INFORME DE AUDITORÍA DE GESTIÓN

Macroprocesos: TECNOLOGÍAS DE LA INFORMACIÓN
Lider del Macroproceso: Wilson Barrios Delgado
Procesos: Tecnologías de la Información

Lugar: Oficina de Tecnologías de la Información, Nivel Central – Auditoría remota

Objetivo de la Auditoría: Verificar los controles establecidos para el manejo del Estado de Emergencia Económica, Social y Ecológica en la entidad, en lo relacionado con la gestión adecuada de la información; su generación, distribución, control y almacenamiento de la misma, a través de los sistemas de información y en atención al estado de emergencia; así mismo, evaluar el avance alcanzado en la implementación de las Políticas de Gobierno Digital y Seguridad Digital en la Superintendencia de Notariado y Registro, de conformidad con la lista de chequeo.

Alcance de la Auditoría: Comprende la evaluación al Macroproceso de Tecnologías de la Información, en lo relacionado con algunas de las actividades desarrolladas para la atención de la medida de emergencia, como herramienta esencial para permitir la protección de la vida y la salud de los funcionarios; así como verificar el avance alcanzado en la implementación de las Políticas de Gobierno Digital y Seguridad Digital, tomando como criterio de auditoría la regulación externa e interna sobre el particular, y que delimitan su funcionamiento y ejecución; con los respectivos registros, indicadores, planes de mejoramientos y gestión del riesgo, por el periodo comprendido entre el 1 de Septiembre de 2019 a Septiembre de 2020.

Criterios de la Auditoría: Revisión de los soportes documentales y digitales que reposan en el Macroproceso en cumplimiento a los procesos y procedimientos desarrollados, en cumplimiento de la siguiente normatividad:

1- Decreto 491/2020, “Por el cual se adoptan medidas de urgencia para garantizar la atención y la prestación de los servicios por parte de las autoridades públicas y los particulares que cumplan funciones públicas y se toman medidas para la protección laboral y de los contratistas de prestación de servicios de las entidades públicas, en el marco del Estado de Emergencia Económica, Social y Ecológica” en lo que tiene que ver con el uso de tecnologías de la información y de acuerdo con el alcance de la auditoría. -Artículo 3.
2- Decreto 1008 de 2018 ""Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y ...""
3- CONPES 3854 POLÍTICA NACIONAL DE SEGURIDAD DIGITAL
4- Decreto 1499 de 2017 – “Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015- MIPG-Modelo Integrado de Planeación y Gestión""
5- Directiva Presidencial No.02 de 2019- SIMPLIFICACIÓN DE LA INTERACCIÓN DIGITAL ENTRE LOS CIUDADANOS Y EL ESTADO
6- Directiva Presidencial No.02 de 2020 - MEDIDAS PARA ATENDER LA CONTINGENCIA GENERADA POR EL COVID-19, A PARTIR DEL USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES (TIC).
7- Decreto 1078 de 2015 - Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.- avances carpeta ciudadana.
8- Decreto 620 de 2020 - ""Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011. los literales e. j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales"". – Avances
9- Resolución MINTIC, Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos. – Avances
10- Norma Técnica Colombiana ISO-27001 Sistema de Gestión de Seguridad de la Información e ISO-27002 guía de buenas prácticas de seguridad de la información-MPSI MINTIC
11- Ley 23 de 1982 ""Sobre derechos de autor”
12- Decreto 2723 de 2014, Art.17 - FUNCIONES OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
13- FURAG: Gobierno Digital y Seguridad Digital
14- Verificar la gestión de los riesgos asociados al Macroproceso.

15- Manuales, Instructivos y Procedimientos Internos; y Demás normas vigentes aplicables a los sistemas objeto y alcance de la auditoria.
La demás normatividad vigente que regula los procesos auditados, de acuerdo con la lista de chequeo."

Equipo Auditor: Luisa Nayibe Barreto López, María Stella Reyes Beltrán, Hugo Alfonso Cepeda.

Tipo de Informe: Informe Final de Auditoría realizada al Macroproceso Tecnologías de la Información

Metodología: El presente informe fue realizado bajo la normatividad señalada en los criterios de auditoría. Para validar el cumplimiento dado a la normatividad vigente y a las actividades de los procedimientos de la muestra seleccionada, se tomaron muestras aleatorias de los diferentes documentos que soportan la gestión efectuada por la Oficina de Tecnologías de la Información, los cuales fueron enviados a través de correo electrónico y en presentaciones virtuales.

Metodológicamente se realizaron las siguientes actividades:
-Se realizaron reuniones de planeación de auditoría con el equipo auditor designado de la Oficina de Control interno.
-Se elaboró y comunicó a los auditados, el Plan de Auditoría, mediante radicado No. SNR2020IE015069 del 27 de octubre de 2020.
-Se determinó la muestra de temas relacionados a auditar, relacionados con el Decreto 491/2020, en lo relacionado con el uso de las tecnologías de la información, en el marco del Estado de Emergencia Económica, Social y Ecológica, declarada por el gobierno nacional; la Política de Gobierno Digital y de la Política de Seguridad Digital.
-Considerando el tiempo de la auditoría, el talento humano disponible y los recursos técnicos y tecnológicos para la ejecución de la auditoría, se decide evaluar una muestra de 13 elementos a ser revisados.
-El equipo auditor elaboró las listas de verificación.
-Se realizó revisión documental y de la información recopilada con los soportes aportados por los responsables.
-Se realizó una mesa de trabajo del equipo auditor con la Jefatura de la Oficina de Control Interno, el día 9 de diciembre de 2020, para verificar el avance de auditoría.
-Finalmente, el equipo auditor realizó sesiones de trabajo para analizar los resultados de la revisión documental y los resultados de la auditoría, con el fin de realizar la clasificación de la información.
-Se realizó el cierre de la auditoría el día 11 de diciembre/2020, donde se rindió un informe verbal al líder del macroproceso auditado, con los principales resultados obtenidos.
-Finalmente, el equipo auditor se reunió para analizar la información recolectada para la elaboración del informe preliminar.
-Se consolidó el informe preliminar.
-Se enviará el informe preliminar al líder de la auditoria y a las partes interesadas para que realicen la revisión y retroalimentación correspondiente.
-Por parte de la Oficina de Control Interno, la responsabilidad como evaluador independiente, consiste en producir un informe objetivo que contenga las observaciones, si hay lugar a ellas, sobre el acatamiento a las disposiciones legales tanto externas como internas y las recomendaciones que le permitan a la alta dirección tomar decisiones de mejora en la gestión institucional.
- Conforme con lo establecido en el parágrafo del artículo 9 de la Ley 87 de 1993, Control Interno utiliza mecanismos de verificación y evaluación que recogen normas de auditoría generalmente aceptadas y la aplicación de principios como integridad, presentación imparcial, confidencialidad e independencia, los cuales se encuentran sustentados en el enfoque basado en evidencias.

Nota: Es responsabilidad de la Oficina de Tecnologías de la Información y las dependencias que aportaron soportes, el contenido de la información suministrada.

Limitaciones: No se presentaron limitaciones, contando con toda la disposición y colaboración por parte de los auditados.

Reunión de Apertura						Ejecución de la Auditoría			
Día	5	**Mes**	11	**Año**	2020	**Desde**	05 / 11 / 2020	**Hasta**	4 / 12/ 2020

La fecha de ejecución de la auditoria anteriormente descrita, hace referencia a las actividades realizadas en el sitio de auditoria, que para el caso que nos ocupa, se realizó de manera remota a la Oficina de Tecnologías de la Información del Nivel Central.

DESARROLLO DE LA AUDITORÍA

Fue revisado dentro del Macroproceso Tecnologías de la Información, y para lo relacionado con el Decreto 491 de 2020, el cumplimiento de la normativa conforme a lo establecido en el Art.3 - que señala lo relacionado con la "*Prestación de los servicios a cargo de las autoridades. Para evitar el contacto entre las personas, propiciar el distanciamiento social y hasta tanto permanezca vigente la Emergencia Sanitaria declarada por el Ministerio de Salud y Protección Social, las autoridades a que se refiere el artículo 1 del presente Decreto velarán por prestar los servicios a su cargo mediante la modalidad de trabajo en casa, utilizando las tecnologías de la información y las comunicaciones*" en lo referente al rol prioritario de esta Oficina de Tecnologías, para apoyar en sus funciones a la entidad.

Así mismo, se realizó la verificación a la Implementación de la Directiva Presidencial No.02 de 2020, relacionada con las medidas para atender la contingencia generada por el covid-19, a partir del uso de las tecnologías de la información y las telecomunicaciones (TIC).

Lo anterior, en atención al Decreto 2723 de 2014, "*Por el cual se modifica la estructura de la Superintendencia de Notariado y Registro",* en el Articulo 17, le asigna a la Oficina de Tecnologías de la Información, funciones relacionadas con los sistemas de información de la Entidad, específicamente lo relacionado con los numerales: 1; 2; 5; 8 y 9.

De acuerdo con lo anterior, en el marco de la auditoría, se realizó revisión documental donde se evidenciaron las siguientes actuaciones, que permitieron a la entidad dar continuidad al servicio prestado al ciudadano, de acuerdo con lo presentado por la Oficina de Tecnologías de la Información y de acuerdo con lo solicitado:

1. **TECNOLOGÍAS DE INFORMACIÓN QUE FAVORECIERON EL FORTALECIMIENTO DEL SERVICIO AL CIUDADANO DECRET0 491 DE 2020, Art 3 (Prestación de los servicios a cargo de las autoridades)**

Las siguientes tecnologías, lograron un fortalecimiento del servicio al ciudadano (para usuario externo e interno), en aras de propiciar el distanciamiento social, de acuerdo con la emergencia sanitaria declarada en Colombia, y como medidas implementadas por la SNR, a partir del uso de las tecnologías de la información, para atender la emergencia generada por el Covid:

1.1. Se realizó el diseño de los ajustes a realizar en el aplicativo misional folio, como un nuevo control permitiendo que las constancias de inscripción y notas devolutivas impresas, salieran con la firma del registrad. Con base en ese diseño, se desarrolló un módulo en el aplicativo de Radicación electrónica (REL), con el cual se avanzan los turnos de la fase de registro "*mesa de control*" y de la fase "*firma de registrador*" a la siguiente, permitiendo incorporar así la firma del registrador. Se anexó como evidencias en archivo: "*Anexo1-Finalización REL*" el cual contiene el manual de usuario de este desarrollo.

SNR SUPERINTENDENCIA DE NOTARIADO & REGISTRO La guarda de la fe pública

Pagina 2

FORMULARIO DE CALIFICACION
CONSTANCIA DE INSCRIPCION

Impreso el 27 de Octubre de 2020 a las 08:03:22 AM
No tiene validez sin la firma y sello del registrador en la ultima pagina

ANOTACION: Nro 12 Fecha: 11-08-2020 Radicacion: 2020-29153 Valor Acto:
Documento: ESCRITURA 756 DEL: 20-05-2020 NOTARIA TREINTA DE BOGOTA D. C.

ESPECIFICACION: 0369 DERECHO DE PREFERENCIA *ART.21 LEY 1537 DE 2012 QUE MODIFICO EL ART.8 DE LA LEY 3 DE 1991 (LIMITACION AL DOMINIO)

PERSONAS QUE INTERVIENEN EN EL ACTO (X-Titular de derecho real de dominio, I-Titular de dominio incompleto)

DE: FONDO NACIONAL DE VIVIENDA FONVIVIENDA	8,301,212,085	
DE: SECRETARIA DISTRITAL DEL HABITAT		
A: REYES LOZADA WILLIAM	79,638,894	X

FIN DE ESTE DOCUMENTO

El Interesado debe comunicar al registrador cualquier falla o error en el registro de los documentos
Documento Generado Electronicamente - Radicacion Electronica
Fecha 27 de Octubre de 2020 a las 08:03:22 AM
Funcionario Calificador ABOGA222
El Registrador - Firma

EDGAR JOSE NAMEN AYUB

1.2. Para las ORIP, que operan sin el aplicativo de IRIS Documental, se diseñó y desarrolló un Gestor Documental básico denominado "*GARC*", a fin de que en la ORIP digitalizaran los documentos radicados desde allí y cargarlos en el gestor documental. Esto con el fin de que la persona que trabaja desde casa, pueda ver dichos documentos. Se anexó como evidencias el archivo denominado "*anexo2 -Manual de Usuario - v1.0 gestor documental*" el cual contiene las correspondientes instrucciones para su uso.

1.3. Se realizó aprovisionamiento y configuración de servidores de infraestructura necesaria para realizar la conexión remota desde casa de los funcionarios, creando los procedimientos necesarios para realizar la configuración correspondiente (Grupo Infraestructura). Se presentaron evidencias desde la Oficina de Tecnologías de la información, sobre la implementación del RemoteApp en las Oficinas de Registro de Instrumentos Públicos, con un total de 53 servidores virtuales configurados para las ORIP y un servidor virtual que proporciona acceso a escritorio remoto a los registradores que en su momento requirieron de dicha configuración para proceder con las actividades correspondientes. También se manifestó que se implementaron dos servidores como puertas de enlace configurados en infraestructura ORACLE – OVM y en infraestructura de virtualización VMWARE.

1.4. Se creó el formato de creación de usuarios en los sistemas antes descritos (REL y GARC); se adjunta ejemplo en el archivo "*anexo3-plantilla para creación de usuarios trabajo remoto".* – Revisado este formato, no se encontró adoptado formalmente en el sistema de gestión institucional - SIG.

1.5. Se realizaron varios ajustes a la plataforma SISG, a través de módulos de gestión de trámites internos para la SNR, los cuales permitieron el control de diferentes aspectos como son:

- Se desarrollò un micrositio web que permite acceder a todos los Servicios de la SNR por parte de los ciudadanos externos a la entidad, al cual se accede a través del Link: https://servicios.supernotariado.gov.co/, logrando obtener acceso a los siguientes servicios electrónicos de la Superintendencia de Notariado y Registro:

Los módulos creados en el SISG por motivos de mejorar la eficiencia y permitir trabajo remoto a los funcionarios como cliente interno son:

1- Correspondencia en línea: En el nivel central de la SNR, se pueden gestionar todas las comunicaciones físicas que hacen parte del sistema de gestión documental de la entidad. Mediante esta herramienta se pueden consultar y gestionar informes, oficios, cuentas de cobro, derechos de petición, tutelas, etc.

https://sisg.supernotariado.gov.co/correspondencia.jsp-

2- Apoyo económico para Notarios: Módulo Control de requisitos para apoyar económicamente a Notarios por motivos de la pandemia, en cumplimiento a lo establecido en el Decreto 813 de 2020. Se accede a través del Link: https://sisg.supernotariado.gov.co/beneficio_notariado.jsp

3- Gestión de cuentas de cobro para contratistas: Gestión de cuentas de cobro para contratistas a nivel nacional gestionado por los grupos y procesos de la dirección administrativa y financiera. https://sisg.supernotariado.gov.co/cuentas_cobro.jsp

4-Gestión de facturas: Control de facturas de la dirección administrativa y financiera: https://sisg.supernotariado.gov.co/cuenta_factura.jspxx

5. Chat: Mediante esta herramienta se establece una comunicación directa con los ciudadanos.
https://sisg.supernotariado.gov.co/chat.jsp y https://servicios.supernotariado.gov.co/Chat/index.php/chat

6. Reactivación de Orip para trabajar: Control de requisitos para que la Orip vuelva a trabajar.
https://sisg.supernotariado.gov.co/reactivacion_orip.jsp: este módulo se encontró en desarrollo, no ha salido a producción.

