



OCIG- 220

SNR2024IE014579

Bogotá, 02 de septiembre de 2024

Doctor

ROOSVELT RODRIGUEZ RENGIFO

Superintendente de Notariado y Registro

Ciudad

Asunto: Informe Interno de Seguimiento a las políticas de Gobierno y Seguridad Digital

Respetado Doctor:

Con el propósito de contribuir al fortalecimiento de los procesos y al mejoramiento continuo del Sistema de Control Interno Institucional y en ejercicio del rol de evaluación y seguimiento establecido en el artículo 17 del decreto 648 de 2017 y en concordancia con las funciones definidas en el artículo 16 del decreto 2723 de 2014 , respetuosamente la Oficina de Control Interno de Gestión se permite remitir el **Informe Interno de Seguimiento a las políticas de Gobierno y Seguridad Digital**, en cumplimiento al procedimiento de informe de Evaluación y seguimiento.

Durante los 15 días hábiles siguientes al recibo del presente informe, los líderes del proceso auditado e involucrados, deben presentar el Plan de Mejoramiento para las no conformidades identificadas en el desarrollo del seguimiento, el cual debe ser radicado en la Oficina Asesora de Planeación, al correo electrónico planes.mejoramiento@supernotariado.gov.co.

MONICA AMATISTA JIMENEZ BARROS

Jefe de Oficina de Control Interno de Gestión.

Anexo: Informe Interno de Seguimiento a las políticas de Gobierno y Seguridad Digital

Con copia a correo electrónico:

Ing. José Ricardo Acevedo Solarte. Jefe de Oficina OTI

Ing. Yaneth Constanza Rincón Pulido

Transcriptor: Luis Emilio Romero Mogollón / Alejandro Castro Ballesteros

Reviso: Jefe de Oficina Control Interno de Gestión.



Superintendencia de Notariado y Registro

INFORME DE SEGUIMIENTO A LA POLÍTICA DE GOBIERNO Y SEGURIDAD DIGITAL CORTE JUNIO 2024.

OBJETIVO

Realizar el seguimiento al estado de avance de la implementación de las Políticas de Gobierno Digital y Seguridad Digital, como parte de la dimensión con valores para los resultados que hace parte del Modelo Integrado de Planeación y Gestión – MIPG.

ALCANCE DEL SEGUIMIENTO

Comprende la revisión al estado de avance en la implementación de las políticas Nacionales de gobierno digital y seguridad digital, con accesiones adelantadas durante el periodo comprendido entre el 1 de noviembre de 2021 al 30 de junio de 2024.

MARCO NORMATIVO

- ✓ Decreto 088 de enero 2022. “Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea”
- ✓ 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”
- ✓ Ley 1341 de 2009 Art. 2 numeral 8 en cual se precisa: “Con el fin de lograr la prestación de servicios eficientes a los ciudadanos, las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones en el desarrollo de sus funciones. El Gobierno Nacional fijará los mecanismos y condiciones para garantizar el desarrollo de este principio. Y en la reglamentación correspondiente establecerá los plazos, términos y prescripciones, no solamente para la instalación de las infraestructuras indicadas y necesarias, sino también para mantener actualizadas y con la información completa los medios y los instrumentos tecnológicos.”
- ✓ Resolución 1951 de 2022. “Por la cual se establecen los requisitos, las condiciones y el trámite de la habilitación de los prestadores de servicios ciudadanos digitales especiales; se dan los lineamientos y estándares para la integración de estos servicios y la coordinación de los prestadores con la Agencia Nacional Digital”
- ✓ Decreto 1263 de julio 22 de 2022, “Por el cual se adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública”.
- ✓ 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



Superintendencia de Notariado y Registro

en su lugar, y cuya fuente de datos es el Formulario Único de Reporte de Avance en la Gestión – FURAG”.

- ✓ Decreto 1008 de 2018. "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”, en su artículo:2.2.9.1.2.2. Manual de Gobierno Digital. 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, el cual será elaborado y publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones, en coordinación con el Departamento Nacional de Planeación”.
- ✓ Anexo 1, Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías de la Información y las Comunicaciones febrero 2021, en el numeral 7.3.3 Plan de tratamiento de los riesgos de seguridad de la información.
- ✓ Manual de Gobierno digital, numeral 2.1 planear, 2.1.1 lineamientos de planeación, “las entidades públicas deberán formular un plan de transformación digital con horizonte a cinco años, incluyendo el uso de tecnologías emergentes y disruptivas”

METODOLOGIA

Para el desarrollo del presente seguimiento, se solicitó a la Oficina de Tecnologías de la Información -OTI, los soportes correspondientes a los cronogramas establecidos para dar cumplimiento a la implementación de las políticas objeto del presente seguimiento; se verificaron los soportes de la información remitida por la OTI.

Verificación en la página web de la Superintendencia, revisando los avances y acciones implementadas durante el periodo objeto del presente seguimiento, frente a los lineamientos y criterios de cada componente y habilitadores transversales definidos en el Autodiagnóstico de Gobierno Digital.

El seguimiento se realizó atendiendo la normatividad aplicable, efectuándose el levantamiento de la información, entrevistas, revisión de información disponible en la web, y análisis de la información aportada por la OTI.

DESARROLLO DEL SEGUIMIENTO.

Este seguimiento fue realizado con base en el análisis de diferentes muestras aleatorias seleccionadas y se fundamenta en el siguiente soporte documental: Procesos y Procedimientos del Sistema de Gestión de la entidad, página web, intranet, normas internas y externas y documentos aportados por el proceso como evidencia.

Teniendo en cuenta el Decreto 707 de mayo 16 de 2022, Art. 2.2.9.1.2.2, el cual estableció la obligatoriedad de aplicar el Manual para la implementación de la política de Gobierno Digital, y que este manual define los lineamientos, estándares, y acciones a ejecutar por parte de los sujetos obligados de esta política; se procedió a revisar su aplicación en la SNR, de acuerdo con lo señalado en la Política:

Política de Gobierno Digital: Entendida como el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el objetivo de 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



Superintendencia de Notariado y Registro

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.

