cumplimiento de los objetivos propuestos.

4. EVALUACIÓN MAPA DE ASEGURAMIENTO

El Mapa de Aseguramiento constituye una herramienta esencial para el seguimiento, control y mejora continua del Sistema de Gestión de Seguridad de la Información, permitiendo mantener un equilibrio entre el control preventivo y el correctivo, y asegurando que la SNR avance hacia un modelo de gestión más transparente, eficiente y orientado a resultados, en línea con los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG) y las políticas de Control Interno establecidas por el DAFP.

La evaluación realizada al **Mapa de Aseguramiento** permitirá evidenciar el nivel de madurez y efectividad de las Actividades de Control o Funciones de Aseguramiento que debe adelantar el Sistema de Seguridad de la Información como *Aspecto Clave de Exito*, así como la coherencia entre los riesgos identificados, los controles implementados y las estrategias de mitigación definidas.



Superintendencia de Notariado y Registro

Tabla No.4 – Mapa de Aseguramiento SSI

FUNCIONES DE ASEGURAMIENTO O ACTIVIDAD DE CONTROL QUE DEBE ADELANTAR	Atributos Función de Aseguramiento o Actividad de Control para la evaluación de confianza
Realizar seguimiento al cumplimiento de la política General y específica del Sistema de Gestión de Seguridad de la información de la SNR, adoptada mediante Resolución No. 06416 de julio 13 de 2021.	<p>El líder de seguridad de la información (JEFE OTI) ejecuta 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.</p> <p>El informe resultado de la auditorias se presentará al Comité de Gestión y desempeño el cual les servirá para la toma de decisiones.</p> <p>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.</p>

Fuente: Mapa de Aseguramiento SNR, v.3 de 2025

La Oficina de Tecnologías de la Información como responsable de la función de aseguramiento “Realizar seguimiento al cumplimiento de la Política General y Especifica del Sistema de Gestión de Seguridad de la Información de la SNR, adoptada mediante Resolución No. 06416 de julio 13 de 2021”, presentó como evidencias del cumplimiento dado y como Segunda Línea de Defensa identificada en la entidad, el informe de aseguramiento realizando en la vigencia 2025, denominado: INFORME PRELIMINAR DE RESULTADOS, Cumplimiento de las Políticas Específicas del SGSI - 01 de enero a 15 de Octubre de 2025.

Resultados de la Evaluación de la Función de Aseguramiento

Una vez realizado el análisis documental del informe presentado y con base en los criterios evaluadores establecidos por el Departamento Administrativo de Función Pública - DAFP, las cuales fueron comunicadas al proceso de TI para realizar la evaluación de la función de aseguramiento o cumplimiento de las actividades de control, se obtuvieron las siguientes calificaciones:

- a) Objetivo y alcance: 3
- b) Metodología establecida para la función de aseguramiento: 3
- c) Responsable: 5
- d) Comunicación de resultados y manejo de la información: 2

Calificación final Total: 3.4

Nivel de confianza del aseguramiento: **MEDIO**

Revisado el contenido del Informe presentado por la OTI, resultado del seguimiento realizado al cumplimiento de las políticas de SI, se observó que fue realizado desde la óptica de la Segunda Línea de Defensa a las medidas de control adoptadas desde el Nivel Central para los sistemas de información, en cuanto a Control de Acceso Lógico; Concientización y comunicación en seguridad de la información; Control de Navegación Hacia Internet; Gestión de la continuidad tecnológica; y Seguridad de las operaciones. No obstante, resulta fundamental que la segunda línea, logre garantizar una amplia cobertura al total de las políticas de seguridad de la información, establecidas en el *MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN*.



Superintendencia de Notariado y Registro

Así mismo, es importante consolidar un ciclo de mejora continua, donde las lecciones aprendidas de la autoevaluación de la segunda línea de defensa se traduzcan en acciones concretas de fortalecimiento institucional, a través de un Plan de Mejoramiento, garantizando así la sostenibilidad de la seguridad de la información y la efectividad de la actividad de aseguramiento realizada en la vigencia 2025.

Por lo anterior y consecuente con la verificación de la información presentada, como resultado de la evaluación de los criterios de la función de aseguramiento, se obtuvo la siguiente calificación, por cuanto:

a) Objetivo y Alcance: 3, teniendo en cuenta que el objetivo y alcance del informe de aseguramiento no contemplaron en su totalidad los parámetros requeridos y socializados por la Oficina de Control Interno para estos dos aspectos, lo que limita la claridad y profundidad del análisis general realizado; dado que el objetivo debe ser directo y claro, al igual que se debe establecer un alcance para la actividad de aseguramiento en general, donde se indiquen, entre otros, -Periodo de tiempo en el que se realizó el aseguramiento -El lugar de trabajo donde va a realizar la actividad de aseguramiento (ORIP, NC, DR) -Periodo de tiempo que se va a evaluar o cubrir con el aseguramiento -Criterios a verificar. Esta situación evidencia la necesidad de ajustarlo según los criterios de evaluación socializados, asegurando que en futuras versiones se incluyan todos los elementos técnicos requeridos para fortalecer la actividad de control ejecutada.

b) Metodología establecida para la función de aseguramiento: 3, aunque se describe y analiza la información objeto del aseguramiento realizado -cumplimiento de las políticas del Sistema SI, se requiere ajustar y fortalecer la metodología para que se informe cuál fue la muestra seleccionada del total de las políticas; así mismo, una cobertura completa a dichas políticas a lo largo de cada vigencia permitirá una visión transversal de la gestión y fortalecimiento de las actividades de control establecidas.

c) Responsable: 5, teniendo en cuenta que el Líder designado a través del mapa de aseguramiento es quien firma el informe de aseguramiento, ya que su firma respalda la validez, trazabilidad y compromiso institucional con los resultados presentados.

d) Comunicación de Resultados/ Acciones Correctivas y Manejo de la información: 3, teniendo en cuenta que a octubre/2025, estos resultados no han sido socializados a la alta dirección; tampoco se evidencian acciones de mejora como resultado del aseguramiento realizado y a través del Plan de Mejoramiento, de tal forma que permitan asegurar la efectividad de las actividades y tiempos para su ejecución.