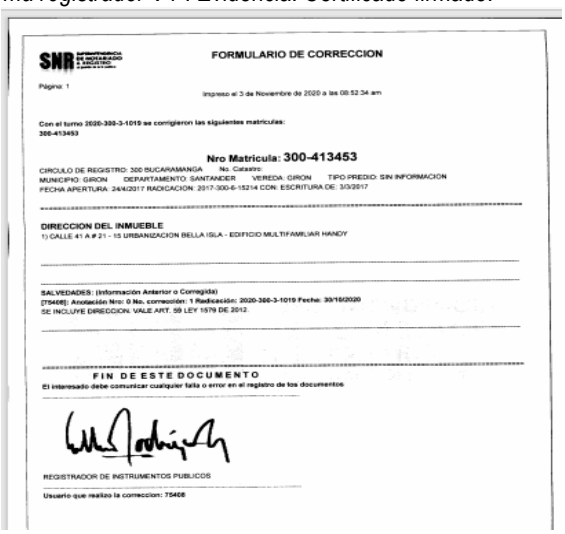
7. Control de suministros de pandemia para cada Orip: Gestión y control de suministros.
https://sisg.supernotariado.gov.co/analisis_orip_suministro.jsp: este módulo se encontró en desarrollo, no ha salido a producción.

8. Control de personal en cada Orip para atender la Pandemia. https://sisg.supernotariado.gov.co/orip&30.jsp: este módulo se encontró en desarrollo, no ha salido a producción.

9. Control de temperatura para funcionarios y ciudadanos: La dirección de talento humano solicito creación de modulo para monitorear control de temperatura a funcionarios de las Orips y ciudadanos. https://sisg.supernotariado.gov.co/control_temperatura.jsp : este módulo se encontró en desarrollo, no ha salido a producción.

Se presentaron evidencias a través del archivo denominado: "*anexo4-Modulos SISG - Vicky".*

1.6. Se realizaron ajustes al aplicativo SIR, para permitir la firma de los formularios expedidos por la ORIP (formulario de calificación, formulario de correcciones, notas devolutivas, reproducciones de sellos), visualizar los formularios por parte de los calificadores y ejecutores de corrección, impresión y reimpresión de formularios. Se adjuntó archivo denominado: "*Anexo 5 Manual Impresión Formularios firma registrador V4*". Evidencia: Certificado firmado:



SNR SUPERINTENDENCIA DE NOTARIADO & REGISTRO

FORMULARIO DE CORRECCION

Página: 1

Impreso el 3 de Noviembre de 2020 a las 08:52:34 am

Con el turno 2020-300-3-1019 se corrigieron las siguientes matrículas:
300-413453

Nro Matricula: 300-413453

CIRCULO DE REGISTRO: 300 BUCARAMANGA No. Catastro:
MUNICIPIO: GIRON DEPARTAMENTO: SANTANDER VEREDA: GIRON TIPO PREDIO: SIN INFORMACION
FECHA APERTURA: 24/4/2017 RADICACION: 2017-300-6-15214 CON: ESCRITURA DE: 3/3/2017

DIRECCION DEL INMUEBLE
1) CALLE 41 A # 21 - 15 URBANIZACION BELLA ISLA - EDIFICIO MULTIFAMILIAR HANDY

SALVEDADES: (Información Anterior o Corregida)
[75408]: Anotación Nro: 0 No. corrección: 1 Radicación: 2020-300-3-1019 Fecha: 30/10/2020
SE INCLUYE DIRECCION. VALE ART. 59 LEY 1579 DE 2012.

FIN DE ESTE DOCUMENTO
El interesado debe comunicar cualquier falla o error en el registro de los documentos

REGISTRADOR DE INSTRUMENTOS PUBLICOS

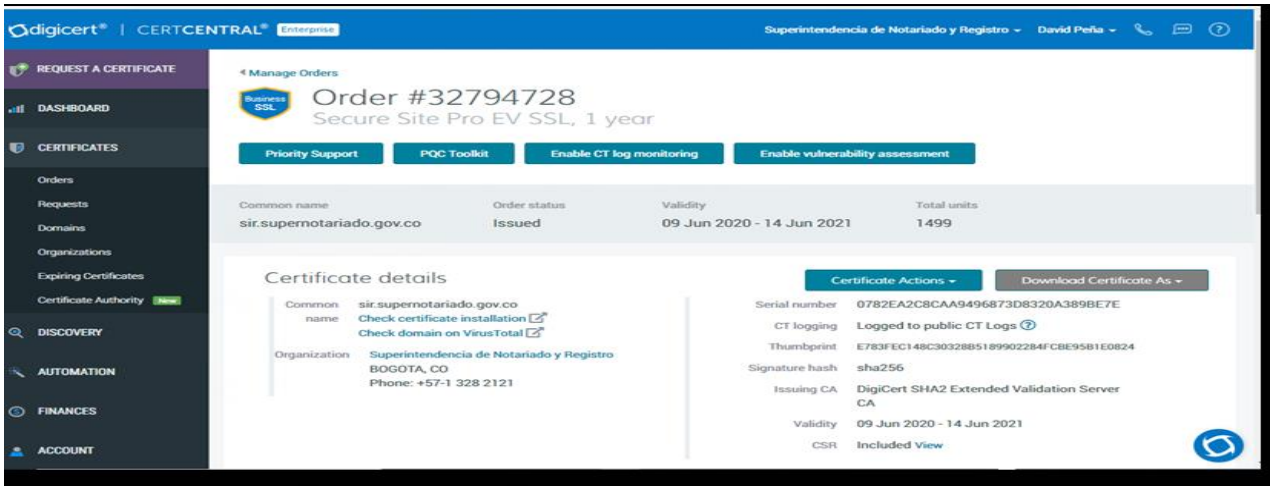
Usuario que realizo la correccion: 75408

Certificado de corrección y constancia de calificación con las respectivas firmas del aplicativo SIR -Sistema de Información de Registro, que ha sido creado para la Superintendencia de Notariado y Registro, con el fin de integrar la información registral de todos los predios a nivel Nacional. Con la unificación de esta información, se puede atender cualquier solicitud que necesiten los ciudadanos de manera eficiente y confiable, sin importar el origen de su radicación. Se desarrollaron nuevas funcionalidades para el proceso de impresión y firma de los formularios por parte del registrador, en los siguientes documentos:

- Formulario de calificación.
- Formulario de corrección.
- Nota devolutiva.
- Constancia de inscripción de testamento.
- Reproducción de sellos.
- Oficio de pertenencia.

Así mismo, se permitió la visualización de los formularios antes de realizar la impresión y también se aplicará para el proceso de reimpresión de estos mismos formatos.

1.7. Se realizó la adquisición de un certificado de sitio seguro (SSL), para permitir exponer la aplicación SIR y el ingreso a los servidores que permiten la comunicación remota, es así como para el ingreso a SIR, se digita https://sir.supernotariado.gov.co:7778/SNR/ y no con http://sir.supernotariado.gov.co:7778/SNR/, se adjunta pantallazo de la plataforma donde se administra:



1.8. Se adjuntan presentaciones en la cual se observa el contenido de las charlas dadas para la salida a producción en las ORIP ya realizados los correspondientes ajustes en los aplicativos misionales así: anexo 6 – TRABAJO REMOTO FOLIO IRIS, anexo 7 TRABAJO REMOTO FOLIO SIN IRIS, anexo 8 TRABAJO REMOTO SIR SIN IRIS, anexo 9 TRABAJO REMOTO SIR IRIS, dependiendo del tipo de implementación de esos aplicativos en la ORIP. Es de resaltar, que en las mismas participaba la Dirección Técnica de Registro, dependencia con la que se trabajó mancomunadamente en este proceso.

1.9. Se adjunta archivo "anexo 10 CONSOLIDADO REMOTO", en el cual se entrega información consolidada de los accesos remotos creados. El programa Remote APP permite obtener acceso mediante Servicios de Escritorio Remoto, desplegándose de tal manera, como si éstos se ejecutaran en el equipo local del usuario final. La Oficina de Tecnologías de la Información – OTI, mediante este tipo de herramientas, ofrece la posibilidad de conexión de manera externa a las aplicaciones que trabajan de manera local en cada una de las sedes, con el fin de proporcionar continuidad a los procesos de calificación y acceso remotos en aproximadamente 53 Oficinas de Registro.

Recomendación General OCI, numeral 1.:

Teniendo en cuenta la creación de nuevos aplicativos o desarrollos en aras de dar continuidad a las diferentes actividades que se desarrollan en la entidad y en atención a la emergencia sanitaria declarada por el Gobierno Nacional, se considera la

necesidad de documentar los manuales de usuario para los roles existentes, así como los formatos diseñados, en atención a las prácticas emprendidas para la atención del trabajo en casa, por lo que se hace oportuno incluir los formatos y demás manuales creados, al Sistema de Gestión Institucional – SIGI de la entidad, y para el caso de los nuevos accesos autorizados para el ingreso a los diferentes aplicativos creados – *"plantilla para creación de usuarios trabajo remoto"*, se sugiere acudir a las buenas prácticas, dejando un espacio en el formato para la autorización del Registrador y/o superior inmediato, de tal forma que se conozca quien se encuentra asignando el permiso. Así mismo, con el fin de dar a conocer al funcionario autorizado, la importancia en la adopción de medidas de seguridad, conservando las buenas prácticas en la autenticación, evitando el riesgo de accesos no autorizados desde una red externa.

Igualmente, se recomienda verificar la suficiencia de los controles que se aplican en la SNR para la administración de las contraseñas, de tal forma que se garantice por parte de los usuarios la confidencialidad de èstas, al momento de ausentarse de sus lugares de trabajo (motivos de reuniones, citas médicas, etc) y teniendo en cuenta el trabajo desde casa. Realizar validaciones periódicas, que garanticen la caducidad de las contraseñas como medidas de seguridad, entre otros.

Con respecto a los servicios de acceso a la conexión remota desde la casa de los funcionarios, se recomienda revisar la política de seguridad en el tema relacionado con el uso de las redes y los servicios de red, de tal forma que se incluya la verificación de los funcionarios a quienes se les ha autorizado la conectividad; los procedimientos de autorización para determinar a quién se permite el acceso y a qué servicios; los controles y procedimientos de gestión para proteger el ingreso a las conexiones; los medios usados; los requisitos de autenticación de usuarios y el seguimiento del uso de estos servicios; entre otros, con el fin de garantizar la seguridad de las cuatro áreas de riesgo principales: arquitectura de red general, control de acceso, denegación de servicio y endpoints.

Lo anterior, para reducir los diversos riesgos asociados al uso de estos equipos, como la filtración de información personal o el uso no autorizado por parte de terceros, por lo cual se requieren medidas de seguridad constantes y eficaces, de tal forma que se logre garantizar que el equipo al cual se le autorizó el acceso, se utilice de forma segura; y en cumplimiento a lo dispuesto en el Decreto 1008 de 2018 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital" 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*". 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*.", situación que podría afectar el registro adecuado de la información de la Entidad.

2. ASPECTOS PRESENTES PARA EL CONTROL Y CORRECTO USO DE LAS TECNOLOGÌAS

De las evidencias aportadas, se concluye que debido al incremento de personas y trabajadores, en contacto con las tecnologías de información y familiarización con las mismas, existen algunos aspectos que fueron considerados para su correcto uso; entre ellos, se solicitaron evidencias respecto a los siguientes temas, encontrando lo siguiente:

- **Capacitaciones realizadas**, Se observó que se han organizado talleres en conjunto con personal de Microsoft de la herramienta colaborativa para los funcionarios de la Entidad; se elaboraron manuales y se procedió a su divulgación a través de correos electrónicos, así como la socialización sobre la forma de acceder al Centro de Aprendizaje de Microsoft sobre las herramientas colaborativas de Office 365 – Forms; Teams y la One Drive, entre otros. Igualmente, se realizó el Taller de Productividad – Office 365: "Trabajemos desde Casa" dirigidos a los Directivos y demás funcionarios de la Superintendencia de Notariado y Registro, efectuada el 02 de abril de 2020. Esto, con el fin de brindar educación a los trabajadores buscando disminuir brechas de conocimiento y culturales que impidan el uso de las tecnologías en su máximo potencial. Para ello se aportaron las siguientes evidencias:

-Entrenamiento y certificación interno del equipo de trabajo en el mes 15 abril y hasta el 15 de mayo, hasta el 15 de mayo: https://www.oracle.com/education/
-Curso virtual para funcionarios sobre integridad, transparencia y lucha contra la corrupción.

-Curso contratación estatal, en la escuela de administración pública, en mayo.
-Curso MIPG en la función pública, en el mes de mayo.
-Capacitación uso ONE-DRIVE:
- Cap 1-1 Qué es OneDrive y uso desde aplicación web.pdf
- Cap 1-2 Uso OneDrive desde Aplicación Escritorio.pdf

-Capacitación MICROSOFT TEAMS:
- Cap 2-1 Guía rápida Microsoft Teams.pdf
- Cap 2-2 Uso de Microsoft Teams.pdf

-Capacitación en LIFESIZE:
- Cap 3-1 Uso de la aplicación de Lifesize.pdf

➢ **Evidencias de los instructivos para facilitar una rápida apropiación de las diferentes herramientas y esquemas de trabajo enfocados en el uso intensivo de tecnologías**; para verificar este ítem, se observó que la Oficina de Tecnologías en acompañamiento con el personal asignado de la Dirección Técnica de Registro y la Mesa de Ayuda Ofimática, desarrolló el protocolo para la configuración de equipos (Ver anexo Protocolo de configuración envío e instalación de equipos.pdf), en el cual se describen las actividades que se deben desarrollar para la correcta configuración de los equipos, que son retirados de la entidad SNR u Oficinas de Registro de Instrumentos Públicos y que estarán a disposición de los funcionarios para el desarrollo de sus actividades según requerimiento y previa autorización del coordinador, jefe o registrador.

Mediante correo de fecha 17 nov/20, enviado a la OTI, se solicitó el envío de información relacionado con *la cantidad de* equipos de propiedad de la Entidad (portátiles y de mesa) que han sido autorizados para que los funcionarios puedan trasladarlos a su residencia y poder atender a través de trabajo en casa, sus responsabilidades laborales, los controles de seguimiento existentes sobre los mismos y responsables, así como las gestiones se han realizado con las aseguradoras de estos equipos, *para cubrir los riesgos que puedan ser objeto fuera de las instalaciones oficiales, como daño, hurto, extravío, etc."*

Una vez que el Equipo Auditor, recibió información de la responsabilidad sobre el Grupo de Servicios Administrativos, a través de correo electrónico, el día 18/nov/2020, se solicitaron las evidencias correspondientes a esta área, obteniendo la relación de los equipos de cómputo, donde se registran los datos de los elementos que a nivel nacional se han autorizado para ser retirados de las instalaciones de las diferentes sedes de la SNR, donde a la fecha de envío del archivo Excel, se han autorizado un total de 174 equipos para ser traslados.

Informan que los requerimientos obedecen a solicitudes enviadas por correo electrónico, a interés de jefes y funcionarios, partiendo de la buena fe de su uso para trabajo en casa; posteriormente, se procede en sinergia con la mesa de ayuda para la configuración del equipo correspondiente; con la Empresa de Vigilancia se coordina la salida, y el funcionario que hizo la solicitud, se encarga de retirar el equipo y transportarlo, mediante firma del Acta de Entrega equipo computador – trabajos transitorios en casa.

Es de mencionar que estos equipos están amparados con la póliza aseguradora vigente, y enviaron como evidencias la copia de la Póliza de Seguros *AXA COLPATRIA SEGUROS S.A*., número: 11638, suscrita por el ordenador del gasto y la aseguradora, llevándose el control en la Oficina de Servicios Administrativos de la Entidad. En la póliza, se puede observar la siguiente anotación expedida por dicha Aseguradora, así:

Tipo de Póliza: Todo Riesgo Daño Material con cobertura a equipos utilizados en casa por parte de los funcionarios de la entidad.
Vigencia: desde: 01-06- 2020 hasta: 04-03-2021
"*AXA COLPATRIA SEGUROS S.A., mediante el presente anexo otorga extensión de cobertura de acuerdo con las condiciones pactadas en la presente póliza. Se extiende cobertura a los equipos usados por los funcionarios del tomador asegurado bajo la modalidad de Teletrabajo*".

Con lo anterior, se evidencia que la Superintendencia de Notariado y Registro, una vez presentada la pandemia del COVID-19, se procedió a cobijar y proteger sus equipos (Computadores de Mesa y Portátiles) destinados a labores de trabajo en

casa, en manos de funcionarios que adelantan actividades desde sus hogares, para cubrir los riesgos que puedan ser objeto de sucederse por fuera de las instalaciones oficiales, tales como daño, hurto, extravío, etc.