Los elementos que componen la estructura de la Política de Gobierno Digital, son *Gobernanza e Innovación Pública Digital*, que son habilitados por cuatro elementos transversales: *Arquitectura, Cultura y apropiación, Seguridad y privacidad de la Información, y Servicios Ciudadanos Digitales*. Estos elementos se desarrollan a través de lineamientos y estándares, que son los requerimientos mínimos que todos los sujetos obligados deben cumplir para alcanzar la implementación de la política:



Verificación sobre la participación de los Ejecutores de la Política de Gobierno Digital en la SNR

Con el objetivo de identificar claramente los roles para la implementación de la Política de Gobierno Digital, se define un esquema institucional que vincula desde la Alta Dirección hasta las áreas específicas de la entidad en el desarrollo de la política y el logro de sus propósitos. A continuación, se presentan las instancias y sus responsables de la implementación en la Superintendencia:

1. Grupo de trabajo OTI

Se evidenció durante este seguimiento, que los grupos internos de trabajo de la Oficina de Tecnologías de la información elaboraron/actualizaron algunos procedimientos entre el 1 de noviembre de 2021 a la fecha del presente informe de seguimiento, los cuales se encuentran publicados en el Mapa de procesos de la SNR:



Superintendencia de Notariado y Registro



- SALIDA DE ELEMENTOS TECNOLÓGICOS EN LOS CENTROS DE CÓMPUTO OTI Y ORIP, fecha de aprobación : 14 de Junio de 2022, su objetivo es establecer el alcance del proceso de retiro de elementos tecnológicos y ejercer seguimiento de los activos de los Centros de Cómputo a cargo de la OTI, con el fin de mantener un control de estos, por medio de los soportes del control de registros de las redes, sistemas misionales y de los equipos de los usuarios finales así como para la actualización de los inventarios tecnológico; se actualizó la política de este procedimiento.
- INGRESO Y SALIDA DE PERSONAL A CENTRO DE CÓMPUTO (EN COLOCATION), aprobado el 14 de Junio de 2022, su objetivo es Implementar el protocolo de ingreso y salida de personal al Datacenter de la SNR mediante mecanismos de biometría e instrumentos construidos con el fin de salvaguardar la seguridad de la información que aloja cada uno de los elementos que resguarda la línea de Centro de Cómputo; se actualizó el 24 de marzo de 2022 el correspondiente “FORMATO DE INGRESO Y SALIDA DEL DATACENTER SNR, así como se actualizó la política de operación de este procedimiento.
- ATENCIÓN DE SOLICITUDES Y REQUERIMIENTOS DE ALMACENAMIENTOS Y SISTEMAS DE VIRTUALIZACION, aprobado el 14 de junio de 2022, objetivo: Gestionar la atención de solicitudes y requerimientos generados al área de almacenamiento y /o plataformas de virtualización (Exalogic, OVM, PCA y Vmware), con el fin de atender, solucionar y dar respuesta a las diferentes solicitudes reportados por los usuarios, de tal forma que se pueda brindar una solución oportuna, trabajando de la mano con el soporte especializado del fabricante cuando se requiera; se actualizó el correspondientes formatos “FORMATO: SOLICITUD PARA SISTEMAS DE VIRTUALIZACIÓN EXALOGIC, OVM, PCA o VMWARE” y “FORMATO DE SOLICITUDES DE ALMACENAMIENTO EXTERNO” de éste procedimiento
- DESARROLLO O ADQUISICIÓN Y REGISTRO DE SOFTWARE, aprobado el 22 de Marzo de 2023, su objetivo es Desarrollar o adquirir programas (software) de tecnología de la información para la ejecución de proyectos de tecnología con cualquier modalidad de contrato que se realice con la Superintendencia de Notariado y Registro, por medio de proyectos internos y/o externos de la Oficina de Tecnología de la información, que conlleven al cumplimiento de objetivos de la entidad como a los activos de información de los procesos de la SNR (Políticas, procedimientos, leyes, decretos, información histórica y lecciones aprendidas), de acuerdo con el marco normativo y/o documentos de la Política de Gobierno Digital y/o buenas prácticas de diseño de programas para la transformación digital, otro propósito es el de obtener toda la información necesaria para una implementación del software esperado, que cumplan con todos los requerimientos del área solicitante y culminando con el registro del mismo ante la entidad competente en Colombia.
- INGRESO DE ELEMENTOS TECNOLÓGICOS EN LOS CENTROS DE COMPUTO OTI, aprobado el 17 de junio de 2022 su objetivo es Establecer los lineamientos bajo los cuales se debe realizar el ingreso de los activos en los Centros de Cómputo a cargo de la OTI en la SNR, por medio del protocolo establecido, con el fin de controlar y conocer todos los elementos que se encuentran resguardados en estas instalaciones y mantener actualizados los inventarios tecnológicos de la SNR.
- RECONOCIMIENTO, MEDICIÓN Y PRESENTACIÓN DE LOS ACTIVOS INTANGIBLES, aprobado el 1 de febrero de 2022, cuyo objetivo es Reconocer contablemente los activos intangibles, mediante su costo y vida útil el cual puede ser medido con soportes de documentos o certificados para registrarlos



Superintendencia de Notariado y Registro

en la contabilidad SNR para el control sobre los recursos en cuestión y la existencia de beneficios económicos futuros.

Fue actualizada la caracterización de los procesos de la OTI:

- **GESTIÓN DE INCORPORACIÓN DE TECNOLOGÍA**, aprobado el 22 de marzo de 2023. objetivo: Evaluar las solicitudes de servicios de tecnología, estableciendo su viabilidad de acuerdo con la planeación estratégica de la entidad, así como el cumplimiento de normatividad jurídica, impacto del ciudadano y su interacción con otras entidades, mediante la planeación de nuevos proyectos y solicitudes tecnológicas viables, en un entorno supervisado y apoyado en buenas prácticas de Gerencia de Proyectos, Desarrollo de Software y Adquisición de Hardware, con el propósito de ejercer seguimiento, control a los proyectos y/o contratos generados a partir de la solicitud de Servicios de Tecnología, fortaleciendo la plataforma tecnológica de la Entidad (Hardware y Software) y manteniendo un esquema de alta disponibilidad y seguridad de la información.
- **GESTION DE RECURSOS DE TECNOLOGIA**, actualizado el 5 de mayo de 2023, su objetivo es Garantizar la planeación, administración, control, ejecución y seguimiento de los recursos de tecnología como son los tangibles (hardware) e intangibles (software o aplicaciones virtuales) mediante la priorización de requerimientos de los usuarios y de acuerdo al presupuesto asignado al área con el fin de fortalecer las operaciones, garantizando la seguridad y disponibilidad de la información para una adecuada implementación de la infraestructura tecnológica y óptima prestación de los servicios de la entidad hacia las partes interesadas y conforme a las necesidades de la transformación digital en la SNR.