En conclusión, se genera una calificación de 3,4; con un nivel Medio de confianza del aseguramiento, de acuerdo a los valores definidos en los criterios evaluadores de las actividades de aseguramiento ejecutadas por el Aspecto Clave de Éxito: SISTEMA DE SEGURIDAD DE LA INFORMACIÓN, lo que determina que: *“La Oficina de Control Interno o quien haga sus veces deberá auditar y generar hallazgos y recomendaciones a la función de aseguramiento (2ª línea) para su mejora y evaluará los aspectos que considere relevantes de la 1ª línea de defensa.”*, según lo definido por el DAFP.

Por lo anterior, se recomienda:

- **Documentar todas las mejoras identificadas** en el proceso de autoevaluación realizado por la 2da. Línea de Defensa, asegurando su trazabilidad y su incorporación al **Plan de Mejoramiento Institucional**.
- Mantener una **bitácora de seguimiento** que refleje avances, ajustes y evidencias asociadas a cada política evaluada.
- Promover la **retroalimentación continua** entre las líneas de defensa para fortalecer el sistema de control interno.



Superintendencia de Notariado y Registro

□ Utilizar herramientas tecnológicas o tableros de control (ejm. Power BI, etc) que faciliten el monitoreo de los resultados.

5. EVALUACIÓN DE EFECTIVIDAD DE LAS ACCIONES ESTABLECIDAS EN LOS PLANES DE MEJORAMIENTO

5.1 Plan de Mejoramiento Suscrito con la Contraloría General de la República.

A partir de la revisión de los hallazgos vigentes en el Plan de Mejoramiento suscrito con la Contraloría General de la República y tomando como base el último reporte presentado por la Oficina Asesora de Planeación, es decir al corte del 30 de junio de 2025, se identificó un (1) hallazgo asociado al alcance del presente seguimiento, por lo tanto, fue incluido en la presente evaluación.

A continuación, se detalla el pronunciamiento emitido por el equipo auditor, como resultado del Proceso de Aseguramiento desarrollado en la Oficina de Tecnologías de la Información en Nivel Central:

Tabla No.5 -Revisión Hallazgos Contraloría General de la República

No.	Código del Hallazgo	Descripción Hallazgo	Pronunciamiento y Recomendaciones OCIG	Estado	Responsable
1	201511	H31. Restauración copias de respaldo. No existe una política de respaldo, salvo la recuperación de la data en el momento de cambio de los data center, así como no se evidencia seguimiento y verificación por medio de un procedimiento institucional. Lo anterior, genera un riesgo en la restauración de la información en el momento que se requiera restaurar y acceder a la data en situaciones.	Luego de realizar la verificación al cumplimiento de cada una de las actividades establecidas para este hallazgo, en las diferentes reformulaciones efectuadas en el transcurso de las vigencias y después de ejecutar las pruebas de restauración en sitio -en la cual se restauró un Servidor Virtual alojado en el sistema de ingeniería de VMware, el cual presta servicios web para interoperabilidad de la SNR y donde se logró evidenciar la configuración de la política de backup asociada al servidor a restaurar; y donde adicionalmente se detalló y registró el proceso de restauración efectuado, el cual finalizó de manera exitosa; aspecto validado en la plataforma de VMware donde la máquina virtual fue restaurada bajo las condiciones solicitadas y desde la cual se evidenció el nuevo servidor restaurado, encendido y solicitando login o inicio de sesión. Para su elaboración se tuvieron en cuenta las herramientas de respaldo	ACCIONES EFECTIVAS	Oficina de Tecnologías de la Información / Nivel Central Primera línea de defensa



Superintendencia de Notariado y Registro

No.	Código del Hallazgo	Descripción Hallazgo	Pronunciamiento y Recomendaciones OCIG	Estado	Responsable
			<p>corporativas y la infraestructura de virtualización (VMware vCenter/ESXi sobre VxRail); así mismo, se logró evidenciar que el proceso es ejecutado por ingenieros de la Oficina de Tecnologías de la Información de la SNR.</p> <p>Igualmente se solicitaron y fueron aportadas las evidencias de restauraciones efectuadas: 30 may; 10 Jul; y 4 sep/2025; así mismo, fue aportada la bitácora donde se lleva el registro de restauración de backups realizadas.</p> <p>A través de esta verificación documental y validación en sitio, permitieron determinar que las actividades desarrolladas por el responsable – OTI para este hallazgo fueron “EFECTIVAS”, motivo por el cual se recomienda realizar el cierre del hallazgo No.201511 suscrito con la CGR.</p>		

Fuente: Consolidado General Plan de Mejoramiento suscrito con la CGR – corte al 30 jun.2025 y pronunciamiento del equipo auditor.