Recomendación OCI:
Al respecto, se observó que en el diligenciamiento del formato de control de equipos retirados, no fueron diligenciadas la totalidad de las casillas en relación con los equipos de cómputo prestados como son: "*Dirección de vivienda – documento de identidad – fecha de autorización de la salida - Cargo*". Así mismo, la Oficina de Control Interno, considera necesario advertir sobre el riesgo que conlleva el hecho de tener prestados los equipos de cómputo a los contratistas y recomienda realizar seguimiento a la devolución de dichos equipos, antes del ultimo pago del contrato. Con respecto a los equipos cubiertos por la póliza de todo riesgo, se recomienda revisar los conceptos de teletrabajo y trabajo en casa, causas y efectos jurídicos para fortalecer los controles sobre los riesgos que puedan presentarse con ocasión a los mismos; teniendo en cuenta que en la póliza se establecen los equipos asegurados en la modalidad de Teletrabajo, a fin de argumentarlo en la misma póliza.

- **Conectividad e infraestructura tecnológica adecuadas**, Se observó que para que se permita la transferencia de imágenes de alta resolución y el uso de plataformas de comunicación en tiempo real, se han establecido controles a través de los aplicativos para los accesos remotos; también se adquirió el certificado de sitio seguro (SSL), para permitir exponer la aplicación SIR y permitir el ingreso seguro a internet de los servidores de la entidad, de tal forma que contaran con la comunicación remota; también se realizó la actualización de la política de backup de la máquina virtual; en acompañamiento de la Mesa de Ayuda – Ofimática, actualmente la Oficina de Tecnologías presta soporte técnico, instalación, configuración, asistencia telefónica y remota a los usuarios que generan las respectivas solicitudes a los correos electrónicos.

El hecho de contar con un Certificado SSL, garantiza a los clientes y visitantes de nuestro site la seguridad, tranquilidad y confianza necesaria para las diferentes consultas y/o pagos que realizan los usuarios.

- **Diseño de aplicaciones**, Los desarrollos anteriormente descritos, tienen el propósito de garantizar el respaldo de la tecnología a las necesidades de los usuarios; incluso, aspectos de atención a los ciudadanos, y en algunos casos, de tipo administrativo para atender las diferentes actividades que realiza la entidad, a través del aplicativo SISG.

- **Revisión de procesos antes de automatizarlos,** se observó que algunas actividades de los diferentes procesos referidos anteriormente, fueron reemplazados por módulos tecnológicos, realizando los cambios necesarios a la plataforma tecnológica para su correcto funcionamiento. Este proceso se realizó de manera coordinada con los diferentes actores de los procesos como son la Dirección Técnica de Registro; encargada de proponer e implementar estrategias relacionadas con la prestación del servicio a cargo de las Oficinas de Registro de Instrumentos Públicos en el País; el área administrativa y financiera; entre otros.

3. USO DE HERRAMIENTAS COLABORATIVAS – DIRECTIVA PRESIDENCIAL 02-2020:
(Numerales revisados: 2.1 – 2.2. – 2.3 – 2.4 y 2.5)

2.1. Minimizar las reuniones presenciales de grupo, y cuando sea necesario realizarlas, propender por reuniones virtuales mediante el uso de las tecnologías de la información y las comunicaciones. Se determina que se ha dado cumplimiento, utilizando las herramientas colaborativas integradas en la plataforma Office 365- Teams y el sistema de videoconferencia Life Size, con el fin de efectuar labores con la modalidad de trabajo en casa.

2.2. Acudir a canales virtuales institucionales, transmisiones en vivo y redes sociales, para realizar conversatorios, foros, congresos o cualquier tipo de evento masivo. Se observa el cumplimiento dado que se ha apoyado técnica y operativamente en diversos eventos en vivo a través de la herramienta Teams de la SNR con entes del gobierno, como es reunión del 1 de octubre a las 8 a.m., donde se llevó a cabo el evento de Digitalización Notarial presentado por Presidencia, Ministerio de Justicia, Dian y Superintendencia de Notariado y Registro a las Notarías a nivel nacional. Este evento se llevó a cabo en el Centro de Innovación y Diseño Empresarial de la Cámara de Comercio de Bogotá. Para dicho acontecimiento, la Superintendencia de Notariado y registro contó con el apoyo de la Oficina de Tecnologías de la Información.

Así mismo, la entidad realizó la Rendición de Cuentas 2019-2020 como espacio de interlocución entre los servidores públicos y la ciudadanía; evento realizado por la SNR, publicado a través de las redes sociales, en Twitter: @Supernotariado y en Instagram: Supernotariado. La transmisión fue en directo por Facebook en el enlace: @Superintendencia de Notariado y Registro de Colombia. Durante los días: 19, 20, 21 y 23 de Octubre de 2020.

2.3. Usar las herramientas tecnológicas para comunicarse, el acuerdo marco de precios de nube pública vigente, trabajo colaborativo y telepresencial -videoconferencia-, para evitar el uso, impresión y manipulación de papel. De acuerdo con las evidencias presentadas hay observancia a este numeral para la vigencia 2020, toda vez que la entidad viene consultando a través de Colombia Compra Eficiente, los productos del acuerdo marco para realizar la contratación de la plataforma de nube pública; así mismo, han permitido la comunicación entre los diferentes funcionarios de la entidad, a través de las videoconferencias, los correos electrónicos y demás herramientas colaborativas; evitando así el uso, la impresión y manipulación de papel. Igualmente, se encontró que la entidad ha implementado desarrollos que permiten el trabajo en casa, accediendo a realizar verificaciones y firmas digitales sin necesidad de realizar la impresión de estos, como es el caso del aplicativo REL.
Evidencias aportadas para dar cumplimiento a este ítem, anexaron la orden de compra No.54548, del 2/09/2020, relacionada con "*Contratar Plataforma de nube pública por demanda (PaaS), con capacidad de almacenamiento y procesamiento, permitiendo el diseño, implementación, soporte, administración y apoyo de la digitalización de la actividad Notarial y consular en Colombia, facilitando las actividades de la OIVC Notarial, mitigando el impacto y riesgo de pérdida de protocolos y actos notariales en un marco de interoperabilidad continuo.*"

2.4. Adoptar las acciones que sean necesarias para que los trámites que realicen los ciudadanos se adelanten dándole prioridad a los medios digitales. Se observó que a través del micrositio web https://servicios.supernotariado.gov.co/, se permite acceder a 14 Servicios de la SNR, por parte de los ciudadanos externos a la entidad, logrando obtener acceso a servicios electrónicos de la Superintendencia de Notariado y Registro. Así mismo, se observó que a través de la página Web de GOV.CO; se cuenta con la publicación de 4 trámites y servicios a los que se puede acceder, como son:
-Consultas en la Ventanilla Única de Registro -VUR: A través de la VUR; las Notarías acceden a las bases de datos de las Oficinas de Registro y de administraciones territoriales con el fin de establecer los estados jurídicos y tributarios de los inmuebles; de esta manera el interesado se ahorra los desplazamientos, pagos y tiempo que le tomaría solicitar la documentación en cada de estas entidades;
-Registro de instrumentos públicos: Registrar en el folio de matrícula inmobiliaria, los actos o contratos que se realizan sobre los bienes inmuebles;
-Consulta Índice Propietarios: Entregar la información del número de matrícula inmobiliaria;
-Certificado de tradición y libertad de inmuebles: para conocer la situación jurídica de los bienes inmuebles sometidos a registro y su tradición.

2.5. Hacer uso de herramientas como e-learning, portales de conocimiento, redes sociales y plataformas colaborativas, para adelantar los procesos de capacitación y formación que sean inaplazables. Como evidencias del cumplimiento a este numeral, se presentaron registros de las capacitaciones que se han adelantado en diferentes temas, requeridos para el aprendizaje en el uso de las tecnologías.

- **Forma de garantizar el cumplimiento de los lineamientos establecidos en materia de ciberseguridad por la entidad y con sujeción a la legislación vigente en materia de habeas data – de acuerdo con el uso de las tecnologías de la información y telecomunicaciones en la SNR** Teniendo en cuenta que la ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos, a través de diferentes mecanismos adoptados por las entidades públicas, se observó que actualmente en la SNR se manejan dos esquemas de seguridad, uno externo y otro interno. En el externo, existe un esquema de cara al usuario, donde se involucra a los administradores de las aplicaciones para cada uno de los servicios que se prestan por parte de la entidad y en lo relacionado con la información registral, en donde la seguridad se maneja a través de los certificados de sitio seguro (SSL), para garantizar la confidencialidad de la información y de las conexiones VPN que los funcionarios tienen con la entidad, esto a nivel de conectividad.

Para lo relacionado con la información que se almacena tanto de las PQRS, al registrarse el usuario con sus datos personales, lo mismo con los datos de los ciudadanos que aparecen en las bases de datos de registro, se encuentra que esa seguridad de la información es de competencia de los ingenieros que administran cada aplicación, donde se deben tomar un conjunto de medidas preventivas y reactivas en los sistemas tecnológicos, que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de los datos.

Igualmente, se viene realizando la actualización de la Política General y políticas específicas del Sistema de Seguridad de la Información, a través de la cual se tiene en cuenta lo establecido en la legislación vigente en materia de habeas data, para el uso de la información entregada por los ciudadanos, se busca que cada uno de los controles sean ajustados por la Oficina de Tecnologías en cada uno de los aplicativos. Igualmente, a través de la topología de red existente, se observa que existen firewall, o dispositivo de seguridad de la red, que monitorea el tráfico de red —entrante y saliente— y decide si permite o bloquea el tráfico específico en función de un conjunto de reglas de seguridad que los administradores han definido previamente, en cuanto a inspección activa con prevención de intrusiones y antivirus; documentado a través de la topología de red, LAN y WAN. Se presentó como evidencias el borrador de la Política General y políticas específicas del Sistema de Seguridad de la Información y de la topología de red.

OBSERVACION OCI:

En atención a las diferentes actividades que la Oficina de Tecnologías viene desarrollando para dar cumplimiento a este lineamiento, y dado que actualmente no se cuenta con una Política del Sistema de Seguridad de la Información aprobada y que contenga las medidas para ser adoptadas en materia de ciberseguridad, con el fin de determinar los posibles incidentes cibernéticos graves o muy graves que puedan llegar a afectar la infraestructura de tecnologías de la información, teniendo en cuenta el nuevo entorno cambiante y digital, marcado por las ciberamenazas, se recomienda adoptar políticas para implementar un sistema de seguridad digital y de seguridad de la información, conforme con las buenas prácticas internacionales, como es la serie ISO 27000, o los recomendados por el Instituto Nacional de Tecnología y Estándares.

4. FUNCIONES OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN – DECRETO 2723 DE 2014, ART.17:
(Numerales verificados: 1 – 2 – 5 – 8- 9):

1. Asesorar al Despacho del Superintendente en la definición de las políticas, planes, programas y procedimientos relacionados con el uso y aplicación de las tecnologías de la información, que contribuyan a incrementar la eficiencia y eficacia en las diferentes dependencias de la Superintendencia, así como a garantizar la calidad en la prestación de los servicios: Se determina que se viene prestando la asesoría a través de las diferentes actividades desarrolladas por la Oficina de Tecnologías, como son los diferentes proyectos tecnológicos implementados al interior de la entidad, en atención a la emergencia sanitaria declarada por el Gobierno Nacional.

2. Realizar el análisis, diseño, programación, documentación, implantación y mantenimiento de los sistemas de información requeridos por la Entidad: Se observa el cumplimiento a través de los diferentes desarrollos con que la entidad cuenta actualmente (ver numerales 1.1; 1.2 y 1.3 del presente informe), así como los soportes de manuales para su funcionamiento; las actas de capacitación realizadas, alistamientos y aprovisionamiento de infraestructura tecnológica, entre otros.

5. Definir los protocolos tecnológicos, apoyar la capacitación y fomentar la cultura organizacional orientada a la utilización y adaptación de tecnologías de punta: Se observa que se está trabajando con el apoyo de Mintic en el Plan de Transformación Digital, orientado a fomentar la cultura organizacional frente a la utilización de las tecnologías, donde se están identificando cuales sistemas de información de los que se utilizan en la entidad, serian de gran impacto para los usuarios, y se está realizando el diagnóstico para el Plan de Transformación Digital; sin embargo, en época de la calamidad sanitaria, se observa el uso de las diferentes tecnologías como herramientas para el trabajo en casa (señaladas en el numeral 1.1 del presente informe).

En cuanto a los protocolos tecnológicos, que hacen parte de TIC para la sociedad de la Política de Gobierno Digital, informó la Oficina de Tecnologías que se ha trabajado en el tema de interoperabilidad, donde la SNR está adelantando actividades de

desarrollo en web service, con la Agencia Nacional Digital (*Entidad encargada de articular los Servicios Ciudadanos Digitales del Decreto 1413 de 2017 y desarrollar actividades de ciencia, tecnología e innovación asociadas a la creación de un ecosistema de información pública. Implementar soluciones de software y analítica de datos en las diferentes problemáticas que presenten las entidades del Estado*) para la consulta de nomenclatura de segregados y consulta de propietarios, para la interoperabilidad con el IGAC, presentando como evidencias el *Protocolo técnico de intercambio de información Superintendencia de Notariado y Registro (SNR) – Instituto Geográfico Agustín Codazzi (IGAC).*

8. Diseñar los mecanismos para aplicar, utilizar, adaptar, aprovechar y darle un buen uso a las tecnologías de la información: Se desarrolla a través de los ítems verificados anteriormente (numerales 1.1 al 1.4 del presente informe); así mismo, a través de las diferentes actividades que se han venido desarrollando desde la Oficina de Tecnologías de la Información, para la implementación de las Políticas de Gobierno Digital y Seguridad Digital; donde se observan los avances presentados en este informe a partir del numeral 1.5, y de acuerdo con lo reportado por la Oficina de Tecnologías.

9. Evaluar la seguridad, calidad y flujo de la información de la Superintendencia a fin de permitir su acceso entre las diferentes Superintendencias Delegadas para el cumplimiento de los objetivos individuales e institucionales en materia de inspección, vigilancia y control: Respecto al flujo de la información de la Superintendencia a fin de permitir su acceso entre las diferentes Superintendencias Delegadas para el cumplimiento de los objetivos individuales e institucionales en materia de inspección, vigilancia y control, se observó que se viene registrando y gestionando el flujo de la información, a través del aplicativo Iris Documental y del aplicativo de PQRSD, donde cada responsable de área, gestiona lo relacionado con su área, a fin de permitir el acceso para dar respuesta a los diferentes requerimientos de información efectuados, tanto por ciudadanos como por las demás superintendencias delegadas.

5- REVISIÓN EFECTUADA A LA IMPLEMENTACIÓN DE LOS SIGUIENTES MANUALES DE LOS DECRETOS:
Decreto 1008 de 2018: "*Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y…, en su Artículo 2.2.9.1.2.2. que establece el Manual de Gobierno Digital, para la implementación de dicha política";* así mismo, se realizó la verificación a lo normado a través del Decreto 1499 de 2017 – *"Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública",* en lo relacionado con el *Sistema de Gestión*, y lo establecido en el artículo 133 de la Ley 1753 de 2015, en lo relacionado con el Manual Operativo del Modelo Integrado de Planeación y Gestión - MIPG.

Considerando el tiempo de la auditoría, el talento humano disponible y los recursos técnicos y tecnológicos para la ejecución de la auditoría, se decide auditar una muestra de diez (10) elementos del universo que se encuentran definidos a través de los dos componentes, como son: TIC para el Estado y TIC para la Sociedad, y que son habilitados a su vez por tres elementos transversales como son: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, verificando el cumplimiento a los requerimientos mínimos que todos los sujetos obligados deben cumplir para alcanzar los logros en la implementación de la política.

Componentes y Habilitadores Transversales:[1]

[1] MANUAL DE GOBIERNO DIGITAL, Implementación de la Política de Gobierno Digital - Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2)

COMPONENTES:

TIC para el Estado: Tiene como objetivo mejorar el funcionamiento de las entidades públicas y su relación con otras entidades públicas, a través del uso de las Tecnologías de la Información y las Comunicaciones. Con este componente, se busca que las entidades fortalezcan sus competencias y las de sus servidores públicos, relacionadas con tecnologías de la información -T.I., a nivel de su arquitectura institucional, como elementos generadores de valor en la gestión pública.