Así mismo, fueron actualizaron o creados los siguientes formatos:

- Solicitudes de almacenamiento externo.
- Supervisión técnica contractual y seguimiento a proveedores de TI. (control forma de pago).
- Historia de usuarios para interoperabilidad
- Alcance del proyecto de interoperabilidad.
- Solicitud de servicios a Mintic / lenguaje común de intercambio – LCI
- Formato modelo indicios de deterioro intangibles

Por medio de esta labor, se busca articular esfuerzos al interior de la Entidad, para lograr avanzar en el proceso de transformación digital, mejorando su funcionamiento a través del uso de las TIC y fortaleciendo la relación del estado con los ciudadanos en desarrollo de las políticas del MIPG.

2. Comité Institucional de Gestión y Desempeño

Responsable de orientar la implementación de la Política de Gobierno Digital, de que trata el artículo 2.2.22.3.8 del Decreto 1083 de 2015; y en el numeral 6, señala. “*Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información*”. Este Comité, será el responsable de orientar la implementación de la Política de Gobierno Digital, conforme a lo establecido en el Modelo Integrado de Planeación y Gestión.

Teniendo en cuenta que la principal función de este Comité, se encuentra orientada hacia la implementación y operación de todas las políticas del Modelo Integrado de Planeación y Gestión -MIPG (entre las que se



Superintendencia de Notariado y Registro

encuentra Gobierno Digital); le corresponde articular todos los esfuerzos institucionales, recursos, metodologías y estrategias para el desarrollo de las políticas del MIPG y en esta medida, lograr que Gobierno Digital, se desarrolle enlazándola con las demás políticas, en el marco del Sistema de Gestión de la Entidad.

Mediante Resolución No. 0090 del 11 de enero de 2018, se crea el Comité Institucional de Gestión y Desempeño de la Superintendencia de Notariado y Registro y dentro de sus funciones establece la siguiente: “Artículo 3 Funciones son funciones del Comité Institucional de Gestión y Desempeño”, numeral 6. “Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información”.

Al respecto, en el seguimiento efectuado por la OCIG, se evidenciaron las reuniones de Comité realizadas con fechas:

REUNIONES DEL COMITÉ.

- 16 de noviembre de 2023.

Conceptualización del Modelo Integrado de Planeación y Gestión – MIPG; se lleva a cabo una presentación y se recalca la obligatoriedad que tienen las entidades del estado en su implementación. Adicionalmente y, teniendo en cuenta que las 19 políticas con que opera MIPG deben estar bajo el liderazgo de algún proceso, la OAP de acuerdo a un estudio realizado de acuerdo a las fusiones, competencias y roles de los líderes de los procesos, determinó las responsabilidades por política.

Para el caso de la oficina de Tecnologías de la Información -OTI, como proceso de apoyo, en la dimensión de Gestión con valores para resultados se le asignó la Política de Gobierno Digital y Seguridad Digital, en las cuales se encuentra trabajando.

- En comité institucional de Gestión y desempeño llevado a cabo el 30 de noviembre de 2023, se aprueba las políticas de MIPG y se reafirma la responsabilidad de la OTI en las mencionadas, Política de Gobierno Digital y Seguridad Digital.

3. Líder TIC

El responsable de liderar la implementación la Política de Gobierno Digital: es el director, jefe de oficina o coordinador de tecnologías y sistemas de la información y las comunicaciones o G-CIO (sigla en inglés de Government Chief Information Officer), o quien haga sus veces en la entidad, de acuerdo con el artículo 2.2.35.5. del Decreto 1083 de 2015. Las demás áreas de la respectiva entidad serán corresponsables de la implementación de la Política de Gobierno Digital en los temas de su competencia.

Como responsable de liderar la implementación de la Política de Gobierno Digital, el Jefe de la Oficina de Tecnologías y Sistemas de la Información y las Comunicaciones, hace parte del Comité Institucional de Gestión y Desempeño y responde directamente al Representante Legal de la entidad, de acuerdo con lo establecido en el artículo 2.2.35.4. del Decreto Único Reglamentario de Función Pública 1083 de 2015.

Así mismo, teniendo en cuenta que el nuevo enfoque de Gobierno Digital, se orienta hacia el uso de la tecnología, como una herramienta que habilita la gestión de la entidad para la generación de valor público, en este sentido, y en atención al rol que le compete, a la Oficina de Tecnologías de la información conforme a lo establecido en el art.147 de la ley 1955 de 2019, que establece que “Los proyectos estratégicos de transformación digital se orientarán por los siguientes principios:



Superintendencia de Notariado y Registro



1. Uso y aprovechamiento de la infraestructura de datos públicos, con un enfoque de apertura por defecto.
2. Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales.
3. Plena interoperabilidad entre los sistemas de información públicos que garantice el suministro e intercambio de la información de manera ágil y eficiente a través de una plataforma de interoperabilidad. Se habilita de forma plena, permanente y en tiempo real cuando se requiera, el intercambio de información de forma electrónica en los estándares definidos por el Ministerio TIC, entre entidades públicas. Dando cumplimiento a la protección de datos personales y salvaguarda de la información.
4. Optimización de la gestión de recursos públicos en proyectos de Tecnologías de la Información a través del uso de los instrumentos de agregación de demanda y priorización de los servicios de nube.
5. Promoción de tecnologías basadas en software libre o código abierto, lo anterior, sin perjuicio de la inversión en tecnologías cerradas. En todos los casos la necesidad tecnológica deberá justificarse teniendo en cuenta análisis de costo-beneficio.
6. Priorización de tecnologías emergentes de la Cuarta Revolución Industrial que faciliten la prestación de servicios del Estado a través de nuevos modelos incluyendo, pero no limitado a, tecnologías de desintermediación, DLT (Distributed Ledger Technology), análisis masivo de datos (Big data), inteligencia artificial (AI), Internet de las Cosas (IoT), Robótica y similares.
7. Vinculación de todas las interacciones digitales entre el Estado y sus usuarios a través del Portal Único del Estado colombiano.
8. Implementación de todos los trámites nuevos en forma digital o electrónica sin ninguna excepción, en consecuencia, la interacción del Ciudadano-Estado sólo será presencial cuando sea la única opción.
9. Implementación de la política de racionalización de trámites para todos los trámites, eliminación de los que no se requieran, así como en el aprovechamiento de las tecnologías emergentes y exponenciales.
10. Inclusión de programas de uso de tecnología para participación ciudadana y gobierno abierto en los procesos misionales de las entidades públicas.
11. Inclusión y actualización permanente de políticas de seguridad y confianza digital.
12. Implementación de estrategias público-privadas que propendan por el uso de medios de pago electrónicos, siguiendo los lineamientos que se establezcan en el Programa de Digitalización de la Economía que adopte el Gobierno nacional.
13. Promoción del uso de medios de pago electrónico en la economía, conforme a la estrategia que defina el Gobierno nacional para generar una red masiva de aceptación de medios de pago electrónicos por parte de las entidades públicas y privadas.