En atención a la verificación realizada en sitio a las acciones emprendidas por la Oficina de Tecnologías de la Información para este hallazgo identificado por la CGR en la vigencia 2015 y una vez evaluada la efectividad de éstas, por parte del equipo auditor de la Oficina de Control Interno se recomienda realizar el cierre del hallazgo con código 201511 – H31 - Restauración copias de respaldo.

5.2 Plan de Mejoramiento Institucional

A partir de la revisión de los hallazgos vigentes en el Plan de Mejoramiento Institucional, se logró identificar la existencia de once (11) No Conformidades, transversales a la unidad auditable, por lo tanto fueron objeto de evaluación en el presente Aseguramiento realizado.

A continuación, se detalla el pronunciamiento emitido por el equipo auditor, como resultado del Proceso de Aseguramiento desarrollado.



Superintendencia de Notariado y Registro

Tabla No.6 -No Conformidades transversales al proceso auditado

No.	Código del Hallazgo	Descripción Hallazgo	Pronunciamiento y Recomendaciones OCIG	Estado	Responsable
1	2019210-	No se evidencian avances de cumplimiento en relación con algunos productos, exigidos como requisitos necesarios conforme a lo establecido en el Manual de Gobierno Digital; se observan productos que requieren mejoras a fin de cumplir con todos los requisitos exigidos, falta de aprobación, socialización e implementación en la Entidad; debilidades frente a los controles que deben ser establecidos, respecto a la infraestructura tecnológica.	Hallazgo cuyas actividades se encuentran en desarrollo al cierre del informe, dado que la fecha máxima es al 22 dic.2022. Se espera que se logre avanzar en la documentación; aprobación; socialización y ejecución de las actividades pendientes del Manual de Gobierno Digital para contar con las evidencias documentales necesarias para su evaluación de efectividad.	EN DESARROLLO	Primera Línea de Defensa Oficina de TI
2	2019211-	No se evidencian avances de cumplimiento en relación con algunos productos, exigidos como requisitos necesarios conforme a lo establecido a través del Conpes de Seguridad Digital; se observan productos que requieren mejoras a fin de cumplir con todos los requisitos exigidos, falta de aprobación, socialización e implementación en la Entidad. Igualmente, se evidenció la falta seguimiento periódico frente al cumplimiento y efectividad de los mismos.	Para este hallazgo se determinó como acción: <i>Actualizar el Plan Estratégico de Seguridad de la Información de acuerdo a la normativa y CONPES vigente.</i> ; Actividad que estaba programada para el 30 de junio de 2025.; la cual se evidenció que fue cumplida, ya que el plan PESI fue aprobado en el CIGD del 27 de mayo al 6 de junio de 2025. No obstante, según la presente evaluación realizada y descrita en este informe, se presenta falta de efectividad de acciones, toda vez que la entidad no ha logrado avanzar en la implementación del esquema de gestión de riesgos digitales, ni en la adopción de protocolos estandarizados de atención a incidentes, lo que evidencia una brecha entre la planeación estratégica del CONPES 3854 y su ejecución operativa en la entidad.	INEFECTIVO	Primera Línea de Defensa Oficina de TI
3	20211012	Verificada la pag. web de la entidad, no se es posible identificar el número de vínculos visitados en ésta por los usuarios (visitas de los contenidos de página); adicionalmente, los enlaces del sitio web, no indican claramente el contenido al cual conducen, como en el caso de los informes subidos al enlace de Control, como se muestra en el anexo, en uso de las buenas prácticas establecidas y recomendadas en la Guía de Accesibilidad de Contenidos Web para los procesos de actualización, estructuración, reestructuración, diseño, rediseño del portal web y sedes electrónicas, así como de los contenidos existentes en éstas.	Para este hallazgo se determinó como acciones: <i>"Dar continuidad con la actualización del HOME de la sede electrónica SNR bajo los lineamiento de MInTic (el kit UI y Resolución 1519-2020)" y "Mesa de trabajo entre las Áreas Planeación, OTI y comunicaciones para definir lineamientos del cargue de la información en la sede electrónica".</i> Se observa que las actividades fueron cumplidas, con "Informe actualizado home sede electrónica con fecha Julio de 2025" actividad que estaba programada para cumplimiento 30-07-2025. También se observan actas de reunión de fechas 15-07-2025, 04-08-2025, 10-09-2025- Correo para <i>"hacer entrega oficial del desarrollo solicitado"</i> . Según la presente evaluación realizada y descrita en este informe, se determinó la efectividad de las acciones, toda vez que la entidad ha logrado avanzar en cumplimiento con los lineamientos mínimos de accesibilidad web, garantizando que su portal es comprensible, perceptible, operable y	EFFECTIVO	Primera Línea de Defensa Oficina de TI