TIC para la Sociedad: Tiene como objetivo fortalecer la sociedad y su relación con el Estado en un entorno confiable, que permita la apertura y el aprovechamiento de los datos públicos, la colaboración en el desarrollo de productos y servicios de valor público, el diseño conjunto de servicios, la participación ciudadana en el diseño de políticas y normas, y la identificación de soluciones a problemáticas de interés común. A través de este componente se busca mejorar el conocimiento, uso y aprovechamiento de las TIC, por parte de los usuarios, ciudadanos y grupos de interés que interactúan con las entidades públicas, para acceder a información pública, a trámites y servicios, participar en la gestión pública y en la satisfacción de necesidades.

HABILITADORES TRANSVERSALES:

Arquitectura: Busca que las entidades apliquen en su gestión un enfoque de Arquitectura Empresarial para el fortalecimiento de sus capacidades institucionales y de gestión de TI. El habilitador de Arquitectura soporta su uso e implementación en el Marco de Referencia de Arquitectura Empresarial del Estado, que es el instrumento que establece la estructura conceptual, define lineamientos, incorpora mejores prácticas y traza la ruta de implementación que una entidad pública debe realizar.

Seguridad de la información: Busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad y disponibilidad y privacidad de los datos. Este habilitador se soporta en el Modelo de Seguridad y Privacidad de la Información -MSPI, que contempla 6 niveles de madurez.

Servicios Ciudadanos Digitales: Busca que todas las entidades públicas implementen lo dispuesto en el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, que establece los lineamientos para la prestación de los servicios ciudadanos digitales, y para permitir el acceso a la administración pública a través de medios electrónicos. Conforme a dicha normativa, los servicios digitales se clasifican en servicios básicos: autenticación biométrica, autenticación con cédula digital, autenticación electrónica, carpeta ciudadana e interoperabilidad, los cuales son de obligatorio uso y adopción; y servicios especiales, que son adicionales a los servicios básicos, como el desarrollo de aplicaciones o soluciones informáticas para la prestación de los servicios ciudadanos digitales básicos.

Teniendo en cuenta la situación de emergencia generada por el COVID-19, las medidas de aislamiento obligatorio definidas en el Decreto 1076 de 2020 "*Por el cual se imparten instrucciones en virtud de la emergencia sanitaria generada por la pandemia del Coronavirus COVID-19, y el mantenimiento del orden público*", el Decreto 491 de 2020, *Por el cual se adoptan medidas de urgencia para garantizar la atención y la prestación de los servicios por parte de las autoridades públicas y los particulares que cumplan funciones públicas y se toman medidas para la protección laboral y de los contratistas de prestación de servicios de las entidades públicas, en el marco del Estado de Emergencia Económica, Social y Ecológica" y* para el ejercicio de obtener la muestra, se definieron los siguientes elementos para auditar, solicitando los soportes de la implementación y/o avance alcanzado, realizando la revisión documental de la información recopilada con base en los soportes aportados por los responsables en la Oficina de Tecnologías de la Información:

5.1. -Criterios de usabilidad web que cumple la entidad en todas las secciones de su portal Web oficial:

Para revisar este ítem, se verificaron algunos de los criterios usados para la creación de la página web de la entidad, donde se encontró que aunque el sitio web permite conocer la ruta recorrida por el usuario en la navegación del sitio (Ruta de migas), el sitio web no le indica al usuario cuando ya ha visitado contenidos de la página (Vínculos visitados). Con respecto al logo de la entidad ubicado en el encabezado, se determinó que éste no direcciona al inicio del sitio web (Vínculo a página de inicio). Así mismo, se observa que 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 a continuación:

34.Auditoria gestion orip popayan - cauca.pdf
35.wlswccportal01158395.pdf
36.wlswccportal01158389.pdf
38.wlswccportal01158297.pdf
39.wlswccportal01158151.pdf
40.Auditoria_gestion_orip_dorada_caldas.pdf
41.wlswccportal01157743.pdf
42.wlswccportal01157743.pdf
43.wlswccportal01158110.pdf
44.wlswccportal01157466.pdf
45.inforautoriamonteria.pdf

Por lo anterior, se recomienda realizar su revisión y actualización de los documentos soportes subidos en cada uno de los contenidos de la página web de la entidad. Con respecto al direccionamiento del logo, se observó que éste fue corregido en el transcurso de la auditoría y para la presentación del informe preliminar; fue subsanado.

5. 2- Verificación del Plan Estratégico de Tecnologías de la Información -PETI y del PESI para las vigencias 2019-2020: Se solicitaron los planes PETI y PESI aprobados en Comité, para lo cual, se entregó como evidencias copia de los documentos PETI y PESI, copia de las actas de comité, realizados en las vigencias 2019 y 2020 -Acta de Comité de Gestión Institucional, desarrollado el día 31 de enero de 2020; estrategias para la construcción del Plan Estratégico de Tecnologías de la Información -PETI. El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan de Seguridad de la Información -PESI; sin embargo, se encontró que estos planes no han sido aprobados, no se encontró publicado en la página web de la entidad y en su contenido no se tuvo en cuenta 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.

Esta situación, puede conllevar a generar inobservancia 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 podría 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*.".

También se genera el riesgo de no disponer de los recursos presupuestales de manera apropiada y coherente; conllevando entre otros, a no contar con la disponibilidad presupuestal para el logro de las metas y objetivos trazados por el área de tecnologías por efectos de una inadecuada planeación, y por ende, insuficiente control y seguimiento al mismo; con lo cual no se está dando cumplimiento a lo establecido en el Decreto 1499 de 2017 - manual operativo de MIPG y Decreto 1008 de 2018 "*Por el cual se establecen los lineamientos generales de la política de Gobierno Digital*" en su Artículo 2.2.9.1.2.2. Manual de Gobierno Digital. 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 la G.ES.06- MINTIC – Guía para la construcción del PETI el cual establece que: "*es el artefacto que se utiliza para expresar la Estrategia de TI. El PETI hace parte integral de la estrategia de la institución y es el resultado de un adecuado ejercicio de Planeación Estratégica de TI".*

Al respecto, la Oficina de Tecnologías presentó evidencias de la actualización que se viene realizando al PETI; sin embargo, en la misma se observó lo siguiente:
-No se han establecido las fechas puntuales de terminación de las actividades allí relacionadas, con el fin de determinar el cumplimiento de éstas, a un corte específico.
-No cumple con todos los requisitos exigidos del Modelo Operativo de la Guía 06; numeral 4.6ª – Capacidad 01: Gestionar el Direccionamiento Estratégico – Modelo Operativo, donde falta el año del formato de formulación del plan anual de gestión.
-Para el numeral 4.6b -Capacidad 02: Gestionar la capacidad estratégica, hacen falta en algunos apartes, el nombre del ID de Recursos.

-Para el numeral 4.6c – Capacidad 04: Gestionar la capacidad Técnica Registral, no se observa el diligenciamiento del nombre del recurso;
- Completar la información que se requiere, como Nombres tanto de los Procesos, de los Recursos y de Roles faltantes; los costos estimados o la proyección total del presupuesto; las hojas de ruta con las fechas.
-Tampoco se encontraron indicadores por cada uno de los dominios y para cada vigencia, que permita determinar el nivel de avance y cumplimiento de las metas definidas en el PETI; el entendimiento estratégico; el plan de comunicaciones del PETI; relación de todos los dominios del Marco de Referencia.

Lo anterior, no permitiría asegurar la alineación y coherencia de los planes, programas y proyectos implementados en TI con los incorporados en el PETI institucional. Por lo tanto, se recomienda realizar la revisión general al Modelo Operativo, con el fin de dar cumplimiento a cada uno de los ítems allí establecidos, teniendo presente la Guía expedida por MINTIC, y en caso de ser necesario, replantear los planes periódicamente, de acuerdo con la dinámica y las prioridades de la OTI, así como también de acuerdo con la evolución tecnológica.

5.3- Verificación de la gestión de tecnologías de la Información con que la entidad cuenta:
Se observó que para la gestión de tecnologías de la información (TI), la Entidad cuenta con un esquema de soporte con niveles de atención realizados a través de la mesa de ayuda tecnológica que gestiona los diferentes incidentes y requerimientos tanto a nivel Ofimático, como del servicio técnico registral a través de SIR; la cual contempla las líneas de operación básica de la entidad, como son:
-Dirección para la gestión del proyecto.
-Suministro e instalación, mantenimiento preventivo, correctivo de aires acondicionados a nivel nacional incluyendo las obras conexas a los mismos.
-Servicios soporte y mantenimiento plantas eléctricas y UPS
-Servicios de administración centro de cómputo
-Servicios mesa de ayuda tecnológica. pc, impresoras, scaners a nivel nacional.
-Servicios de soporte, administración y mantenimiento del sistema registral – SIR
-Servicios de voz ip y videoconferencia
-Bolsa de repuestos

Al respecto, se presentó como evidencias un procedimiento en construcción denominado: "*Atención a incidentes y solicitudes Mesa de Ayuda Tecnológica*" el cual tiene como objetivo -*Brindar solución al reporte de incidentes y solicitudes de los usuarios en cada una de las ORIP y nivel central de la SNR, de acuerdo a los acuerdos de nivel de servicio (ANS) establecido;* se observa que el documento se encuentra en borrador y que solo se está documentando la gestión atendida por el nivel 1, situación que genera el riesgo de desconocimiento de la gestión para la atención de incidentes de los demás niveles, de tal forma que se garantice la transferencia de conocimiento en caso de rotación del personal asignado.

Se recomienda documentar el proceso paso por paso, con roles y responsabilidades para todos los niveles de soporte, de acuerdo con los requerimientos para la prestación de los servicios que incluya un monitoreo de incidentes identificando casos recurrentes con el fin de buscar una solución definitiva a los incidentes que han sido repetitivos, ya que desde soporte se observa que se realizan correcciones; más no, acciones preventivas y/o acciones correctivas para dar solución a los errores presentados por los sistemas de información, lo cual genera reprocesos administrativos, pérdidas de tiempo, debilidades en los controles y reincidencia de las fallas.

- En este ítem, también se realizó la verificación al esquema de soporte y mantenimiento de los sistemas de información, donde se observó que existen Oficinas de registro y dependencias del nivel central que de acuerdo con las fechas establecidas en el cronograma de mantenimientos preventivos presentado, les fue aplazado el mantenimiento preventivo inicialmente programado debido a los diferentes obstáculos presentados en atención a la pandemia y para realizar los mantenimientos en las fechas previstas (como cierre de vías y cabeceras municipales, ausencia de medios de transporte, orden público y cierre de ORIP), por lo que se hace necesario advertir sobre el riesgo de no desarrollar la totalidad de actividades programadas de acuerdo con el contrato celebrado por la entidad para contratar los "*servicios de mesa tecnológica y mantenimiento de equipos ofimáticos, servicios de voz ip y videoconferencia; suministro de equipos y repuestos*

necesarios para la operación"; con el fin de dar cumplimiento a las cláusulas estipuladas en el mismo, teniendo en cuenta la importancia de los mantenimientos preventivos, esenciales para evitar arreglos mayores y costosos de los equipos tecnológicos, previniendo las posibles fallas.

Estas situaciones observadas pueden conllevar a generar inobservancia a lo establecido mediante Decreto 1008 de 2018 *"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital*" 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 - Servicios de mantenimiento de sistemas de información con terceras partes - Ámbito: Ciclo de Vida de los Sistemas de Información – Dominio: 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 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."*

5.4- Verificación aspectos del esquema de gobierno de tecnologías de la información (TI):

Verificada la información correspondiente al esquema de gobierno de tecnologías incorporado, se encontró que la Oficina de Tecnologías aunque cuenta con el mapa de procesos de la Oficina de Tecnologías de la Información, éste no estuvo disponible durante el desarrollo de la auditoría, por lo que no fue posible acceder a la documentación de los procesos, procedimientos, ni formatos, que estuviesen publicados en la página web de la entidad, situación que podría conllevar al riesgo de incumplir con lo establecido en la Política de Fortalecimiento organizacional y simplificación de procesos del MIPG, numeral 3.2.1.1.- "*la operación de la entidad se haga acorde con la manera en la que se han documentado y formalizado los procesos.",* al no contar con la documentación necesaria para la gestión de las actividades que se desarrollan en la Oficina de Tecnologías.

Así mismo, se encontró que esta situación generó la materialización del riesgo: "*Daño de activos de tecnología que afecten la disponibilidad de la información de los aplicativos misionales u otra información"*, que como causa generadora, se presentó el inconveniente técnico ocurrido a la infraestructura donde se encuentra alojado el portal web de la entidad, lo que limitó la posibilidad de visualizar y acceder al Mapa de procesos, y al botón de transparencia y acceso a la información pública.

- En este mismo ítem, fueron revisados los indicadores definidos para medir el desempeño de la gestión de Tecnologías de la Información, verificando su medición y seguimiento. Fueron verificados los indicadores:

  - ✓ Proceso: Gestión Incorporación Tecnológica: Porcentaje de Disponibilidad del Nodo Central, que mide en porcentaje *las "Horas disponibles del nodo central en el mes, sobre el Total de horas disponibles.",* a este indicador se le han realizado los análisis cualitativos de datos y tendencias, de manera trimestral.

Los servidores que se están analizando son: Servidores:1- 5 -9 y 10, para el periodo de Abril, Mayo y Junio/2020:

MAQUINA	TIPO	IP	NOMBRE	DESCRIPCIÓN	ROL	S.O
El03vur01	VSERVER	192.168.76.66	NODO CENTRAL1	Servidor de Nodo Central Glassfish	Servidor de Aplicaciones	Oracle Linux Server release 5.9
El03vur05	VSERVER	192.168.76.70	NODO CENTRAL2	Servidor de Nodo Central Glassfish	Servidor de Aplicaciones	Oracle Linux Server release 5.9
El03vur09	VSERVER	192.168.76.74	NODO CENTRAL3	Servidor de Nodo Central Glassfish	Servidor de Aplicaciones	Oracle Linux Server release 5.9
El03vur10	VSERVER	192.168.76.75	NODO CENTRAL4	Servidor de Nodo Central Glassfish	Servidor de Aplicaciones	Oracle Linux Server release 5.9

De acuerdo con las evidencias presentadas, de donde se extraen los datos soportes del indicador: *Disponibilidad Servidores Nodo Central*, se observa que el reporte trimestral presenta el rango de tiempo que duraron los servidores fuera de servicio, el cual ha sido por debajo de los 6 segundos, por lo tanto de acuerdo con el porcentaje definido como meta aceptable, éste se encuentra por debajo, quedando dentro del rango establecido.

- ✓ Proceso: Gestión Recursos de Tecnología: "*Porcentaje de equipos (PC´s y Servidores) con protección de antivirus para la vigencia 2020.",* se observó que a este indicador se le ha realizado trimestralmente el análisis cualitativo de datos y tendencias; sin embargo, de acuerdo con las evidencias presentadas: Informe antivirus KASPERSKY SECURITY CENTER 11; de los meses de Julio, Ago y Sep/2020, se observó que en el informe entregado como soporte, no se mencionan los datos registrados en el "Reporte de Datos" del indicador, respecto a los "*Equipos con instalación de protección (antivirus)",* es decir, que no se observó el soporte de reporte para los siguientes datos:

Jul	Ago	Sep
2071	2110	2136

Esta situación genera el riesgo de no contar con los soportes del reporte realizado mensualmente, es decir no se cuenta con la trazabilidad del dato consignado en el indicador, con el fin de tener un conocimiento documentado del grado de avance, o el logro de los objetivos y resultados esperados, por lo que se recomienda aprovechar la información generada en el proceso de seguimiento y evaluación para responder a requerimientos externos y / o toma de decisiones; máxime si se tiene en cuenta la actual situación de pandemia, donde puede ocurrir que no se visualicen los equipos que llevan días sin encenderse, o que fueron llevados a casa de los funcionarios.