Superintendencia de Notariado y Registro

De acuerdo al Manual de Gobierno digital, numeral 2.1 planear, 2.1.1 lineamientos de planeación, “las entidades públicas deberán formular un plan de transformación digital con horizonte a cinco años, incluyendo el uso de tecnologías emergentes y disruptivas”; para el presente seguimiento la OTI aportó el PLAN DE TRANSFORMACIÓN DIGITAL VISIÓN DIGITAL Y HOJA DE RUTA 2021 – 2022, el cual no contempla actividades proyectadas a cinco años y tampoco se encuentra aprobado por el comité institucional; esta situación conlleva que la entidad no pueda alcanzar el objetivo de optimizar la gestión, generar valor público en la interacción digital entre ciudadano y Estado y lograr un impacto positivo en la calidad de vida de los ciudadanos mediante el uso de las TIC.

De otra parte, mediante la Resolución No.10243 de Dic. 2020, fue creado el Grupo Interno de Trabajo de Innovación y Desarrollo en la planta global de la SNR, el cual está adscrito a la Oficina de Tecnologías de la Información, encomendado entre otras funciones, las siguientes, a fin de lograr el propósito de la política:

1. Definir las políticas, metodologías y mecanismos técnicos de seguimiento, ejecución, evaluación y control de proyectos de innovación y desarrollo de software.
2. Facilitar la administración, desarrollo, ejecución y el control de proyectos de transformación digital en la entidad.
3. Orientar y articular la gestión de las tecnologías de la información con los objetivos estratégicos de la entidad.
4. Desarrollar mecanismos tecnológicos que permitan aumentar la eficiencia de la entidad y mejorar la forma como se prestan los servicios a los ciudadanos y otras entidades del estado mediante la innovación y construcción de productos tecnológicos.
5. Coordinar la identificación y orientación de soluciones tecnológicas a las necesidades de la entidad, aplicando marcos de referencia, estándares y atributos de calidad de software en el marco del ciclo de desarrollo e ingeniería de software.
6. Definir e implementar buenas prácticas en el diseño, desarrollo e implementación y mantenimiento del software para mejorar los procesos y procedimientos al interior de la entidad.
7. Impulsar e implementar proyectos de investigación, desarrollo e innovación de Tecnologías de la Información a partir de la articulación de grupos internos y externos a fin de fomentar la eficiencia administrativa, racionalizar los trámites y agilizar los servicios a cargo de la entidad.

Se recomienda involucrar al grupo interno de trabajo de innovación y desarrollo en la implementación de la Política de Gobierno Digital y Seguridad Digital. Este grupo, en conjunto con el líder TIC y el equipo correspondiente, deberá ejecutar activamente las funciones detalladas en la Resolución No. 10243 de diciembre de 2020

4. Acompañamiento del MINTIC

En la documentación aportada por el proceso, se observa que la SNR, a través de Mintic como líder de la Política de Gobierno Digital, ha recibido acompañamiento mediante la capacitación en Política de Gobierno Digital en el marco de MIPG, a partir de las preguntas del FURAG, organizada por Función pública y Mintic; también, calidad y procesos y sesión de construcción de PETI, socialización resultados del FURAG, Plan nacional de infraestructura, Actualización del marco de referencia de arquitectura empresarial, cédula sectorial de arquitectura empresarial, cédula sectorial de cultura y apropiación, servicios ciudadanos digitales, taller seguridad de la información, de la transformación al cambio, organizadas por Munjusticia.

Se recomienda dar continuidad a la actividad para fortalecer los aspectos claves en el proceso de implementación de la política de Gobierno Digital.



Superintendencia de Notariado y Registro

5. Verificación Realizada al Rol de Responsable de Seguridad de la Información

Atendiendo la necesidad de articular los esfuerzos institucionales, recursos, metodologías y estrategias para asegurar la implementación de las políticas en materia de Seguridad de la Información, incluyendo la Seguridad Digital, en la respectiva entidad, y según lo señalado en el Manual de Gobierno Digital, se debe designar un Responsable de Seguridad de la Información que a su vez responderá por la Seguridad Digital en la entidad, el cual debe pertenecer a un área que haga parte del direccionamiento estratégico o Alta Dirección (MIPG, 2017).

El responsable de Seguridad de la información será el líder del proyecto, escogido dentro del equipo designado en cada entidad y tendrá las responsabilidades establecidas en la guía de Roles y Responsabilidades del Modelo de Seguridad y Privacidad de la Información (Guía 4 - Roles y Responsabilidades), quien, a su vez, tiene responsabilidades asignadas dentro de cada dominio del Marco de Arquitectura Empresarial. El responsable de seguridad de la información deberá participar en los comités de desempeño institucional.

De conformidad con lo establecido en el numeral 7.2.3 Roles y responsabilidades, del Documento Maestro del MSPI, del Ministerio de Tecnologías de la Información y las Comunicaciones octubre 2021; la SNR, mediante Resolución No.4905 de mayo 13 de 2016 artículo décimo primero: Funciones del Oficial de seguridad, así como las suscritas en la Guía No.4 del Ministerio de las Tecnologías de la Información – Roles y Responsabilidades – Responsable de Seguridad de la Información, designó al ingeniero Hugo Alejandro Casallas Larrotta como oficial de Seguridad de la Información.