Superintendencia de Notariado y Registro

No.	Código del Hallazgo	Descripción Hallazgo	Pronunciamiento y Recomendaciones OCIG	Estado	Responsable
			robusto, en conformidad con los criterios establecidos por el MinTIC y las Pautas de Accesibilidad para el Contenido Web. Por lo anterior, se recomienda el cierre del hallazgo.		
4	20211013	<p>El Plan de Tecnologías de la Información, así como el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan de Seguridad de la Información -PESI no han sido aprobados; y no se encontró su publicación en la página web de la entidad; en los borradores presentados como evidencia en el desarrollo de la auditoría, se identificó la falta de documentación de algunas actividades de la estructura definida por el Mintic a través de las diferentes Guías - Guía G.ES.06- Guía como estructurar el plan estratégico de Tecnologías de la Información – PETI; Versión: 1.1.Oct.2019; inobservándose con éste, el cumplimiento frente a lo establecido en el Decreto 2723 de 2010 artículo 17 numeral 1- “Funciones de la Oficina de Tecnologías de Información. Son funciones de la Oficina Tecnologías de la Información, las siguientes: 1. Asesorar al Despacho del Superintendente en la definición de las políticas, planes, programas y procedimientos relacionados con el uso y aplicación de tecnologías información, que contribuyan a incrementar la eficiencia y eficacia en diferentes dependencias de Superintendencia, así como a garantizar calidad en la prestación los servicios.”, igualmente se puede incumplir lo determinado en el 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.” Adicionalmente, se advierte sobre el riesgo de no contar con el recurso necesario que debe disponerse presupuestalmente, para garantizar el cumplimiento de las metas y objetivos que debe trazar el área de tecnologías a través de una adecuada planeación, control y seguimiento, mediante la formalización de planes estratégicos; para permitir con éste, no solo la alineación y coherencia de los planes, programas y proyectos implementados en TI con los incorporados en el PETI institucional; sino también, para fortalecer la justificación de las necesidades y estudios de mercado en los procesos de contratación asociados a los proyectos tecnológicos que se adelanten en la Entidad y determinar con suficiente claridad, los productos o servicios que se esperan obtener en términos calidad y cantidad, a fin de garantizar los indicadores de eficiencia, eficacia y efectividad; adicionalmente, en aras de determinar el valor real de los contratos tecnológicos que se requieran adelantar en la Entidad y cumplir a cabalidad</p>	<p>Para este hallazgo se determinó como acciones: “Actualizar el Plan estratégico de Tecnología de la Información - PETI, plan de tratamiento de riesgos de Seguridad de la información.”, Y la actividad “Actualizar el Plan de tratamiento de riesgos de seguridad de la Información”, Actividades programadas para el 30 de junio de 2025.</p> <p>También se contaba con la acción: “Socializar el Plan estratégico del sistema de gestión de seguridad de la Información”, Actividad con fecha límite de cumplimiento al 30-08-2025.</p> <p>Según la revisión realizada en el presente informe se evidenció que estos dos planes fueron realizados conforme a los lineamientos establecidas por el Mintic; así mismo, se evidenció que fueron aprobados en comité Institucional de Gestión y Desempeño virtual del 27 de mayo al 6 de junio de 2025; también se evidenció la alineación de estos dos planes con el Plan Anual de Acción de la SNR, el cual es sujeto a seguimiento al cumplimiento por parte de la Segunda Línea de Defensa de manera trimestral; También se observó el video de “Presentación Plan Estratégico de seguridad de la Información (PESI) y roles del SGTI” del 19 de septiembre de 2025.</p> <p>Por lo anterior, se determinó que las acciones fueron cumplidas y son efectivas. Por lo tanto, se recomienda el cierre del hallazgo.</p>	EFFECTIVO	<p>Primera Línea de Defensa</p> <p>Oficina de TI</p>