De otra parte, se observó que en el denominador se están relacionando 3000 equipos, como la cantidad de equipos reportados en el Directorio Activo – (Equipos programados para instalación de antivirus de la SNR (inlcuye orips)), cantidad que es inferior a la totalidad de equipos existentes en la SNR, que de acuerdo con el último reporte de información realizada a la Dirección Nacional de Derechos de Autor, asciende a 4.273 equipos, situación que evidencia el riesgo de dejar sin protección mensual de antivirus un total de 1.273 equipos. – aspecto que ha sido evidenciado en informes anteriores de seguimiento efectuados por la Oficina de Control Interno.

- ✓ Proceso: Gestión Recursos de Tecnología: "*Porcentaje de Mantenimientos preventivos realizados."* Se observó que a este indicador se le ha realizado trimestralmente el análisis cualitativo de datos y tendencias; sin embargo, de acuerdo con las evidencias presentadas: Cronograma de actividades para los mantenimientos preventivos a realizarse en los meses de Jul, Ago, y Sep/2020, se encontró que los datos de origen reportados inicialmente, para el mes de Julio/2020, difieren de los datos reportados y consignados en el reporte de datos del indicador, de acuerdo con los soportes de consolidado y seguimiento presentado por la Mesa de Ayuda.

De otra parte, en la verificación de los indicadores del sistema de gestión de seguridad y privacidad de la información, se encontró que estos indicadores, aunque fueron incluidos en el formato establecido, no están siendo gestionados, toda vez que no se están haciendo los análisis cuantitativos o cualitativos de datos que permitan observar las tendencias de cambio generadas, de tal forma que se monitoree y evalúe la gestión, se monitoreen los riesgos que pueden afectar tal cumplimiento y la aplicación de controles para su mitigación. Así mismo, se observó que éstos no se encuentran aprobados por el Comité de Gestión y Desempeño Institucional.
Tampoco se presentaron evidencias de indicadores definidos para medir el desempeño alcanzado en las TI, ni indicadores de uso y apropiación de las mismas, que permitan evaluar el nivel de adopción de las mismas, así como la satisfacción en su uso, y tampoco se presentaron evidencias de indicadores de resultado, con los cuales se busca medir el cumplimiento de los logros de la política de Gobierno Digital, en cuanto a los siguientes temas:

- Ahorro en términos de tiempos y recursos
- Disminución de costos
- Nivel de satisfacción de usuarios internos y externos
- Tasas de uso de procesos, trámites y servicios digitales vs. Presenciales
- Uso de datos e información por parte de ciudadanos

Entre otros, tampoco se ejecutan acciones de mejora y transformación a partir de los resultados obtenidos. Estas situaciones contravienen lo establecido en la Política de Gobierno Digital, numeral, 4.1. Seguimiento y Evaluación por parte de la Entidad; y los numerales 5.5. Anexo 5 – Indicadores de Cumplimiento: Arquitectura y numeral 5.6. Anexo 6 – Indicadores de Cumplimiento: Seguridad. Así como lo señalado en el MIPG, *4ª. Dimensión: Evaluación de Resultados, numeral 4.2.1. - Seguimiento y evaluación del desempeño institucional: Revisar y actualizar los indicadores y demás mecanismos de*

seguimiento y evaluación establecidos en la entidad y por otras autoridades; donde se precisa tener en cuenta que, si bien desde la dimensión de Direccionamiento Estratégico y Planeación se lleva a cabo el diseño de los indicadores, antes de su aplicación, no sobra validar que éstos brindan la información suficiente y pertinente para establecer el grado de avance, para el caso de los indicadores de seguimiento, o el logro de los objetivos y resultados esperados. De no ser así, es importante efectuar los ajustes a que haya lugar.

Así mismo, se recomienda revisar y tener como referente, en uso de las buenas prácticas, indicadores utilizados por otras entidades líderes de políticas y órganos de control para medir el desempeño de la entidad. De esta manera, se podrá aprovechar la información generada en el proceso de seguimiento y evaluación para responder a requerimientos externos.

5.5- Verificación de aspectos relacionados con la planeación y gestión de los componentes de información de tecnologías de la información (TI):

Se revisó el catalogo de componentes de la información aportado como evidencias, el cual una vez revisado se observa que no cuenta con fechas de las actualizaciones realizadas o control de versiones, que permita conocer su estado de actualización. Así mismo, aunque cuenta con las tablas de los atributos de información (Atributos de Información; Atributos de Datos; de Flujo de Información; de flujo de información sectorial; y de Servicios de Información); se encontró que éste presenta desactualización en su consolidación respecto a la totalidad de los componentes de información existentes en la entidad, toda vez que solo fueron consolidados los siguientes atributos de información:

-Cambio de propietario o poseedor de un bien inmueble
-Índices de Propietarios
-Estudios Traditicios
-Servicio Consulta datos básicos de un predio
-Servicio Consulta datos jurídicos de un predio
-Servicio Consulta del PDF copia simple

Teniendo en cuenta que la Guía de Mintic - G.INF.07- cómo construir el Catálogo de Componentes de Información, señala en el numeral 3.1, Cuál es la información que se debe identificar para construir al catálogo, y señala:

"*a. Identificar y reunir las fuentes de información: entre las fuentes de información que la entidad debe identificar y revisar son el registro de activos de información que definió la entidad en virtud de la Ley de acceso y transparencia a la información pública, los datos abiertos que tiene publicados, el listado de datos maestros si la entidad ya los tiene identificados, entre otras fuentes de información que posea la entidad y que sirvan de insumo para la consolidación de la información que produce la entidad.*
b. Identificar a partir de las funciones y obligaciones legales de la entidad que información debe producir.
c. Realizar la validación de la información identificada con todas las áreas, con el fin de identificar información faltante."

Y toda vez que no se están relacionando los diferentes servicios que presta la SNR y que están gestionados como datos abiertos: por citar un ejemplo: -Hipotecas en Colombia, Remates en Colombia, Embargos en Colombia.

Lo anterior, en el entendido que el catálogo de componentes de información, representa el punto de partida para la construcción de la arquitectura de información y la base para iniciar procesos de calidad de información de la entidad e interoperabilidad entre entidades, por lo que se hace necesario que la entidad conozca cuales componentes de información posee y sus características con el fin de proyectar nuevos servicios de información, identificar fuentes únicas de información, oportunidades de mejora en seguridad y calidad de los datos e información, identificar datos maestros, datos abiertos, definir controles y mejorar el nivel de acceso a la información y demás actividades propias de la gestión de información, tal como lo señala la mencionada Guía, por lo tanto se recomienda dar cumplimiento a lo establecido en la Guía G.INF.07- cómo construir el Catálogo de Componentes de Información, teniendo en cuenta que Mediante Decreto 1008 de 2018 *"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital*" en su Artículo 2.2.9.1.2.2. Manual de Gobierno Digital. 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"*, de la cual hace parte integral la Guía Inf.07.

5.6- Verificación de aspectos relacionados con la planeación y gestión de los sistemas de información de tecnologías de la información (TI):

Para este ítem, se verificó el catálogo de los sistemas de información. En la revisión documental de la información aportada por la Oficina de Tecnologías de la Información, se evidenció que éste no presenta fecha de actualización, por lo tanto no se puede establecer la última actualización que refleje fielmente la realidad de los sistemas de información. Así mismo, se encontró que en algunos apartes del formato faltó diligenciar la descripción del "Sistema", la "ubicación de la documentación técnica", "la categoría", "el tipo", el "proveedor", el "licenciamiento", el "tipo de desarrollo", "vencimiento de la licencia", la "plataforma de aplicaciones", la "ubicación del servidor de aplicaciones", "lenguaje de programación", la "plataforma de base de datos", "ubicación del servidor de base de datos", entre otros. Con respecto a la guía No.3- faltan atributos como: versión del sistema, tipo de desarrollo, fecha de vencimiento del soporte, sistema operativo. Finalmente, no se encontró publicado en la pág. Web de la entidad.

Se recomienda dar cumplimiento al lineamiento, teniendo en cuenta que mediante Decreto 1008 de 2018 "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital" en su Artículo 2.2.9.1.2.2. Manual de Gobierno Digital. 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 el lineamiento LI.SIS.02- MINTIC – Catálogo de sistemas de información, establece que: "es un instrumento base sobre el cual se inicia la documentación de una arquitectura de sistemas de información", no obstante en la guía G.SIS.03 describe los atributos para la construcción del catálogo de sistemas de información.

5.7- Verificación del soporte y operación de la infraestructura de TI (o servicios tecnológicos):

En la revisión documental de la información aportada por la Oficina de Tecnologías de la Información, se evidenció que la entidad ha implementado un instructivo para el manejo de residuos peligrosos – RAES, sobre cómo hacer la correcta disposición final de los residuos tecnológicos, de acuerdo con la normatividad expedida por el Gobierno Nacional. Así mismo, hace uso de servicios de computación en la nube para mejorar los servicios que presta la entidad; sin embargo, con relación a la implementación de un plan de continuidad del negocio se observó que éste 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.

Igualmente, se observó que éste documento como está planteado, no 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 al negocio; tampoco 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 podría conllevar a generar inobservancia a lo establecido mediante Decreto 1008 de 2018 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital" en su Artículo 2.2.9.1.2.2. Manual de Gobierno Digital 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", en la Guía para la preparación de las TIC para la continuidad del negocio señala*: "La gestión de la continuidad del negocio, es un proceso para holístico a través del cual se identifican los impactos potenciales que amenazan la continuidad de las actividades de las Entidades, proveyendo un marco de referencia para la construcción de la resiliencia y la capacidad de una respuesta efectiva, que le permita proteger los intereses de las Entidades debido a disrupciones. La guía expuesta en este documento es un complemento del modelo de seguridad y privacidad de la información y se constituye en un referente de la continuidad del negocio para las entidades del Estado."*

Con el fin de prevenir la afectación de la cadena de valor de la información existente en la Entidad, la Oficina de Control Interno recomienda dar cumplimiento a la mencionada guía, contando con un plan de contingencia para mantener o recuperar las operaciones, asegurar la disponibilidad de la información en el grado y la escala del tiempo requerido por la Entidad, teniendo presentes las siguientes características, dentro del plan:

a) Una estructura organizacional adecuada para prepararse, mitigar y responder a un evento contingente, usando personal con la autoridad, experiencia y competencia necesarias.

b) Personal formalmente asignado de respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para manejar un incidente y mantener la seguridad de la información.

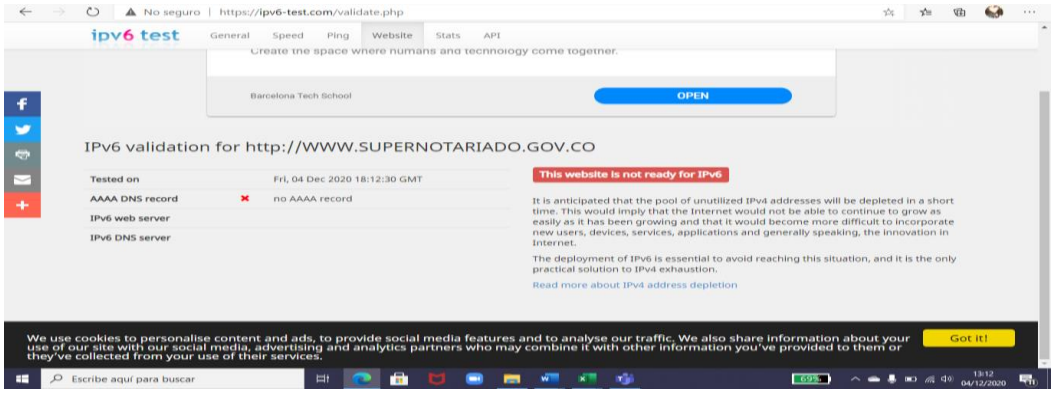
c) Planes aprobados, procedimientos de respuesta y recuperación documentados, en los que se especifique en detalle como la organización gestionará un evento contingente y mantendrá su seguridad de la información en un límite predeterminado, con base en los objetivos de continuidad de seguridad de la información aprobados por la Dirección.

5.8- Verificación realizada a la adopción de IPv6 en la entidad

Para la verificación de este ítem, se solicitaron evidencias de la documentación existente sobre las pruebas de funcionalidad efectuadas para la adopción de IPv6 en la entidad, así como el estado actual de su implementación.

En la revisión documental de la información aportada por la Oficina de Tecnologías de la Información, se observó el documento denominado DISEÑO, DESARROLLO E IMPLEMENTACIÓN PARA LA TRANSICION DEL PROTOCOLO IPV4 A IPV6, el cual se encuentra en borrador; también se entregaron los ANEXOS 1.- EQUIPOS Y SOFTWARE BASE DE SNR v1.8.xlsx y ANEXO 2. SISTEMAS DE INFORMACIÓN DE SNR v1.9.xlsx. Así mismo, la OTI aportó acta de realización de pruebas, con fecha 2 de diciembre de 2019.

El borrador no presenta fecha de elaboración, ni control de versiones. Así mismo, 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.supernotariado.gov.co, como se muestra a continuación:



Como se puede observar, el reporte arrojado manifiesta: "*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.,* Art. 3- Plazo de adopción, que señala: *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. Por su parte, las entidades territoriales deberán finalizar dicho proceso a más tardar el 31 de diciembre del año 2020, acorde al plan de diagnóstico formulado por cada entidad.",* 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*", entregado como evidencia y donde se describen las fases establecidas para el proceso de transición del protocolo, se observa que en la fase 1 se realizó la validación de la infraestructura tecnológica de la entidad con el grado de compatibilidad del protocolo IPV6, encontrando inconsistencias respecto al inventario de aplicativos y su validación de soporte al protocolo IPv6, toda vez que se menciona la siguiente información para los aplicativos:

1-FOLIO si soporta IPv6,
2-SIAN no soporta IPv6,
3-VIKI no soporta IPv6,
4-SIR no soporta IPv6,
5-Sucesiones si soporta IPV6,
6- E-learning si soporta IPV6.

Para el caso No.3, se presentaron evidencias que contradicen el diagnóstico consignado en el informe, con lo anterior se advierte sobre el riesgo de no contar con un inventario real de los aplicativos existentes y que soporten el nuevo protocolo en la entidad para realizar la implementación de IPv6, por lo que la Oficina de Control Interno de Gestión, advierte sobre la

necesidad de que se cuente con un certificado de compatibilidad al nuevo protocolo IPV6 de cada uno de los aplicativos, y en lo posible, que sea expedido por el proveedor de éstos, de acuerdo con pruebas y validaciones que deberán ejecutarse por cada uno de ellos, tal como lo señala la guía de transición de IPv4 a IPv6 expedida por MINTIC.

Así mismo, se recomienda contar con un plan de acción y cronograma documentado para aquellos aplicativos que no soportan el protocolo IPv6. Tener presente los planes de capacitación para los diferentes funcionarios, y contar con los soportes documentales para cada una de las fases (**Planeación**- plan de diagnóstico - Plan detallado del proceso de transición - Plan de direccionamiento IPv6 - Plan de contingencias para IPv6; **Implementación** - Documento de diseño detallado de la implementación de IPv6- Informe de activación de políticas de seguridad en IPv6; **Pruebas de funcionalidad** - Documento de pruebas de funcionalidad en IPv6 - Acta de cumplimiento a satisfacción de la entidad sobre el funcionamiento de los elementos - intervenidos en la fase de implementación; y **adopción del protocolo**), de acuerdo a la Guía de Transición de IPv4 a IPv6 para Colombia.

5.9- Verificación realizada a los trámites o servicios de la entidad que requieren interoperabilidad y uso del Marco de Interoperabilidad para realizar intercambio de información con otras entidades: En la revisión documental de la información aportada por la Oficina de Tecnologías de la Información, se observó que actualmente se están realizando acciones tendientes a lograr la integración de los Sistemas de Información para realizar intercambio de información a través de interoperabilidad entre los sistemas de información del IGAG y la SNR; y aunque se presentó como evidencias el Protocolo Técnico de Intercambio de Información Superintendencia de Notariado y Registro (SNR) - Instituto Geográfico Agustín Codazzi (IGAC), y algunas pruebas efectuadas; a la fecha de la auditoria, no se presentaron soportes de las diferentes reuniones sostenidas entre la Delegada de Registro, la Dirección Técnica Registral y la Oficina de Tecnologías, que permitan determinar los acuerdos o autorizaciones que se pudieron establecer en el marco de éstas reuniones y como soporte de las mismas para el intercambio de información.