6. Plan Estratégico de Tecnologías de la Información – PETI

Dentro de la Política de Gobierno Digital, se detalla el Habilitador de Arquitectura, el cual contiene todas las temáticas y productos que deberán desarrollar las entidades en el marco del fortalecimiento de las capacidades internas de gestión de las tecnologías, de acuerdo con lo señalado en el Marco de Referencia de Arquitectura Empresarial; uno de los pilares de este habilitador y el Plan Estratégico de las Tecnologías de la Información (PETI), como herramienta que se utiliza para expresar la Estrategia de TI.

En revisión del Plan Estratégico de Tecnologías de la Información – PETI V.1 que se encuentra publicado en la página web de la entidad, se evidenció que no se han iniciado acciones de mejora para subsanar las observaciones emitidas en el informe de seguimiento a la Política de Gobierno Digital del año 2021, en los siguientes aspectos:

- ✘ Inexistencia de indicadores para cada una de las iniciativas de inversión, necesarios para poder realizar seguimiento y control al avance del PETI, en cuanto a los gastos de operación y las metas de la estrategia de TI.
- ✘ Plan de Comunicaciones, aunque en el numeral 15 del PETI, se comprometen a elaborar el Plan según las políticas de comunicaciones aprobadas en la Entidad, el PETI, no contiene este plan y no se encuentran definidas las actividades que se realizarán, los responsables y las fechas de su ejecución.

Se recomienda fortalecer la definición de indicadores en el PETI para una mejor evaluación de las iniciativas de inversión en tecnología; la definición de indicadores claros y medibles es fundamental para evaluar el éxito de las iniciativas y permitirá determinar si las iniciativas de inversión están generando los resultados esperados; adicionalmente, ayudará para una toma de decisiones basada en datos. Tener en cuenta para su construcción la Guía para la construcción y análisis de indicadores de gestión. V4, mayo de 2018.



Superintendencia de Notariado y Registro

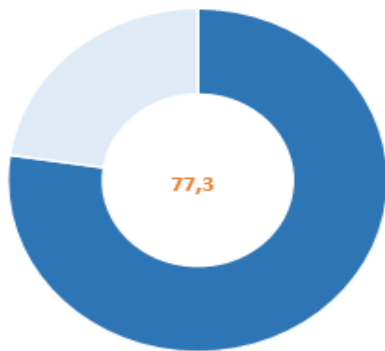
También se recomienda fortalecer la definición y ejecución del Pan de comunicaciones es fundamental para Alinear a las partes interesadas asegurando que todos compartan la misma visión del proyecto y sus objetivos, Evita la desinformación y las falsas expectativas, mitiga riesgos al identificar y gestionar de manera proactiva los posibles problemas de comunicación, y mejora la colaboración facilitando la comunicación y la colaboración entre los diferentes equipos involucrados en el proyecto.

7. Verificación a la Evaluación Realizada a Través del Formulario Único Reporte de Avances de la Gestión – FURAG, Vigencia 2023

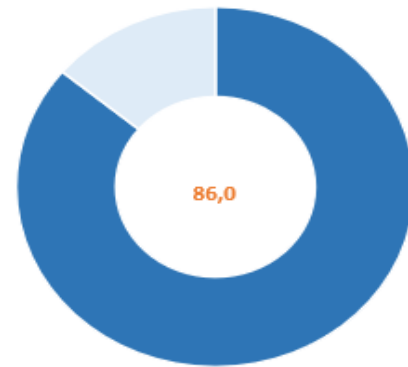
Teniendo en cuenta que el FURAG, es el instrumento que permite medir anualmente a las entidades públicas en el ejercicio de la gestión y desempeño de su labor, a continuación, se presentan los principales resultados alcanzados por la Oficina de Tecnologías en las Políticas de Gobierno Digital y de Seguridad Digital (fortalezas y debilidades), de acuerdo con los resultados publicados por el DAFP.

Índices de las políticas de gestión y desempeño:

P7 GOBIERNO DIGITAL



P8 SEGURIDAD DIGITAL



Índice desagregado	Puntaje consultado	Promedio grupo par
GOBIERNO DIGITAL: Arquitectura	73,7	73,5
GOBIERNO DIGITAL: Cultura y apropiación	83,3	75,1
GOBIERNO DIGITAL: Decisiones basadas en datos	71,4	67,5
GOBIERNO DIGITAL: Estado abierto	96,5	88,3
GOBIERNO DIGITAL: Gobernanza	88,9	75,4
GOBIERNO DIGITAL: Innovación Pública Digital	69,4	56,3
GOBIERNO DIGITAL: Proyectos de Transformación Digital	44,4	84,2
GOBIERNO DIGITAL: Seguridad y Privacidad de la información	63,6	75,1
GOBIERNO DIGITAL: Servicios Ciudadanos Digitales	28,6	16,2
GOBIERNO DIGITAL: Servicios y Procesos Inteligentes	41,2	51,8



Superintendencia de Notariado y Registro

Índice desagregado	Puntaje consultado	Promedio grupo par
SEGURO DIGITAL: Asignación de Recursos	85,4	66,9
SEGURO DIGITAL: Despliegue de Controles	60,0	84,6
SEGURO DIGITAL: Implementación Lineamientos de Política	91,7	76,6

Se observa en los resultados del FURAG de la vigencia 2023; que en la entidad, se identifican las debilidades enmarcadas en los temas de Gobierno digital, servicios ciudadanos Digitales donde se obtuvo un puntaje de 28.6, proyectos de transformación digital con 44,4 y en Seguridad Digital, Despliegue de controles con 60,0 puntos, representados como los temas con menor puntaje obtenido. Por el contrario, los aspectos con mayor fortaleza son Gobierno Digital, estado abierto con 96.5 y Seguridad Digital, Implementación lineamientos de política con 91.7.

Se recomienda que por parte de la OTI Fortalecer la Estrategia de Servicios Ciudadanos Digitales y Proyectos de Transformación Digital, así como despliegue de controles, con el fin de obtener un mayor impacto positivo en la entidad y, en términos de calidad y eficiencia en los servicios ciudadanos digitales y proyectos de transformación digital.

8. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

De conformidad con el Anexo 1, Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías de la Información y las Comunicaciones febrero 2021, en el numeral 7.3.3 Plan de tratamiento de los riesgos de seguridad de la información la entidad debe:

Lineamiento: Definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información, que permita:

- Seleccionar las opciones (controles) pertinentes y apropiadas para el tratamiento de riesgos.
- Elaborar una declaración de aplicabilidad que contenga: los controles necesarios, su estado de implementación y la justificación de posible exclusión.
- Definir un plan de tratamiento de riesgos que contenga, fechas y responsables con el objetivo de realizar trazabilidad.
- Los dueños de los riesgos deben realizar la aprobación formal del plan de tratamiento de riesgos y esta aceptación debe llevarse a la revisión por dirección en el Comité Institucional y de Desempeño, o quien haga sus veces.

Propósito: Estructurar una metodología que permita definir las acciones que debe seguir la Entidad para poder gestionar los riesgos de seguridad y privacidad de la información.

Entradas recomendadas:

- ✓ Inventario de activos de información de la Entidad.
- ✓ Valoración de los riesgos de seguridad de la información.

Salidas:

- ✓ Plan de tratamiento de riesgos aprobado por los dueños de los riesgos y el comité institucional de gestión y desempeño (Decreto 612 de 2018 Publicación antes de 31 de enero de cada vigencia).
- ✓ Declaración de aplicabilidad, aceptada y aprobadas en el comité de gestión institucional.



Superintendencia de Notariado y Registro

Para el desarrollo del presente seguimiento, el proceso manifiesta que “el equipo de seguridad de la información viene trabajando de la mano con la Oficina Asesora de Planeación en la integración de la gestión de activos y riesgos de seguridad de la información dentro de la metodología de gestión de riesgos institucional”.

Ya que no se evidencia avance en la elaboración del Plan de tratamiento de riesgos del SGSI se recomienda dar celeridad a ésta actividad toda vez que se requiere identificar claramente todas aquellas amenazas que pueden impactar negativamente en los objetivos de seguridad de la información de la SNR y así, proteger y preservar la confidencialidad, la integridad y la disponibilidad de la información crítica, valiosa y sensible de la entidad.

9. Plan de Seguridad y Privacidad de la información.

Dentro de la revisión documental de la información aportada por el proceso, no se observó evidencia del desarrollo del Documento Plan de Recuperación de Desastres.

Se recomienda que teniendo como base la Guía No. 10, Guía para la preparación de las TIC para la continuidad del negocio, se implemente un proceso de preservación de la información ante situaciones disruptivas, que permita minimizar el impacto y recuperación por pérdida de activos de información de la SNR, hasta un nivel aceptable mediante la combinación de controles preventivos y de recuperación.

10. Verificación efectuada a las directrices de usabilidad que cumple la entidad en su sitio Web

De acuerdo al diagnóstico de usabilidad y, frente a los lineamientos y metodologías para Gobierno Digital establecidos en la Guía para la implementación de la usabilidad web, la SNR se encuentra en un 57% de cumplimiento de los mencionados criterios de usabilidad, observándose incumplimiento en aspectos relacionados con Visibilidad del estado del sistema, coincidencia entre el sistema y el mundo real, suministrar al usuario el control y la libertad, consistencia y estándares, prevención de errores, reconocer en lugar de recordar, ayuda al usuario a reconocer, diagnosticar y recuperarse de los errores, ayuda y documentación.

Se recomienda iniciar las acciones pertinentes para dar cumplimiento a la totalidad de los criterios de usabilidad establecidos en la Guía para la implementación de la usabilidad web.

VERIFICACIÓN PLAN DE MEJORAMIENTO

Plan de mejoramiento suscrito con la Contraloría General de la República

Según lo observado en el Plan de mejoramiento vigente, no se encuentran hallazgos asociados a la Política de Gobierno y Seguridad Digital.

Plan de mejoramiento Institucional.

Se procede con la evaluación de las acciones de mejora y se emite pronunciamiento de efectividad.



Superintendencia de Notariado y Registro

Código	Descripción No Conformidad	Pronunciamiento y Recomendaciones OCIG	Estado	Responsable
20211011	No se evidencian Manuales y formatos estandarizados, para el uso de los nuevos aplicativos o desarrollos tecnológicos implementados en la vigencia 2020, con ocasión a la emergencia sanitaria declarada por el Gobierno Nacional, por causa de la pandemia Covid-19, en atención a las nuevas prácticas emprendidas para la atención del trabajo en casa, a fin de que se asegure la transferencia de la información a los usuarios de estos aplicativos, para garantizar el cumplimiento de los controles en los procesos y prevenir cualquier desviación que ponga en riesgo el mejoramiento y la continuidad en la prestación del servicio misional. Se advierte sobre la necesidad de avanzar con prontitud en la documentación de estos productos, 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."	Se encuentra publicado en el portal Web Guía de radicación, creación de user oficina, Notarías, anexo técnico REL. Se evidencia instructivos trabajo remoto en Folio IRIS, SIN IRIS, SIR IRIS; En SISG-Vicky se crearon modulo gestión trámites internos. Capacitación en Teams a nivel nacional. Las acciones fueron efectivas, se recomienda el cierre del hallazgo	ESTADO DEL HALLAZGO: EFECTIVO	Oficina de Tecnologías de la Información



Superintendencia de Notariado y Registro

Código	Descripción No Conformidad	Pronunciamiento y Recomendaciones OCIG	Estado	Responsable
20211014	No obstante, evidenciarse en la Entidad, la prestación del servicio de soporte técnico o mesa de ayuda tecnológica para brindar solución al reporte de incidentes y solicitudes de los usuarios en cada una de las Orip y dependencias del Nivel Central de la Entidad, mediante los acuerdos de nivel de servicio (ANS) establecidos; y encontrarse un documento en borrador, que contiene información parcial sobre el trámite que se debe adelantar para atender el primer nivel de servicios de TI, no se evidencia la formalización y aprobación de un procedimiento documentado que detalle cada una de las actividades, puntos de control, roles y responsabilidades para todos los niveles de soporte de acuerdo con los requerimientos realizados, en cumplimiento a los lineamientos de 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 los lineamientos LI.SIS.19- MINTIC - Sistema de Información establece: “La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, debe establecer criterios de aceptación y definir Acuerdos de Nivel de Servicio (ANS) cuando se tenga contratado con terceros el mantenimiento de los sistemas de información.” Se deben tener en cuenta las etapas de	Se observa documento ESTUDIOS PREVIOS PARA CONTRATAR EL SERVICIO DE OPERACIÓN DE LA SNR Y OFICINAS DE REGISTRO A NIVEL NACIONAL; se observa borrador del PROCEDIMIENTO: GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN, sin embargo, el mismo no está aprobado ni publicado en el portal web de la SNR. Se recomienda cargar evidencias que soporten el cumplimiento de las acciones propuestas	ESTADO DEL HALLAZGO: INEFECTIVO	Oficina de Tecnologías de la Información