Superintendencia de Notariado y Registro

No.	Código del Hallazgo	Descripción Hallazgo	Pronunciamiento y Recomendaciones OCIG	Estado	Responsable
		con los principios de la contratación pública, en aras de evitar la materialización de riesgos que puedan afectar el cumplimiento del Proceso Contractual y las consecuencias que con éstos, se puedan generar en otros procesos.			
5	20211019	Revisado el plan de continuidad del negocio en la Entidad, se observó que este documento se encuentra desactualizado, toda vez que en la hoja uno refiere la versión 2 de 2015 y en las subsiguientes, refiere la versión 1 de 2013, situación que no permite determinar un efectivo control documental de la versión; tampoco permite identificar las amenazas potenciales que podría enfrentar la SNR en sus procesos y productos críticos del negocio, como resultado de un análisis real del impacto que se haya realizado; no se determina la forma en que serán controlados y mitigados a través de la configuración de procedimientos o guías, en caso de un desastre y para cada uno de los servicios críticos vitales que sean determinados, situación que conlleva a generar inobservancia a la Política de Gobierno Digital establecidos en el Decreto 1008 de 2018, en su Artículo 2.2.9.1.2.2. Manual de Gobierno Digital, que establece que para la implementación de la Política de Gobierno Digital, las entidades públicas deberán aplicar el Manual de Gobierno Digital que define los lineamientos, estándares y acciones a ejecutar por parte de los sujetos obligados de esta Política de Gobierno Digital", y en la Guía para la preparación de las TIC para la continuidad del negocio.	<p>Establecieron como acción, "Realizar el plan de continuidad DTI (DRP)"; acción que está programada para el 22 dic.2022.</p> <p>A la fecha del presente seguimiento las actividades están en DESARROLLO; no obstante, según la verificación realizada en el presente informe, y en atención a los avances presentados para este elemento, se recomienda agilizar su documentación con el fin de dar cumplimiento a las fechas establecidas para la actividad, que es fundamental para asegurar la continuidad operativa y la resiliencia tecnológica de la entidad, al permitir restaurar servicios críticos, proteger la información institucional y minimizar el impacto de incidentes o fallas graves; su implementación reflejará una gestión proactiva del riesgo digital y el compromiso con la seguridad, disponibilidad y confianza en los servicios que ofrece la SNR.</p>	EN DESARROLLO	Primera Línea de Defensa Oficina de TI
6	20211020	A la fecha de la presente auditoria (4 Dic.2020), se realizó la prueba de validación de uso de IPV6 a través de la página www.supermotariado.gov.co, como se muestra en anexo del test o prueba realizada, arrojando como resultado que "Este sitio web no está preparado para IPV6", situación que contraviene lo estipulado en la Resolución 2710 de 2017 – "Por la cual se establecen lineamientos para la adopción del protocolo IPV6., ARTÍCULO 3o. PLAZO DE ADOPCIÓN. Las entidades estatales de carácter nacional que trata el artículo segundo de la presente resolución, deberán culminar el proceso de transición a protocolo IPV6 en convivencia con el protocolo IPv4 a más tardar el 31 de diciembre de 2019...", situación que conlleva al riesgo de posibles sanciones por incumplimiento de las disposiciones de la presente resolución. Con respecto al informe denominado "DISEÑO, DESARROLLO E IMPLEMENTACIÓN PARA LA TRANSICIÓN DEL PROTOCOLO IPv4 A IPV6", se observa que en la primera fase se realizó la validación de la infraestructura tecnológica de la entidad versus el grado de compatibilidad del protocolo IPV6,	<p>Establecieron como acción, "Realizar informe de la planeación detallada de transición de IPV6, en la infraestructura de TI de la SNR acorde a la guía de transición de IPV 4 a IPV 6 para Colombia y a la Guía para el aseguramiento del protocolo IPV6."</p> <p>La actividad presentaba fecha de cumplimiento al 30-abr-2025; No se encuentra la evidencia en la One Dive – Plan de Mejoramiento.</p> <p>No obstante, en el seguimiento realizado a las Políticas de Gobierno y Seguridad Digital del presente informe, se pudo identificar que se cuenta con el documento titulado "Plan de diagnóstico IPV4 a IPV6 para la SNR" y "Plan de Pruebas Piloto", donde documentaron las pruebas de implementación realizadas en la vigencia 2025. Sin embargo, y dado que existen aún elementos de hardware que solo soportan el protocolo IPV4, y que no hay un documento de soporte que indique que la SNR ya cuenta con la transición</p>	INEFECTIVO	Primera Línea de Defensa Oficina de TI



Superintendencia de Notariado y Registro

No.	Código del Hallazgo	Descripción Hallazgo	Pronunciamiento y Recomendaciones OCIG	Estado	Responsable
		encontrando inconsistencias respecto al inventario de aplicativos y su validación de soporte al protocolo IPv6, como fue señalado en el numeral 5.8 del presente informe, contradiciendo lo señalado en la Guía de Transición de IPv4 a IPv6 para Colombia.- numeral 7.1 Fase I. Planeación de IPv6.	del protocolo IPv4 al IPv6, se determina que las acciones, aunque necesarias para la adopción del IPv6, aún no han logrado dar cumplimiento a la culminación del proceso de transición al protocolo IPv6 en convivencia con el protocolo IPv4 en la SNR y según los términos que fueron ajustados por MINTIC para la vigencia 2022. Por lo anterior, se considera que las acciones establecidas son INEFECTIVAS.		
7	20211021	No se presentaron evidencias de la realización de un convenio que permita establecer el cumplimiento frente al acuerdo marco de interoperabilidad para Gobierno Digital, situación por la cual se materializa el incumplimiento del numeral 2.2.1 -Elementos de Gobernanza de la Interoperabilidad, que señala: "Contrato de descripción del servicio de intercambio: Deberá existir un contrato de descripción del servicio de intercambio de información entre el proveedor y consumidor del servicio para garantizar la correcta "entrega" del servicio..."; en cuanto al Monitoreo y disponibilidad del servicio: "Los contratos de servicio de intercambio deben ser monitoreados a través de indicadores que darán cuenta de la disponibilidad del servicio de intercambio de información y deben estar disponibles en cualquier momento". Así mismo, se advierte sobre la necesidad de dar cumplimiento al Decreto No.1377 de 2013, artículo 4, en cuanto a la "Recolección de los datos personales" y al artículo 5 "Autorización". De otra parte, no se cuenta con evidencias de las diferentes actas de reunión realizadas, en atención de cada una de las actividades programadas, generando el riesgo de no contar con trazabilidad de las decisiones tomadas sobre el tema.	Para este hallazgo se plasmaron como acciones las siguientes, "Presentar PROTOCOLO TÉCNICO DE INTERCAMBIO DE INFORMACIÓN, con entidad del Estado que solicite interoperabilidad con la SNR." Esta actividad cuenta con fecha límite de cumplimiento al 30-06-2025 y se presentaron las siguientes evidencias: En la One Drive -Plan de Mejoramiento se observó pdf que contiene: 1. Protocolo Técnico firmado Minambiente. 2. Procolo técnico WS último propietario y segregados ICA. 3. Protocolo técnico WS último propietario y segregados Minambiente. En el desarrollo del presente informe se logró determinar que la acción propuesta se cumplió y fue efectiva, dado que se cuenta con los protocolos debidamente suscritos con distintas entidades, es decir, entre el proveedor y consumidor del servicio de información; se sugiere continuar documentando todo acuerdo donde exista la interoperabilidad. Por lo anterior, se recomienda realizar el cierre del presente hallazgo.	EFFECTIVO	Primera Línea de Defensa Oficina de TI
8	20211023	No se presentaron evidencias respecto al establecimiento de canales de comunicación, soportados en convenios a nivel nacional, con diferentes entidades (tales como: Coordinación Nacional de Seguridad Digital (Presidencia de la República); Comité de Seguridad Digital; CCP (Centro Cibernético Policial); ColCERT; Unidades cibernéticas de las Fuerzas Militares; CSIRT de Gobierno, entre otros), generando el riesgo de no contar con mecanismos para facilitar la cooperación, colaboración y asistencia entre las diferentes entidades estatales y la SNR, y con el fin de prevenir cualquier incidente digital.	Las acciones establecidas, fueron: "Generar formato para la documentación de contactos con autoridades y grupos de interés." Y "Divulgar y apropiar el formato para su diligenciamiento" Estas actividades tienen fecha límite de cumplimiento al 30-06-2025 y 30-11-2025, lo que significa que al cierre del presente informe están en desarrollo; no obstante, se revisó la One Drive encontrando que para la primera acción se subió un formato en Excel que no registra código, versión, ni fecha, por lo cual se determinó que está en borrador; y para la segunda actividad, no hay evidencias subidas a la One Drive.	EN DESARROLLO	Primera Línea de Defensa Oficina de TI