Igualmente, no se presentaron evidencias de la realización de un convenio que permita establecer el cumplimiento frente al acuerdo marco de interoperabilidad para Gobierno Digital, 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. Este contrato incluye información relacionada con la identificación del servicio como son: entidad proveedora, responsables, descripción, contactos, versión, disponibilidad, documentación normativa. Adicionalmente, este contrato describe información técnica como: la implementación de la interfaz de los servicios de intercambio, la forma de comunicación, es decir, los requisitos del protocolo y los formatos de los mensajes necesarios para interactuar con los servicios listados en su catálogo, los cuales deben estar estandarizados en el Lenguaje Común de Intercambio de Información. También describe las operaciones y mensajes que soporta junto con el protocolo concreto del formato del mensaje.";* 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, de acuerdo con el cronograma general de actividades del proyecto que fue denominado *"Plataforma de Interoperabilidad Registro Inmobiliario - Segregados y Propietarios"*, se solicitaron evidencias de las pruebas y aprobación efectuada por parte de Mintic y de la entidad, para el despliegue en ambiente de producción y las pruebas ejecutadas para el ambiente en preproducción contempladas en las fases 3 y 4, encontrando que no se cuenta con las actas que evidencien estas aprobaciones, y no se presentaron evidencias de los "Lineamientos de interoperabilidad" en el cual se formalice la interacción entre las entidades IGAC-SNR.

Estas situaciones denotan la necesidad de contar con soportes documentales de cada una de las actividades programadas, así como lo contemplado en cada una de las fases establecidas, a fin de dar cumplimiento a lo señalado mediante Decreto 1008 de 2018 "*Por el cual se establecen los lineamientos generales de la política de Gobierno Digital"* en su Artículo 2.2.9.1.2.2. "*Manual de Gobierno Digital 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 de acuerdo con el Marco de interoperabilidad para Gobierno

Digital cuyo objetivo señala: *"Apoyar a las entidades públicas en sus esfuerzos por diseñar y ofrecer trámites y servicios en línea a otras entidades públicas, ciudadanos y empresas que, en la medida de lo posible, sean digitales por defecto, es decir, que proporcionen servicios y datos preferentemente a través de medios digitales, siendo accesibles para todas las entidades, los ciudadanos y que permitan la reutilización, participación, acceso y transparencia*".

5.10- Verificación realizada a los Riesgos de los Procesos de Tecnologías de la Información:
Para la verificación de este ítem, se revisaron las evidencias documentales que fueron subidas por el macroproceso a la One Drive, a la fecha de auditoría. Así mismo, se solicitaron soportes de los riesgos identificados para el Sistema de Gestión de Seguridad de la Información – SGSI. Se revisó este tema teniendo en cuenta la importancia de las acciones para abordar los riesgos frente al impacto del servicio prestado y el cumplimiento de los objetivos de los procesos que por misionalidad y transversalidad debe ejecutar la Oficina de Tecnologías de la Información.

Se lleva un informe de seguimiento de riesgos, en el cual se encontró un riesgo materializado – *Daño de Activos de Tecnología que afecten la disponibilidad de la información de los aplicativos misionales u otra información*; de acuerdo con informe de seguimiento segundo cuatrimestre de 2020, donde se manifiesta que el riesgo de gestión *"se Materializo, ya que la oficina de Tecnologías de la Información se permite indicar que actualmente se encuentra realizando las actividades técnicas correspondientes para garantizar la publicación de la información del portal web de la entidad como es el caso del link o botón de transparencia y acceso a la información pública como lo ordena la Ley 1712 de 2014".*

Esta situación podría conllevar a generar incumplimiento con lo establecido en el Decreto No.1499/2017: MIPG – 4ta Dimensión, numeral 4.2.1 – Seguimiento y evaluación del desempeño institucional, en lo relacionado con Evaluar la Gestión del Riesgo de la Entidad, donde se debe analizar el contexto interno y externo de la entidad para la identificación de los riesgos y sus posibles causas, así como retos, tendencias y oportunidades de mejora e innovación en la gestión, teniendo presente que cuando se detecten desviaciones en los avances de gestión e indicadores, o posibilidad de materialización de un riesgo, es indispensable que el responsable establezca las acciones de mejora de manera inmediata. La utilidad de este ejercicio es apoyar la toma de decisiones para lograr mejores resultados, gestionar con mayor eficacia y eficiencia los recursos y facilitar la rendición de cuentas a los ciudadanos e informes a los organismos de control.

Así mismo, y una vez valorados los cinco (5) riesgos de procesos publicados en la One Drive, se evidenció en la ejecución de la auditoría que de acuerdo con el formato de la matriz de riesgos, en la redacción de los controles, que se obtuvo una calificación de 35 puntos, encontrándose en un rango entre 0 y 85; lo que significa conforme a la Guía de Administración de Riesgos vigente, que la solidez del conjunto de controles es débil, y la ejecución del control no es suficiente para evitar la materialización de los riesgos. Con respecto a los soportes documentales de ejecución de controles existentes en la One Drive, se evidenció que estos se encontraron incompletos. Por lo anterior, es necesario y se debe establecer un plan de acción donde se indiquen claramente las 6 variables para la redacción del control. Se recomienda seleccionar actividades de control preventivas que por sí solas ayuden a la mitigación de las causas que puedan originar los riesgos.

Con respecto a los riesgos de seguridad y privacidad de la información, luego de verificar el avance alcanzado, se encontró que no se está utilizando la metodología para la identificación, tratamiento, valoración de los riesgos identificados, por lo que no se están gestionando. También se evidencia que no han sido aprobados por el Comité de Gestión y Desempeño Institucional, incumpliendo lo establecido en el Manual de Gobierno Digital, Política General para la Administración de Riesgos y Oportunidades Código: DE - SOGI - POL - 01 Versión: 03 Fecha: 24 de abril del 2020. Guía para la identificación de riesgos, oportunidades, evaluación del diseño y efectividad de controles Código: DE - SOGI – PR – 07 -GI - 01 Versión: 03 Fecha: 06 de febrero de 2020. Así como lo establecido en el Decreto 1008 de 2018 "*Por el cual se establecen los lineamientos generales de la política de Gobierno Digital*" en su Artículo 2.2.9.1.2.2. Manual de Gobierno Digital 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". En el Lineamiento LI: ST.14- MINTIC –"*La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe realizar el análisis y gestión de los riegos asociados a su infraestructura tecnológica haciendo énfasis en aquellos que puedan comprometer la seguridad de la información o que puedan afectar la prestación de un servicio de TI."*

De igual manera, se considera indispensable y oportuno, fortalecer la identificación de los riesgos y diseño de los controles del Macroproceso de Tecnologías de la Información, tomando en cuenta, las advertencias identificadas en el desarrollo de esta auditoría y las oportunidades de mejora que se han recomendado por parte del Equipo Auditor, a fin de prevenir, mitigar y evitar la materialización de situaciones críticas o desviaciones que pongan en riesgo el cumplimiento del objetivo de sus procesos.

6- REVISIÓN EFECTUADA A LA IMPLEMENTACIÓN DEL CONPES 3854 – "*POLÍTICA NACIONAL DE SEGURIDAD DIGITAL"*

Teniendo en cuenta el creciente uso del entorno digital en Colombia y para desarrollar las diferentes actividades económicas, se generan incertidumbres y riesgos inherentes de seguridad digital que deben ser gestionados permanentemente. No hacerlo, puede resultar en la materialización de amenazas o ataques cibernéticos, generando efectos no deseados de tipo económico para el País, y afectando la integridad de los ciudadanos en este entorno, tal como lo señala el Documento Conpes 3854, motivo por el cual se hace necesario el fortalecimiento de capacidades de ciberseguridad, y actividades de investigación y concientización para la generación de conocimiento en torno a la seguridad digital.

A continuación, se presentan los ítems verificados, respecto a la gestión de la Política Nacional de Seguridad Digital en la Superintendencia.

6.1. Verificación de acciones realizadas por la entidad para fortalecer las capacidades en seguridad digital

En la revisión efectuada a este ítem, se solicitaron evidencias respecto a las acciones realizadas por la Oficina de Tecnologías, en representación de la Superintendencia para fortalecer las capacidades en seguridad digital, en cuanto a si se han establecido convenios o acuerdos de intercambio de información para fomentar la investigación, la innovación y el desarrollo en temas relacionados con la defensa y seguridad nacional en el entorno digital.

Al respecto, se presentaron evidencias correspondientes al intercambio de información entre el Comando Conjunto Cibernético - CCOCI y la Superintendencia, que contiene el reporte periódico de incidentes informáticos, para que las entidades tomen las medidas correspondientes, respecto a las IP reportadas y con las siguientes recomendaciones de seguridad: Agregar los indicadores de compromiso en Listas Negras; Generar campañas de concientización hacia los usuarios de la red en cuanto a seguridad contra ataques de Phishing; y Mantener sistemas informáticos y sistemas de seguridad actualizados.

Así mismo, se presentaron evidencias de la reunión a la que asistió la SNR, realizada con el sector Justicia realizada el 2 de abril de 2020, cuyo objetivo refiere "*Sensibilizar a funcionarios y contratistas del Ministerio que deben identificar activos y riesgos en los procesos. Adicionalmente, sensibilización a los líderes de seguridad de la información del Sector justicia (Ministerio de Justicia y del Derecho, SNR, USPEC, INPEC, Agencia Nacional de Servicios Penitenciarios) en temas de activos y gestión de riesgos."* Y reunión del 27 de mayo de 2020, de sensibilización sobre temas como -protección de datos personales; -explicación de la herramienta TrendMicro brindada por la OEA donde hay cuatro herramientas para phishing, evaluación de diagnóstico de seguridad de la información, antivirus y análisis y detección de software malicioso. -Definición de actividades, responsables y fechas para el plan de trabajo Célula SGSI. También presentaron copia del borrador de la Política de Seguridad de la Información.

Las anteriores, son acciones tendientes para fortalecer las capacidades en seguridad digital; sin embargo, 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) y como mecanismos para facilitar la cooperación, colaboración y asistencia entre las diferentes entidades estatales y la SNR, con el fin de prevenir cualquier incidente digital. Por lo anterior, se recomienda realizar los convenios a que haya lugar, con el fin de documentar la cooperación y compromiso por parte de las entidades.

6.2- Avance alcanzado en el uso de los instrumentos en seguridad digital, definidas por el Gobierno Nacional:

Se solicitaron evidencias que permitan revisar el avance alcanzado en el uso de la Política de Seguridad Digital, de acuerdo con lo definido por el Gobierno Nacional a través del CONPES 3854 de 2016.

- En la revisión documental de la información aportada por la Oficina de Tecnologías de la Información, se observó que se está avanzando en la actualización del Manual del SGSI, con el fin de velar por la seguridad de la información de la Superintendencia de Notariado y Registro (SNR), para el Sistema de Gestión de Seguridad y bajo la Norma Internacional ISO/IEC 27001:2013 - que establece los requisitos para la implementación del SGSI, para proteger los activos de la información, puesto que día a día se incrementa el nivel de amenazas que pone en riesgo el desarrollo y crecimiento de las entidades.

También presentaron como soporte la "*Política de Gestión de Incidentes de Seguridad de la Información*", el cual se encuentra en proceso de actualización con el fin de preparar, detectar y analizar, contener, erradicar y recuperar, y generar actividades post-incidente, de los incidentes de seguridad de la información que puedan llegar a generar un riesgo a los procesos de la entidad. Presentaron también la "*Política de Requerimientos Legales, Regulatorios y Contractuales",* a fin de evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad. Y finalmente, presentaron el borrador de la "*Política de Seguridad de la Información por Dominio de la Norma NTC-ISO-IEC 27001:2013*", alineadas a los 14 dominios de la NTC-ISO-IEC 27001:2013 y bajo las recomendaciones de la NTC-ISO-IEC 27002:2013; a través de la cual se busca garantizar y exigir el buen uso de la información a todos los funcionarios, contratistas, proveedores, visitantes, terceros entre otros; así como Implementar las normas bajo las premisas de las políticas de seguridad que garantice el cumplimiento de los requisitos y promover la cultura frente a la Seguridad de la Información a nivel interno y externo, con la finalidad de aplicar controles de seguridad de la información, y así disminuir en índice de eventos de los riesgos tecnológicos.

Con estos documentos, se observa que la Oficina de Tecnologías de la Información pretende fortalecer las capacidades de respuesta de la entidad, ante un posible evento de riesgo que pueda ocurrir a los activos de información, de acuerdo con los lineamientos definidos por el Gobierno Nacional; sin embargo, se observó que estos documentos fueron presentados por la Empresa Alina Tech S.A.S, en la vigencia 2019 y a la fecha de la auditoría, no han sido gestionados en su actualización, aprobación y difusión para su aplicación al interior de la entidad.

Por lo anterior, se recomienda gestionarlos con el fin de contar con estas herramientas de trabajo, en el marco de la Política de Seguridad Digital, utilizando los modelos de guías y manuales existentes en Mintic.

- Con respecto a la herramienta de Autenticación Electrónica, y la Carpeta Ciudadana, donde MinTIC ha conceptualizado y diseñado un modelo integral que incorpora los proyectos de Interoperabilidad, Autenticación Digital y Carpeta Ciudadana, bajo el nombre de '*Servicios Ciudadanos Digitales'*, modelo que tiene por objeto, facilitar a los ciudadanos su interacción con la administración pública y optimizar la labor del Estado, estableciendo la necesidad de garantizar la transformación digital de los trámites y servicios mediante el modelo de los Servicios Ciudadanos Digitales (SCD), para enfrentar los retos que imponen los entornos digitales.

De acuerdo con la revisión documental de la información aportada por la Oficina de Tecnologías de la Información, se informó que el 10 de julio del 2020 la SNR envía comentarios y observaciones a la "Guía Integración de Trámites y Servicios." a gov.co que viene consolidando MINTIC, evidencia archivo de excel "*Observaciones Guía Integración de Trámites*", e informa que el 09 de Nov./2020 se solicita a MINTIC los lineamientos de la "Guía de integración de trámites y servicios". Por su parte, el ministerio TIC expide la Resolución 02160 de 23 de Oct.2020 y sus anexos: "*Por la cual se expide la Guía de lineamientos de los servicios ciudadanos digitales y la Guía para vinculación y uso de estos*". En los anexos 2 y 3 podrán encontrar proceso de vinculación al servicio de carpeta ciudadana digital, Requerimientos, Alcances y Definiciones.

Se presentan evidencias del 20 de Nov./2020, por el cual se envía los documentos a los coordinadores y el jefe de la OTI para análisis y revisión de los respectivos lineamientos, con el fin de aclarar dudas para realizar las mesas de trabajo con MINTIC, y para lograr e iniciar el plan de implementación de la carpeta ciudadana.

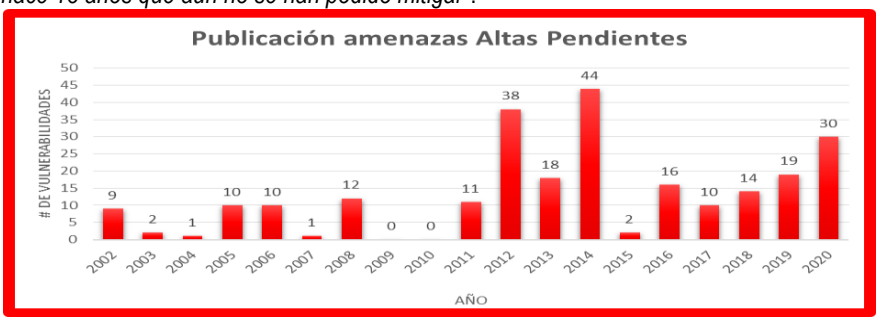
Al respecto, se recomienda realizar las gestiones necesarias para dar cumplimiento a los lineamientos definidos por Mintic, teniendo en cuenta que la Guía para la vinculación y uso de los Servicios Ciudadanos Digitales es el documento expedido y publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones destinado a las autoridades referidas en el

artículo 2.2.17.1.2. del Decreto 1078 de 2015, que indica cuáles son las condiciones necesarias y los pasos que deben realizar para la preparación, adecuación, integración, uso y apropiación de los servicios ciudadanos digitales, a través de los cuales podrán vincular a sus sistemas de información los mecanismos de autenticación digital, interoperabilidad y carpeta ciudadana digital.