Superintendencia de Notariado y Registro

Código	Descripción No Conformidad	Pronunciamiento y Recomendaciones OCIG	Estado	Responsable
	transición, prestación y devolución de los mismos, para asegurar la continuidad de los sistemas de información involucrados.” y LI.ST.09-Soporte a los servicios tecnológicos – “La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir e implementar el procedimiento para atender los requerimientos de soporte de primer, segundo y tercer nivel, para sus servicios de TI, a través de un único punto de contacto como puede ser una mesa de servicio. “Lo anterior, pone en riesgo la continuidad en la prestación del servicio misional y el cumplimiento de los objetivos de los procesos, entre otros.			
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	En la validación realizada para el presente informe de seguimiento, no se observó evidencia del desarrollo del Documento Plan de Recuperación de Desastres. Se recomienda que se implemente un proceso de preservación de la información ante situaciones disruptivas, que permita minimizar el impacto y recuperación por pérdida de activos de información de la SNR, hasta un nivel aceptable mediante la combinación de	ESTADO DEL HALLAZGO: INEFECTIVO, RECURRENTE.	Oficina de Tecnologías de la Información



Superintendencia de Notariado y Registro

Código	Descripción No Conformidad	Pronunciamiento y Recomendaciones OCIG	Estado	Responsable
	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.	controles preventivos y de recuperación. El hallazgo persiste		
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	Se observa un PROTOCOLO TÉCNICO DE INTERCAMBIO DE INFORMACIÓN de la SNR con otras entidades; sin embargo, no se evidencia avances para establecer contrato de descripción del servicio de intercambio de información para dar cumplimiento al acuerdo marco de interoperabilidad de Gobierno Digital. El hallazgo persiste, se recomienda análisis causa raíz, reformular y reprogramar de acciones	ESTADO DEL HALLAZGO: INEFECTIVO	Oficina de Tecnologías de la Información



Superintendencia de Notariado y Registro

Código	Descripción No Conformidad	Pronunciamiento y Recomendaciones OCIG	Estado	Responsable
	trazabilidad de las decisiones tomadas sobre el tema.			
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</p>	<p>La SNR cuenta con la Política General y políticas específicas del Sistema de Seguridad de la Información; sin embargo, no se evidencia avance en el establecimiento de las demás políticas, manuales y procedimientos como parte del cumplimiento a los lineamientos de la política de Gobierno Digital. El hallazgo persiste, se recomienda análisis causa raíz, reformular y reprogramar de acciones</p>	ESTADO DEL HALLAZGO: INEFECTIVO	Oficina de Tecnologías de la Información



Superintendencia de Notariado y Registro

Código	Descripción No Conformidad	Pronunciamiento y Recomendaciones OCIG	Estado	Responsable
	habilitadores: Arquitectura..."La entidad asegura que sus sistemas de información cuenten con la documentación técnica y funcional debidamente actualizada."			
20220516	<p>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 sw 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.</p> <p>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</p>	<p>Se sigue evidenciando debilidades en la implementación de las Políticas de Gobierno Digital, Seguridad Digital y arquitectura empresarial, toda vez que los avances son insipientes. El hallazgo persiste, se recomienda análisis causa raíz, reformular y reprogramar de acciones.</p>	ESTADO DEL HALLAZGO: INEFECTIVO,	Oficina de Tecnologías de la Información
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</p>	<p>En revisión realizada para el presente informe de seguimiento, no se evidencia avance en la elaboración del</p>	INEFECTIVO, RECURRENTE	Oficina de Tecnologías de la Información.



Superintendencia de Notariado y Registro

Código	Descripción No Conformidad	Pronunciamiento y Recomendaciones OCIG	Estado	Responsable
	<p>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,</p>	<p>Plan de tratamiento de riesgos del SGSI. Se recomienda dar celeridad a ésta actividad toda vez que se requiere identificar claramente todas aquellas amenazas que pueden impactar negativamente en los objetivos de seguridad de la información de la SNR y así, proteger y preservar la confidencialidad, la integridad y la disponibilidad de la información crítica, valiosa y sensible de la entidad.</p>		



Superintendencia de Notariado y Registro

Código	Descripción No Conformidad	Pronunciamiento y Recomendaciones OCIG	Estado	Responsable
	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 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.			

MAPA DE ASEGURAMIENTO

Frente al aspecto de Política de Gobierno y Seguridad Digital, se realizó el seguimiento a la función de aseguramiento o actividad de control que se debe adelantar, denominada: 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.

En revisión de la solicitud de comisiones para realizar las auditorías internas y sensibilización del sistema de seguridad de la información del mes de octubre de 2023, como soporte para el cumplimiento de las actividades establecidas en el mapa de aseguramiento, se evidenció que dicha información no cumple con la totalidad de los atributos de función de aseguramiento para la evaluación de confianza; lo anterior, teniendo en cuenta que no es posible evidenciar la realización de dichas auditorías.

Como resultado de la verificación de la información suministrada, la evaluación de los criterios de la función de aseguramiento del cumplimiento de las actividades de control propuesta por la Oficina de Tecnologías de la Información, se obtuvo la siguiente calificación; a) Objetivo y Alcance de la función de aseguramiento: 2, b) metodología: 3 c) Responsable: 3, d) Comunicación: 0, dando como resultado una calificación de la función de aseguramiento de 2,2 y con un nivel de confianza correspondiente a bajo aseguramiento, de acuerdo valores definidos en los criterios evaluadores de la función.