Superintendencia de Notariado y Registro

No.	Código del Hallazgo	Descripción Hallazgo	Pronunciamiento y Recomendaciones OCIG	Estado	Responsable
			<p>De otra parte, en desarrollo del presente informe tampoco se presentaron evidencias de la interacción de la SNR con las diferentes entidades estatales.</p> <p>Por lo anterior, se espera que al término de la fecha límite de cumplimiento de acciones, la OTI pueda tener las evidencias correspondientes a las acciones establecidas.</p>		
9	20211024	<p>Se observó que los documentos: Política de Seguridad de la Información, el procedimiento: Gestión de Incidentes de Seguridad de la Información, así como el Manual del SGSI, la Política de Gestión de Incidentes de Seguridad de la Información, la Política de Requerimientos Legales, Regulatorios y Contractuales, la Política de Seguridad de la Información por Dominio de la Norma NTC-ISO-IEC 27001:2013, entre otros, (estos últimos) fueron presentados por la Empresa Alina Tech S.A.S, en la vigencia 2019 y a la fecha de la auditoría, no han sido actualizados en su totalidad ni han sido aprobados y difundidos para su aplicación al interior de la entidad. Esta situación podría conllevar al riesgo de no lograr garantizar y exigir el buen uso de la información a todos los funcionarios, contratistas, proveedores, visitantes, terceros entre otros; a fin de darle cumplimiento a lo establecido el Decreto 1008 de 2018 lineamientos generales de la política de Gobierno Digital" artículo 2.2.9.1.2.2. Manual de Gobierno Digital. Lineamiento LI.SIS.16- MINTIC, Gobierno Digital, Manual del usuario, técnico y de operación de los sistemas de información. "La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe asegurar que todos sus sistemas de información cuenten con la documentación técnica y funcional debidamente actualizada."; Manual de Gobierno Digital, numeral 5.2. Anexo 2. Segmentación Elementos habilitadores: Arquitectura..."La entidad asegura que sus sistemas de información cuenten con la documentación técnica y funcional debidamente actualizada."</p>	<p>Hallazgo cuyas actividades se encuentran en desarrollo al cierre del informe, dado que la fecha máxima es al 22 dic.2022.</p> <p>Así mismo, en desarrollo del presente informe de seguimiento se realizaron recomendaciones frente al tema que se espera sean tenidas en cuenta para su mejora. Se espera que se logre avanzar en la documentación total de las acciones propuestas; tanto en su aprobación; socialización y ejecución de las actividades pendientes para contar con las evidencias documentales necesarias para su evaluación de efectividad. Por lo anterior se deja en desarrollo.</p>	EN DESARROLLO	Primera Línea de Defensa Oficina de TI
10	20211025	<p>Revisado el cuadro de mando del mes de Agosto/2020, se encuentra que existió un total de 931 vulnerabilidades de las cuales 889 vulnerabilidades están clasificadas con "Estado" – Pendiente de mitigación; de éstas existen 211 que han sido clasificadas como vulnerabilidad "Alta y Crítico" y cuyo "Estado de la vulnerabilidad" está en proceso o por definir. Así mismo, en el informe denominado "Informe Ejecutivo de Seguridad de la Información" del mes de agosto de 2020, se observó que registran la siguiente información: "Conforme a este gráfico se observa que a fecha 24 de Agosto de 2020,</p>	<p>Las acciones establecidas, fueron: "Ejecutar prueba de Ethical Hacking a la infraestructura tecnológica. Y Establecer plan de remediación para las vulnerabilidades o brechas encontradas", actividades establecidas para el 30 de marzo y 30 de abril de 2025, respectivamente.</p> <p>Aunque las actividades fueron cumplidas, y se estableció un plan documentado, no se evidenció su ejecución efectiva, por lo que el control se considera inefectivo.</p>	INEFECTIVO	Primera Línea de Defensa Oficina de TI