- Adicionalmente, se solicitaron evidencias sobre los estudios realizados en la SNR, relacionados con Seguridad Digital (Impacto económico de los incidentes, amenazas y ataques cibernéticos), y si la entidad efectúa ejercicios de simulación y respuesta a ataques cibernéticos, o evaluaciones de vulnerabilidades informáticas.

Al respecto, en la revisión documental de la información aportada por la Oficina de Tecnologías de la Información, se observó que se están generando los cuadros de mando mensuales, desde Abril de 2020 a noviembre de 2020 - herramienta a través de la cual la Oficina de Tecnologías realiza el análisis al estado de vulnerabilidades presentadas en la entidad, identificando sus características como son la IP, el puerto, segmento de red, la vulnerabilidad, el nivel de criticidad, el tipo de ataque, el estado actual, la gestión de la remediación, entre otros items. Así mismo, presentaron evidencias de los informes consolidados mensualmente como línea de seguridad.

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 Critico" 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, aún existen amenazas de nivel crítico detectadas hace 18 años que aún no se han podido mitigar*".



Fuente: Informe Ejecutivo de Seguridad de la Información" del mes de agosto de 2020

Por lo anterior, se recomienda establecer un plan de trabajo para determinar las acciones tendientes a solucionar o corregir las vulnerabilidades presentadas y que a la fecha se encuentran sin un tratamiento efectivo de mitigación, de acuerdo con el comportamiento de las amenazas registradas mes a mes, con el fin de evitar el riesgo de permitir a un ciberdelincuente obtener acceso de forma remota, sin necesidad de tener ningún tipo de autenticación.

6.3- Verificación efectuada a la implementación de un Sistema de Gestión de Seguridad de la Información en la SNR: Verificado el documento aportado por la OTI, sobre la implementación de un Sistema de Gestión de Seguridad de la Información, se observa que se viene documentando el Manual del SGSI y la Política de Seguridad de la Información por Dominio de la Norma NTC-ISO-IEC 27001:2013. Igualmente, se observa el proyecto o borrador del procedimiento: Gestión de Incidentes de Seguridad de la Información, entre otros; los cuales se observa que no han sido aprobados por la Oficina Asesora de Planeación, generando el riesgo de no contar con las diferentes herramientas que permitan identificar, atender y minimizar los riesgos que puedan atentar contra la integridad, confidencialidad y disponibilidad de la información en la entidad.

Se recomienda avanzar con las gestiones necesarias a fin de documentar e implementar el conjunto de controles y procedimientos para alcanzar un correcto nivel de seguridad en el manejo, transformación y operación de la información y de igual forma administrar estos controles para mantener este nivel a lo largo del tiempo, el cual ayudará a centrar los esfuerzos y recursos en la mitigación de los riesgos que sean identificados como de mayor impacto y/o probabilidad conforme al análisis y

evaluación de éstos y para dar cumplimiento a los lineamientos establecidos a través del CONPES 3854 POLÍTICA NACIONAL DE SEGURIDAD DIGITAL", en lo relacionado con la gestión del riesgo de seguridad digital.

Igualmente, se observa que no han sido caracterizados los riesgos cibernéticos ni se han identificado los supuestos, ni se ha logrado analizar el impacto que podría ocasionarse en caso de tener afectaciones de este tipo.

Cabe señalar, que mediante la adopción del Modelo de Seguridad y Privacidad por parte de las Entidades del Estado, se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.

7. Verificación Planes de Mejoramiento:
Luego de verificado el seguimiento consolidado a los Planes de Mejoramientos que se lleva en la Oficina de Control Interno, se observó que para la Oficina de Tecnologías de la Información presenta acciones para el Plan de Mejoramiento Institucional y para el plan de mejoramiento con la Contraloría General de la Republica; sin embargo, a través de la evaluación efectuada en la presente auditoría, se logró evidenciar el vencimiento de estas acciones, como se describe en la muestra seleccionada:

7.1. Verificación Hallazgos Plan de mejoramiento Institucional.
Fueron revisados las siguientes acciones para los hallazgos:

a. **Hallazgo:** Verificación del registro del SISG ante la Dirección Nacional de Derechos de Autor: se encuentra que aunque se han adelantado gestiones para su registro; a la fecha de esta auditoría, no se ha surtido el trámite correspondiente; adicionalmente, la actividad o acción se encuentra en estado vencida, la cual estaba programada para el 30 de mayo de 2020.

b. **Hallazgo:** En la entidad se evidencian equipos de cómputo que no cuentan con el software de antivirus instalado, situación que genera el riesgo de pérdida de información.

Acciones:
1. Actualizar inventario de computadores (PC) e informe de implementación del antivirus (incluyendo información de equipos con versiones anteriores)
3. Estudio previo de renovación de equipos.
Estas dos acciones se encuentran vencidas e incumplidas; por cuanto la primera, tenía plazo de cumplimiento hasta el 30 de enero y la tercera, al 30 de noviembre de 2020.
Adicionalmente, se considera importante advertir, que este hallazgo, se evidencia como recurrente, por las situación evidenciada en el desarrollo de esta auditoría.

c. **Hallazgo:** Desconocimiento y falta de aplicación del procedimiento “Back up y protección de la información”, razón por la cual no se está garantizando la salvaguarda de la información (Aplicaciones, Bases de Datos y data no estructurada) de la Superintendencia de Notariado y Registro, mediante la generación de copias de seguridad en medios magnéticos y su posterior almacenamiento y custodia en una entidad externa.
Acción: Actualización de procedimiento de Backups, la cual se encuentra vencida e incumplida con fecha 30 de mayo de 2020.

d. **Hallazgo**: En algunas oficinas de registro y nivel central, no se ha dado cumplimiento al uso del FORMULARIO PARA ADMINISTRACIÓN DE USUARIOS NUEVOS, ACTIVOS E INACTIVOS, Código: GT-RT-PR-08-FR-01; V.5; el cual contempla la aceptación de las responsabilidades generadas en el uso del aplicativo.
Acciones:
1. Procedimiento ajustado de Administración de Usuarios.
2. Formulario actualizado para administración de usuarios nuevos, activos e inactivos, publicado en la web SNR.
3. Mesa de trabajo con la dirección Técnica de Registro, para divulgación del formulario.

Las tres acciones se encuentran vencidas e incumplidas, las cuales estaban programadas para el 30 de marzo y 30 de abril de 2020.

e. **Hallazgo:** Se observó que conforme a la información suministrada por la Oficina de Control Interno Disciplinario, en las vigencias 2017 y 2018, se iniciaron ocho (8) procesos disciplinarios, por presuntas faltas relacionadas con Manipulación, utilización y adulteración del aplicativo misional SIR; sin embargo estas conductas no han sido identificadas como causas o riesgos de posibles actos de corrupción y/o procesos.
Acción: Realizar mesas de trabajo con diferentes áreas de la SNR para verificar casos de presunta manipulación de la información, que sirvan de insumo para la Dirección Técnica de Registro y la OTI; acción vencida e incumplida, con fecha 31 de agosto 2020.

f. **Hallazgo:** Se observó que el cuarto de cómputo no cuenta con control de temperaturas y no se tiene la certeza si el detector de humo funciona o no; con respecto a la red de datos está sin identificación en el rack de alojamiento como se observa en la foto del anexo No.1. Igualmente, se encontraron cajas de cartón almacenadas en este sitio.
Acción: Crear procedimiento de buenas prácticas en centro de cómputo. Acción vencida e incumplida con fecha del 30 de junio de 2020.

g. **Hallazgo:** Se observó que existen usuarios activos en el aplicativo Folio Magnético, que no pertenecen a la ORIP. Así mismo, se encuentra necesario revisar los diferentes roles asignados a los funcionarios a través del aplicativo Folio, toda vez que existen algunos incompatibles con las funciones asignadas actualmente, conllevando al riesgo de no dar la aplicación de las buenas prácticas definidas en la Circular No.795 de 2017.
Acción: Realizar reporte y análisis de usuarios del Sistema Folio en la ORIP de Girardota para identificar usuarios activos e inactivos. Acción vencida e incumplida con fecha del 15 de mayo de 2020.

h. Hallazgo: Se encontraron diferencias en la información reportada para consolidar el reporte exigido por la Dirección Nacional de Derechos de Autor -DNDA, sobre el número de equipos tecnológicos existentes en la Oficina de Registro, de acuerdo con el inventario físico de los mismos, puesto que no fueron reportados los dos servidores existentes, en el archivo enviado a la Oficina de Control Interno (insumo de control para el informe Derechos de Autor) por la Dirección Regional. Esta situación conlleva a determinar una No Conformidad en atención al riesgo de generar información no verídica en la rendición del informe a la DNDA. Acciones vencidas al 15 de mayo de 2020. Así mismo, genera incumplimiento al Numeral 8.5.1 Control de la producción y de la provisión del servicio - ISO 9001:2015.
Acción: 1. Diseñar plantilla de inventario de servidores (Para ser enviado a nivel nacional) 2. Verificar inventario de Servidores en sitio. Acciones vencidas e incumplidas el 30 de junio y 29 de febrero de 2020.

i. **Hallazgo**: De acuerdo con los datos registrados en las Tablas Nos.13 y 14 del presente informe, se encuentran diferencias entre la información suministrada por el nivel central y la suministrada en la Oficina de Registro, con relación a la cantidad de turnos pendientes de corrección.
Acción:1. Realizar análisis de los reportes en sitio y en la ORIP. 2. Socializar a las áreas de Control Interno y la Dirección Técnica de Registro el modelo y descripción funcional del sistema Folio, Acciones vencidas e incumplidas de fecha 22 de mayo y 20 de marzo respectivamente.

7.2. Verificación Hallazgos Contraloría General de la República.

a. **Verificado el hallazgo 55**: "*ORIPS. Saldos negativos registrados en la Base de Datos que corresponden a imputaciones aritméticas entre las cuantías de los radicados. No se cuenta con los manuales de procedimientos para los aplicativos FOLIO e IRIS implementados en las Orip´s."*

Acciones:
2- *Proyectar circular o memorando del manual de Folio*: Las acciones implementadas siguen siendo no efectivas, toda vez que se observa que fue elaborada la circular 196/feb.20, cumpliendo la acción y señalando la ruta del manual de Folio; sin embargo, al revisar el Manual existente en el SIG, se encuentra que éste, está siendo actualizado con los ajustes o los correctivos técnicos realizados en el sistema, para los Saldos Negativos; sin embargo, dado que el Manual de Folio no ha sido

aprobado por la oficina de planeación, se podría determinar cómo no efectiva la acción planteada, a la fecha de la auditoría. Igualmente, se hace necesario considerar la posibilidad de implementar acciones orientadas a hacer seguimiento a la efectividad de los controles implementados en el Manual y en la Circular, por parte del dueño del Proceso, a fin de garantizar que esta misma situación evidenciada en este hallazgo, no se vuelva a presentar en las Oficinas de Registro que cuentan con el Sistema de Folio magnético.

b. **Verificado el Hallazgo 53:** "*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 de co".*

Acciones:
1. Realizar ajustes del procedimiento denominado Backup y protección de la información, así mismo revisar y analizar la modificación, eliminación o creación de los formatos y manuales asociados al mismo procedimiento y
2. Realizar Acta o documento de aprobación de la Política de Seguridad de la información por dominio ISO 27001:2013.
Se observó que las acciones del hallazgo 53, se encuentran vencidas a la fecha de la presente auditoría, toda vez que aunque existen soportes del avance alcanzado, se observó que estos documentos no han sido aprobados, ni incluidos al SIG de la entidad, por lo cual las acciones que fueron establecidas para ser implementadas no son efectivas al momento de la auditoría.

c. **Verificado Hallazgo 40**. "*No hay custodia de la información en otro sitio, las cintas están guardadas en lugares inseguros; en razón a que el contrato de la empresa que almacena y guarda la información finalizó, a la fecha no se ha renovado, la información queda expuesta (ORIP's: Medellín Sur, Medellín Nte, Rionegro, Marinilla, Girardota, Cali, Palmira, Dosquebradas, Sta Rosa de Cabal)."*

Acciones:
"Realizar estudios previos para renovación de contrato de almacenamiento y custodia con entidad externa- Seguimiento al contrato por medio de informe - ACTIVIDADES / CANTIDADES UNIDAD DE MEDIDA: 2".
Se encontró que para este hallazgo se presentó un informe de seguimiento o supervisión del contrato, dado que se dejó como unidad de medida dos informes, no se puede dar por cumplida la acción. Así mismo, de acuerdo con las acciones emprendidas, se determinan como no efectivas, toda vez que en el evento de existir algún periodo en que haya falta de renovación del contrato de custodia externa de almacenamiento de cintas, existe el riesgo de volverse a materializar el hallazgo para el Nivel Central.

El Equipo Auditor recomienda, fortalecer del análisis causa raíz de los hallazgos identificados por la Oficina de Control Interno y por la Contraloría General de la República, a fin de que se procure reformular las acciones tendientes a subsanar las desviaciones identificadas en los informes de auditorías y seguimientos correspondientes, procurando el cierre de los hallazgos; adicionalmente, se sugiere plantear acciones en los planes de mejoramientos, orientadas al monitoreo de los controles que se implementen, con el propósito de que el mismo dueño del Proceso o primera línea de defensa, constante o se asegure que éstos hayan sido efectivos.

De acuerdo con lo verificado en los numerales 7.1 y 7.2, se hace necesario tener presente por parte de cada líder de Macroproceso, como primera línea y/o segunda línea de defensa, tratándose de procesos transversales, lo señalado en el Modelo Integral de Planeación y Gestión –MIPG, establecido mediante Decreto 1499/2017, en su 7ª. Dimensión: **Evaluación de Resultados, Actividades de Monitoreo**, y respecto al numeral -7.2.1 Diseñar y mantener de manera adecuada y efectiva el MECI, desarrollando las siguientes actividades:
Cuarto componente:
-Implementar las actividades de monitoreo y supervisión continúa en el proceso que lidera, a fin de asegurar o garantizar el cumplimiento de los objetivos trazados en los mismos:
… "*- La evaluación continua o autoevaluación lleva a cabo el monitoreo a la operación de la entidad a través de la medición de los resultados generados en cada proceso, procedimiento, proyecto, plan y/o programa, teniendo en cuenta los indicadores de gestión, el manejo de los riesgos, los planes de mejoramiento, entre otros. De esta manera, se evalúa su diseño y operación*

en un período de tiempo determinado, por medio de la medición y el análisis de los indicadores, cuyo propósito fundamental será tomar las decisiones relacionadas con la corrección o el mejoramiento del desempeño.
– En ese orden de ideas se busca que cada líder de proceso, con su equipo de trabajo, verifique el desarrollo y cumplimiento de sus acciones, que contribuirán al cumplimiento de los objetivos institucionales. Se convierte, entonces, la autoevaluación en el mecanismo de verificación y evaluación, que le permite a la entidad medirse a sí misma, al proveer la información necesaria para establecer si ésta funciona efectivamente o si existen desviaciones en su operación, que afecten su propósito fundamental.
– La autoevaluación se convierte en un proceso periódico, en el cual participan los servidores que dirigen y ejecutan los procesos, programas y/o proyectos, según el grado de responsabilidad y autoridad para su operación. Toma como base los criterios de evaluación incluidos en la definición de cada uno de los elementos del control interno, así como la existencia de controles que se dan en forma espontánea en la ejecución de las operaciones y en la toma de decisiones."

8. CONCLUSIONES

La Oficina de Tecnologías de la Información a través de los diferentes desarrollos efectuados y en atención a la emergencia sanitaria declarada por el Gobierno Nacional, ha contribuido en el fortalecimiento de los servicios de la Superintendencia, de cara al cliente interno y externo, en aras de dar continuidad a las diferentes actividades desarrolladas por la entidad; sin embargo, es necesario dejar documentados los registros, producto de estas nuevas formas de realizar las actividades, con el propósito de contar con una Guía o instructivo sobre la aplicación de estas herramientas, que sirva como manual de aprendizaje.