Superintendencia de Notariado y Registro

Lo anterior imposibilita la tomar decisiones oportunas y efectivas por parte de la Alta Dirección frente a posibles desviaciones o incumplimiento en la Normatividad Vigente y aplicable a la entidad respecto a la Política del Sistema de Gestión de Seguridad de la Información.

Como conclusión, siendo inefectivas las actividades de control definidas para el ASPECTO CLAVE DE ÉXITO relacionados con SISTEMA DE SEGURIDAD DE LA INFORMACIÓN, se advierte sobre la necesidad reevaluar su formulación, de tal forma que, se fortalezcan los controles para prevenir, mitigar y evitar la materialización de riesgos de incumplimiento de la Normatividad Vigente y aplicable a la entidad enfocada a la Política del Sistema de Gestión de Seguridad de la Información.

Así mismo, se recomienda fortalecer las actividades del mapa de aseguramiento del Proceso de Tecnologías de la Información, evaluando la efectividad de los planes, programas, proyectos de TIC y sistemas de información, entre otros temas misionales claves para la operación y el cumplimiento de objetivos estratégicos (considerando el mayor impacto presupuestal y reputacional).

CONCLUSIONES Y RECOMENDACIONES

- ✓ La SNR por medio del Ministerio de Tecnologías de la Información, como líder de la Política de Gobierno Digital, ha realizado acompañamiento y la capacitación en Política Gobierno Digital en el marco de MIPG, también, calidad y procesos y sesión de construcción de PETI, socialización resultados del FURAG, Plan nacional de infraestructura, Actualización del marco de referencia de arquitectura empresarial, cédula sectorial de arquitectura empresarial, cédula sectorial de cultura y apropiación, servicios ciudadanos digitales, taller seguridad de la información, de la transformación al cambio. Se recomienda dar continuidad a la actividad para fortalecer los aspectos claves en el proceso de implementación de la política de Gobierno Digital.
- ✓ De conformidad con lo establecido en el numeral 7.2.3 Roles y responsabilidades, del Documento Maestro del MSPI, del Ministerio de Tecnologías de la Información y las Comunicaciones octubre 2021; la SNR, mediante Resolución No.4905 de mayo 13 de 2016 artículo décimo primero: Funciones del Oficial de seguridad, así como las suscritas en la Guía No.4 del Ministerio de las Tecnologías de la Información – Roles y Responsabilidades, la entidad cuenta con un Responsable de Seguridad de la Información.
- ✓ Frente a la implementación de usabilidad web, la SNR se encuentra en un 57% de cumplimiento de los mencionados criterios de usabilidad, observándose incumplimiento en aspectos relacionados con Visibilidad del estado del sistema, coincidencia entre el sistema y el mundo real, suministrar al usuario el control y la libertad, consistencia y estándares, prevención de errores, reconocer en lugar de recordar, ayuda al usuario a reconocer, diagnosticar y recuperarse de los errores, ayuda y documentación. Se recomienda iniciar las acciones pertinentes para dar cumplimiento a la totalidad de los criterios de usabilidad establecidos en la Guía para la implementación de la usabilidad web.
- ✓ Se observa en los resultados del FURAG de la vigencia 2023; que en la entidad, se identifican debilidades enmarcadas en los temas de Gobierno digital, servicios ciudadanos Digitales donde se obtuvo un puntaje de 28.6; proyectos de transformación digital con 44,4 y en Seguridad Digital, Despliegue de controles con 60,0 puntos.
Por el contrario, los aspectos con mayor fortaleza son Gobierno Digital, estado abierto con 96.5 y Seguridad Digital, Implementación lineamientos de política con 91.7 puntos.



Superintendencia de Notariado y Registro

Se recomienda que por parte de la OTI Fortalecer la Estrategia de Servicios Ciudadanos Digitales y Proyectos de Transformación Digital, así como despliegue de controles, con el fin de obtener un mayor impacto positivo en la entidad y, en términos de calidad y eficiencia en los servicios ciudadanos digitales y proyectos de transformación digital.

- ✓ Se recomienda fortalecer la definición de indicadores en el PETI para una mejor evaluación de las iniciativas de inversión en tecnología; la definición de indicadores claros y medibles es fundamental para evaluar el éxito de las iniciativas y permitirá determinar si las iniciativas de inversión están generando los resultados esperados; adicionalmente, ayudará para una toma de decisiones basada en datos. Tener en cuenta para su construcción la Guía para la construcción y análisis de indicadores de gestión. V4, mayo de 2018.
- ✓ Se recomienda fortalecer la definición y ejecución del Plan de comunicaciones es fundamental para Alinear a las partes interesadas asegurando que todos compartan la misma visión del proyecto y sus objetivos, evita la desinformación y las falsas expectativas, mitiga riesgos al identificar y gestionar de manera proactiva los posibles problemas de comunicación, y mejora la colaboración facilitando la comunicación y la colaboración entre los diferentes equipos involucrados en el proyecto.
- ✓ Se recomienda involucrar al grupo interno de trabajo de innovación y desarrollo en la implementación de la Política de Gobierno Digital y Seguridad Digital. Este grupo, en conjunto con el líder TIC y el equipo correspondiente, deberá ejecutar activamente las funciones detalladas en la Resolución No. 10243 de diciembre de 2020.
- ✓ Para el presente seguimiento la OTI aportó el plan de transformación digital visión digital y hoja de ruta 2021 – 2022, el cual no contempla actividades proyectadas a cinco años y tampoco se encuentra aprobado por el comité institucional. Se recomienda la actualización del Plan de Transformación Digital, ya que la situación actual conlleva el riesgo de que la entidad no pueda alcanzar el objetivo de optimizar la gestión, generar valor público en la interacción digital entre ciudadano y Estado y lograr un impacto positivo en la calidad de vida de los ciudadanos mediante el uso de las TIC.
- ✓ Para efectos de hacer seguimiento al estado de avance en la implementación de la Política de Gobierno Digital, la entidad debe realizar el autodiagnóstico general de la Política de Gobierno Digital, a través de la herramienta dispuesta para tal fin.

Cordialmente,

MONICA AMATISTA JIMENEZ BARROS.
Jefe Oficina de Control Interno de Gestión.

Proyectó: Luis Emilio Romero Mogollón / Alejandro Castro Ballesteros.