Superintendencia de Notariado y Registro

No.	Código del Hallazgo	Descripción Hallazgo	Pronunciamiento y Recomendaciones OCIG	Estado	Responsable
		aún existen amenazas de nivel crítico detectadas hace 18 años que aún no se han podido mitigar". Esta situación conlleva al riesgo de permitir a un ciberdelincuente obtener acceso de forma remota, sin necesidad de tener ningún tipo de autenticación, pudiendo afectarse la integridad, confidencialidad y disponibilidad de la información de la entidad.	La falta de evidencias documentadas y operativas, así como resultados verificables, limita la valoración del avance en la mitigación de las amenazas críticas, y demuestra una brecha entre la planeación y la ejecución. Se recomienda activar el plan, asignar responsables y establecer mecanismos de seguimiento o indicadores periódicos que aseguren y evidencien su cumplimiento.		
11	20220516	Se evidencian debilidades en la implementación de las Políticas de Gobierno Digital, y Seguridad Digital, asociadas con los siguientes aspectos de verificación (falta de seguimiento a los indicadores del Plan de Transformación Digital; estándares de accesibilidad y contenidos- ejm. acceso para personas con discapacidad sensorial e intelectual, que no han sido activados en la web; Inaplicación del lineamiento LI.ES.04- Proceso para evaluar y mantener la Arquitectura Empresarial; falta de publicación del PETI en la web; inexistencia de indicadores en el PETI, para cada una de las iniciativas de inversión; falta de un Plan de Comunicaciones con actividades, fechas y responsables de su ejecución; avance poco significativo en la implementación ipv6), los cuales fueron señalados e identificados en el presente informe, y de manera general, frente a cada uno de los temas verificados. Esta situación, pone en riesgo, la observancia frente a los lineamientos establecidos en el Manual de Gobierno Digital, para la Implementación de la Política de Gobierno Digital, conforme al Decreto 1008 de 2018	Hallazgo cuyas actividades se encuentran en desarrollo al cierre del informe, dado que la fecha máxima es al 22 dic.2022. Así mismo, en desarrollo del presente informe de seguimiento se realizaron recomendaciones frente al tema que se espera sean tenidas en cuenta para su mejora. Se espera que se logre avanzar en la documentación total de las acciones propuestas; tanto en su aprobación; socialización y ejecución de las actividades pendientes para contar con las evidencias documentales necesarias para su evaluación de efectividad. Por lo anterior se deja en desarrollo.	EN DESARROLLO	Primera Línea de Defensa Oficina de TI

De los 11 hallazgos evaluados relacionados con la implementación de las políticas de Gobierno Digital y Seguridad Digital, se encontraron 5 hallazgos en desarrollo, es decir que sus acciones están en periodo de ejecución; con 3 hallazgos que fueron evaluados como efectivos, por lo cual se recomendó su cierre; No obstante, 3 hallazgos resultaron inefectivos, por lo que se determinó que persisten debilidades en la implementación, seguimiento y verificación de resultados, debido a las observaciones consignadas en este informe, por lo cual se hace necesario realizar el ejercicio de análisis causa raíz, asignación de responsabilidades y efectuar el monitoreo con indicadores, en aras de asegurar la efectividad de las acciones, que redundará en el cumplimiento de los marcos MECI, MIPG y las directrices del MINTIC sobre gestión de riesgos y madurez digital institucional.

3. CONCLUSIONES Y RECOMENDACIONES GENERALES

Teniendo en cuenta el impacto generado por la implementación de los lineamientos de las políticas de Gobierno y Seguridad Digital, que buscan fortalecer la prestación de servicios de las Entidades Públicas hacia los ciudadanos mediante el uso de Tecnologías de la Información y las Comunicaciones (TIC), así como fomentar su aprovechamiento bajo estándares de seguridad de la información, resulta fundamental evaluar el estado



Superintendencia de Notariado y Registro

actual de su implementación en la SNR. Este análisis está centrado en la identificación de los avances y la aplicación de las políticas, en línea con el marco normativo establecido.

Como resultado de la evaluación y de manera general se encuentra que cada uno de los dominios que conforman el Modelo de Gestión y Gobierno de TI en la SNR, hacen importantes esfuerzos para que la entidad pueda disponer de los diversos componentes de TI, que con su ejecución e implementación permitirán habilitar con tecnología, los diferentes procesos y servicios de la entidad.

En ese sentido, se evidenció la necesidad de fortalecer los instrumentos de medición a la implementación de los lineamientos establecidos en las Políticas de Gobierno Digital y Seguridad Digital, por lo cual se **recomienda** a la Oficina de Tecnologías de la Información - OTI consolidar un instrumento que permita medir de manera específica, puntual y periódica, los avances de cada una de las líneas de acción o elementos definidos en las Políticas, que se cuente con la información que la clasifique y permita determinar un peso de criticidad o balance de cumplimiento.

Se **recomienda** fortalecer el ejercicio de Arquitectura de TI en la entidad, promoviendo su articulación con el grupo de innovación y desarrollo de la entidad, de acuerdo con las funciones asignadas en la estructura organizacional. Esta integración permitirá alinear las iniciativas tecnológicas e innovadoras con la estrategia institucional, potenciar el uso eficiente de los recursos, fomentar la interoperabilidad y la mejora continua, y consolidar un enfoque integral de madurez digital y gestión de la innovación pública, conforme a los lineamientos del MinTIC y el MIPG.

En la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), la entidad ha demostrado avances significativos en documentar las diferentes actividades de control; sin embargo, el proceso de identificación de activos de información se mantiene como un hito crítico para consolidar la gestión del riesgo digital en la Superintendencia; igualmente, la documentación de los procedimientos y manuales orientados a cubrir los controles del desarrollo de software y su ciclo de vida, documentación que es esencial para asegurar la implementación de prácticas seguras, trazables y controladas en el desarrollo de soluciones tecnológicas de la entidad, hacen que sea necesaria y prioritaria su inclusión al SIGI. Por lo que **se recomienda** agilizar su documentación, formalización, implementación, divulgación y apropiación, con el fin de mitigar posibles riesgos asociados a vulnerabilidades en el software, garantizar la protección de la información desde su diseño, fortaleciendo el cumplimiento normativo y regulatorio aplicable, como son los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y en cumplimiento con los requisitos establecidos por la norma ISO/IEC 27001, particularmente los controles relacionados con la adquisición, desarrollo y mantenimiento de los sistemas de información.

Se **recomienda** dar continuidad al rol del Oficial de Seguridad de la Información, reconociendo su papel fundamental en la implementación, seguimiento y mejora continua de las políticas de seguridad digital. Su participación activa permitirá garantizar el cumplimiento normativo, la protección de la información institucional y la promoción de entornos digitales seguros.

La implementación de IPv6 es una necesidad estratégica para garantizar la continuidad operativa, la escalabilidad y la seguridad de las redes institucionales; al respecto se evidenció que el personal de la OTI realizó pruebas para configurar el direccionamiento IPv6, pruebas ejecutadas en la vigencia 2025 y que fueron documentadas en el "*Plan de Pruebas Piloto*", el cual fue compartido al equipo auditor; no obstante existen pruebas piloto realizadas, se hace necesaria la adopción del protocolo IPv6 en toda su extensión y actualización, por lo cual se **recomienda** agilizar su implementación, de tal forma que permita las conexiones a IPv4 e IPv6 desde cualquier usuario; esto con el fin de dar cumplimiento al Art.3. de la Resolución No.01126 de 2021, que



Superintendencia de Notariado y Registro

señala: “**Plazo de adopción. Las entidades estatales del orden nacional que trata el artículo segundo de la presente resolución, deberán culminar el proceso de transición al protocolo IPv6 en convivencia con el protocolo IPv4 a más tardar el 30 de junio de 2022.**” No adoptar IPv6 expone a la entidad a riesgos como limitaciones de crecimiento, problemas de interoperabilidad, vulnerabilidades de seguridad no gestionadas y desventajas frente a estándares tecnológicos emergentes. Por tanto, se recomienda continuar con la ejecución del plan de transición progresiva hacia IPv6, asegurando la compatibilidad dual y la capacitación del personal técnico. Esta transición no solo es una medida de mitigación de riesgos, sino también una oportunidad para modernizar la infraestructura tecnológica y prepararse para los desafíos del ecosistema digital futuro.

Otro aspecto que se considera importante y **se recomienda** es dar continuidad a los análisis de vulnerabilidades a la infraestructura tecnológica de la entidad, fortaleciendo su alcance y frecuencia (incluyendo sistemas, redes, aplicaciones, bases de datos y la nube), como proceso de ciberseguridad para la identificación de puntos débiles como configuraciones incorrectas, software obsoleto y/o puertos abiertos innecesarios, para lograr corregirlos antes de que sean explotados por atacantes; esto con el fin de mantener un nivel adecuado de protección en la infraestructura tecnológica. Igualmente, se hace necesario y se **recomienda atender oportunamente las recomendaciones derivadas de dichos análisis, implementando las acciones correctivas y/o preventivas necesarias para mitigar los riesgos identificados**, dejando documentación de lo actuado. El No abordar estas observaciones puede dejar expuesta a la entidad frente a amenazas reales y comprometer la eficacia del sistema de gestión de seguridad de la información.

En el informe del FURAG y para las políticas de Gobierno y Seguridad Digital, existen actividades reportadas como pendientes de ejecución, por lo cual se **recomienda** realizar el análisis y validación de las recomendaciones resultantes, e incluirlas en los planes diseñados por la Oficina de Tecnologías de la Información, priorizando las necesarias para dar cumplimiento a los lineamientos establecidos en esta materia.

Asimismo, se **recomienda** mantener un seguimiento continuo y documentado a las acciones establecidas en el Plan de Mejoramiento Institucional, las cuales deben ser cumplidas en su totalidad, conforme a los plazos, responsables y evidencias definidos, en aras de asegurar la efectividad de las medidas correctivas y preventivas implementadas, y de tal forma que permita verificar la ejecución real de cada acción para evaluar su efectividad.

La ejecución inmediata de las recomendaciones aquí propuestas permitirán alcanzar resultados verificables en el corto plazo, fortalecer la madurez institucional en seguridad de la información y garantizar la conformidad con las Políticas de Gobierno y Seguridad Digital, así como los lineamientos del MinTIC y se constituye en una herramienta de retroalimentación para el Sistema de Control Interno de la SNR, permitiendo cumplir plenamente con los requerimientos del Decreto 767 de 2022 y el Decreto 1083 de 2015.

Copia de este mismo informe será remitido para su conocimiento y fines pertinentes, al líder de las Políticas de Gobierno y Seguridad Digital - Oficina de TI por la responsabilidad que le asiste, según el rol correspondiente y conforme al Modelo Integrado de Planeación y Gestión – MIPG.

Cordialmente,

MONICA AMATISTA JIMENEZ BARROS
Jefe Oficina de Control Interno

Proyectó: Luisa Nayibe Barreto López – Profesional Especializado OCI / Stella Reyes – Técnico OCI