En términos generales y de conformidad con lo revisado en los numerales y 5 y 6 del presente informe, las Políticas de Gobierno Digital y Seguridad de la información, vienen siendo implementadas a través de los diferentes elementos que la conforman; sin embargo, se encuentra la necesidad de establecer controles que permitan evidenciar el avance real alcanzado, así como su articulación con cada una de las políticas de gobierno, dejando la trazabilidad y la documentación necesaria para permitir su fácil ubicación en cada uno de los elementos que la componen; integrando estos documentos al Sistema de Gestión de Calidad de la Entidad.

Se observa la necesidad de dar a conocer al funcionario autorizado para el uso de accesos remotos, en cada una de las dependencias de la Entidad, la importancia en la adopción de medidas de seguridad, conservando las buenas prácticas en la autenticación, evitando el riesgo de accesos no autorizados desde una red externa.

Con respecto a los equipos de cómputo prestados para trabajo en casa, se considera necesario advertir sobre los riesgos que puedan generarse por el desplazamiento fuera de las instalaciones de la entidad, como daño, hurto, extravío, etc.; también por el hecho de tener prestados los equipos de cómputo a los contratistas, por lo que se recomienda realizar seguimiento a las devoluciones de estos equipos, antes del último pago del contrato.

Se encontró que los planes: Plan Estratégico de Tecnologías de la Información - PETI, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan de Seguridad de la Información, no han sido aprobados y no se encontró su publicación en la página web de la entidad; por lo que se hace necesario revisar las obligaciones de la Oficina de Tecnologías de la Información, contenidas en el Decreto 2723 de 2010 artículo 17, especialmente, el numeral 1- *"Funciones de la Oficina de Tecnologías de Información;* así como 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*."

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.

Se observó que existen Oficinas de registro y dependencias del nivel central que de acuerdo con las fechas establecidas en el cronograma de mantenimientos preventivos presentado, les fue aplazado el mantenimiento preventivo inicialmente programado debido a los diferentes obstáculos presentados en atención a la pandemia y para realizar los mantenimientos en las fechas previstas (como cierre de vías y cabeceras municipales, ausencia de medios de transporte, orden público y cierre de ORIP), por lo que se hace necesario advertir sobre el riesgo de no desarrollar la totalidad de actividades programadas, de acuerdo con el contrato celebrado por la entidad para contratar los "*servicios de mesa tecnológica y mantenimiento de equipos ofimáticos, servicios de voz ip y videoconferencia; suministro de equipos y repuestos necesarios para la operación".*

Se encontró que la Oficina de Tecnologías aunque cuenta con el mapa de sus procesos, éste no estuvo disponible en la página web durante el desarrollo de la auditoría, por lo que no se logró acceder a la documentación de sus procedimientos, formatos, manuales, etc, situación conlleva al riesgo de incumplir con lo establecido en la Política de Fortalecimiento organizacional y simplificación de procesos del MIPG, numeral 3.2.1.1.- "*la operación de la entidad se haga acorde con la manera en la que se han documentado y formalizado los procesos.",* al no contar con la documentación necesaria para la gestión de las actividades que se desarrollan en la Oficina de Tecnologías.

Verificado el avance alcanzado en la actualización de los riesgos de seguridad y privacidad de la información, se encontró que aunque fueron identificados, no se está utilizando la metodología establecida por la entidad para su identificación, tratamiento, valoración de los riesgos identificados, etc; y no se están gestionando dichos riesgos en la entidad, situación que podría conllevar a la materialización de amenazas o ataques cibernéticos, generando efectos no deseados de tipo económico para la entidad y afectando la integridad de los ciudadanos. Igualmente, se observa que no han sido caracterizados los riesgos cibernéticos, no se han identificado los supuestos, y no se ha logrado analizar el impacto que podría ocasionarse en caso de tener afectaciones de este tipo.

Se observó que en el denominador del indicador "*Porcentaje de equipos (PC´s y Servidores) con protección de antivirus para la vigencia 2020"* se están relacionando 3000 equipos, como la cantidad de equipos reportados en el Directorio Activo – (Equipos programados para instalación de antivirus de la SNR (inlcuye orips)), cantidad que es inferior a la totalidad de equipos existentes en la SNR, que de acuerdo con el último reporte de información realizada a la Dirección Nacional de Derechos de Autor, asciende a 4.273 equipos, situación que puede generar la pérdida de información por causa de no contar con un sistema de protección integral de la totalidad de los equipos, que puedan afectar los pilares de seguridad de la información– aspecto que ha sido evidenciado en informes anteriores de seguimiento efectuados por la Oficina de Control Interno.

En la verificación de los indicadores del sistema de gestión de seguridad y privacidad de la información, se encontró que, aunque fueron incluidos en el formato establecido, no se están gestionando, toda vez que no contienen los análisis cuantitativos o cualitativos de los datos; no existe monitoreo que permitan observar las tendencias de cambio generadas.

Con relación a la implementación de un plan de continuidad del negocio, se observó que éste 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 vigente. Igualmente, se observó que este documento como está planteado no 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 al negocio; tampoco 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.

Se evidenció que la entidad no ha implementado el protocolo de comunicación IPv6 en atención a la Resolución No.2720 de 2017, Art.3-Plazo de adopción; Con respecto a las acciones tendientes a su implementación se presentó el documento en borrador denominado: "*DISEÑO, DESARROLLO E IMPLEMENTACIÓN PARA LA TRANSICIÓN DEL PROTOCOLO IPV4 A IPV6*", en donde se observan inconsistencias en el inventario de aplicativos (que de acuerdo con las validaciones efectuadas por la OTI) soportan el protocolo IPv6; esta situación genera el riesgo de no contar con un inventario real de los aplicativos existentes, que soporten el nuevo protocolo para la implementación de IPv6.

Se encontró en la revisión efectuada al cuadro de mando de vulnerabilidades que existen 211 clasificadas como vulnerabilidad "Alta y Critica" que a la fecha de la auditoría no han sido gestionadas desde el mes de Agosto de 2020. 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, aún existen amenazas de nivel crítico detectadas hace 18 años que aún no se han podido mitigar*". Se recomienda establecer un plan de trabajo para determinar las acciones tendientes a solucionar o corregir las vulnerabilidades presentadas y que a la fecha se encuentran sin un tratamiento efectivo de mitigación, de acuerdo con el comportamiento de las amenazas registradas mes a mes

Verificado el documento aportado por la Oficina de Tecnologías sobre la implementación de un Sistema de Gestión de Seguridad de la Información se observa que se viene documentando el Manual del SGSI; la Política de Seguridad de la Información por Dominio de la Norma NTC-ISO-IEC 27001:2013; el procedimiento Gestión de Incidentes de Seguridad de la Información, entre otros; los cuales no han sido aprobados por la Oficina Asesora de Planeación, generando el riesgo de no contar con las diferentes herramientas que permitan identificar, atender y minimizar los riesgos que puedan atentar contra la integridad, confidencialidad y disponibilidad de la información en la entidad, a fin de dar cumplimiento a los lineamientos establecidos a través del CONPES 3854 POLÍTICA NACIONAL DE SEGURIDAD DIGITAL", en lo relacionado con la gestión del riesgo de seguridad digital.

Es importante dar cumplimiento a los términos y actividades establecidas en los Planes de Mejoramientos suscritos por la Oficina de Tecnologías de la Información, con el fin de minimizar los riesgos que ocasionaron los hallazgos, de igual manera realizar el análisis pertinente a fin de establecer o replantear nuevas acciones en el caso de no ser eficaces y eficientes las acciones planteadas inicialmente.

Se espera que con las oportunidades de mejora identificadas en este informe, se contribuya a la labor de mejora continua de los procesos de Tecnologías de la Información, de manera que sirva de herramienta para el logro de los objetivos propuestos, como en la implementación de las Políticas de Gobierno Digital y de Seguridad Digital, y su habilitador transversal - Seguridad de la información: que busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad y disponibilidad y privacidad de los datos; Habilitador soportado en el Modelo de Seguridad y Privacidad de la Información –MSPI.

9. A continuación, se relacionan los principales hallazgos evidenciados

RESULTADOS DEL SEGUIMIENTO – Oportunidades de Mejora

ITEM	HALLAZGO	TIPO DE HALLAZ-GO NC / OBS	RECOMENDACIÓN COMO OPORTUNIDAD PARA LA MEJORA	RESPONSABLES
1	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 atenciòn 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	OBS	Se hace necesario y urgente, la formalización de los manuales de uso de los aplicativos que se encuentran en funcionamiento en la Entidad, así como la actualización de los manuales existentes, cuyas herramientas tecnológicas, han sido	**Lidera:** 1**ra. Línea de Defensa:** Oficina Tecnologías de la Información

	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*.",		objeto de modificación; igualmente, se recomienda, la estandarización y adopción de los formatos requeridos en el Sistema de Gestión Institucional.	
2	Se advierte sobre un posible riesgo de pérdida de los equipos de cómputo de la Entidad que son objeto de préstamo, toda vez que verificado el formato utilizado para realizar el control de los mismos, se identificaron 25 casos, en los cuales no se diligenció completamente la información necesaria sobre los datos puntuales de dirección, documento de identidad, fecha de autorización de la salida de los equipos y cargo que ocupa en la Entidad o servicio que presta.	OBS	Se recomienda documentar con suficiente claridad, los controles implementados en el procedimiento de préstamo de inventarios y los formatos utilizados con este fin; diligenciando de manera completa los datos requeridos en los espacios del mismo, validando la información contenida en el archivo de préstamos realizados y realizar seguimiento a la devolución de los equipos, especialmente para el caso de los contratistas, antes de que finalice el contrato y se produzca el último pago Se recomienda igualmente, verificar que las pólizas de seguro de todo riesgo de los equipos de cómputo de la Entidad, que son objeto de préstamo, se encuentren cubiertos en su totalidad. Especialmente, se sugiere analizar jurídicamente los conceptos de teletrabajo y trabajo en casa, teniendo en cuenta que en la póliza de seguro, se determina el amparo para el seguro de los equipos que son prestados a los funcionarios y contratistas que se encuentran prestando servicio a través la modalidad de Teletrabajo.	**Lidera:** 1r**a. Línea de Defensa:** Gestión Administrativa
3	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.	OBS	Realizar la revisión y actualización de la pág. Web, en cuanto a los documentos soporte subidos en cada uno de los contenidos de la página web de la entidad.	**Lidera:** 1r**a. Línea de Defensa:** Oficina Tecnologías de la Información
4	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; inobservàndose 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,*	NC	Elaborar todos los planes tecnológicos requeridos en alineación con las políticas, planes, programas, y proyectos implementados bajo el liderazgo de la OTI, siguiendo las instrucciones de las guías expedidas por MINTIC para cada uno de estos planes y buscar la aprobación de los mismos, a fin de dar cumplimiento con lo establecido en el decreto 1499 de 2017, Art.17; numeral 1, realizando	**Lidera:** 1r**a. Línea de Defensa:** Oficina Tecnologías de la Información

	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 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.		permanentemente la revisión general de las metas trazadas, y en caso de ser necesario, replantearlas periódicamente, de acuerdo con la dinámica y las prioridades de la OTI, así como también de acuerdo con la evolución tecnológica, a fin de fortalecer el apoyo de gestión institucional requerido para mejorar la prestación del servicio misional en la Entidad especialmente, en cumplimiento a lo establecido en el artículo 17, numeral 1 del Decreto 2723 de 2010 y Decreto 612 de 2008 y prevenir la materialización de riesgos advertidos en èste.	
5	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 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.	OBS	Es necesario y urgente, agilizar la gestión pertinente para documentar el proceso, detallando las actividades por orden de prioridad, controles, roles y responsabilidades para todos los niveles de soportes, de acuerdo con los requerimientos legales para la prestación de los servicios que incluya el monitoreo de incidentes identificando los casos recurrentes, a fin de garantizar la continuidad en la prestación del servicio de manera eficaz, oportuna y permanente; adicionalmente, con el objetivo de que además de las acciones de corrección tomadas como definitiva a los incidentes repetitivos, se implementen acciones preventivas y/o acciones correctivas para subsanar los errores presentados por los sistemas de información, en aras de evitar reprocesos administrativos, pérdida de tiempo y recursos y reincidencia de las fallas, entre otros. Es necesario además, garantizar la transferencia de conocimiento, en caso de rotación del personal asignado para la prestación de este servicio en la Entidad.	**Lidera:** 1**ra. Línea de Defensa:** Oficina Tecnologías de la Información
6	En desarrollo de la auditoría, se observó el incumplimiento del cronograma previamente establecido con el fin de garantizar el mantenimiento preventivo a las Oficinas de registro y dependencias del nivel central de la Entidad, en cumplimiento al objeto contractual y obligaciones relacionadas con la prestación de *servicios de mesa tecnológica y mantenimiento de equipos ofimáticos, servicios de voz ip y videoconferencia; suministro de equipos y repuestos necesarios para la operación*, toda vez que conforme a las fechas establecidas en el cronograma de mantenimiento preventivo presentado, en su momento fue aplazado el mantenimiento inicialmente programado por causa de la declaración de emergencia sanitaria declarada con ocasión a la pandemia	OBS	En ejercicio de la supervisión contractual, se recomienda realizar un seguimiento a los cronogramas de mantenimiento preventivo contratados versus los mantenimientos ejecutados, a fin de verificar el nivel de cumplimiento de los mismos; igualmente, revisar cada una de las obligaciones estipuladas en el contrato de la referencia, de tal	**Lidera:** 1**ra. Línea de Defensa:** Oficina Tecnologías de la Información.

	Covid-189 (cierre de vías y cabeceras municipales, ausencia de medios de transporte, orden público y cierre de ORIP); razón por la que se hace necesario advertir sobre el incumplimiento parcial del objeto contractual y obligaciones pactadas en el mismo, que puede generar posibles daños en los equipos, pérdida de información, pérdida de recursos, entre otros.		forma, que se tomen las acciones oportunas en procura de evitar la materialización del riesgo de incumplimiento contractual y consecuencias que se puedan generar por este hecho.	
7	Se advierte sobre un posible riesgo de incumplimiento a lo establecido en la Política de Fortalecimiento organizacional y simplificación de procesos del MIPG, numeral 3.2.1.1.- "*la operación de la entidad se haga acorde con la manera en la que se han documentado y formalizado los procesos.*", ocasionando con éste, la inobservancia de la Ley de Transparencia y Acceso a la Información (Ley 1712 de 2014); toda vez que durante el desarrollo de la auditoría, se encontró que aunque la Oficina de Tecnologías cuenta con el mapa de procesos de la OTI, esta información no se encontraba disponible, por lo que no fue posible acceder a la documentación de los procesos, procedimientos, ni formatos, que estuviesen publicados en la página web de la entidad. La materialización del riesgo: "*Daño de activos de tecnología que afecten la disponibilidad de la información de los aplicativos misionales u otra información*", causado por el inconveniente técnico ocurrido a la infraestructura donde se encuentra alojado el portal web de la entidad, limitó la posibilidad de visualizar y acceder al Mapa de procesos, y al botón de transparencia y acceso a la información pública. Este riego fue reportado a la Oficina Asesora de Planeación, para su debido tratamiento.	NC	Se hace necesario y urgente, proceder a realizar un ejercicio de análisis causa raíz a fin de determinar los factores que dieron origen a la materialización del riesgo referenciado y sus consecuencias, lo cual originó el incumplimiento a la Ley de Transparencia y Acceso a la Información Púbica; a fin de documentar las acciones de control orientadas a evitar su recurrencia. Establecer backups periódicos de la información subida a la página web, fijando unas políticas apropiadas para su almacenamiento.	**Lidera:** 1**ra. Línea de Defensa:** Oficina Tecnologías de la Información. **Apoyo: 2da. Línea Defensa:** Oficina Asesora de Planeación
8	Revisados los indicadores de los Procesos de Gestión Recursos de Tecnología, denominado: *"Porcentaje de equipos (PC´s y Servidores) con protección de antivirus para la vigencia 2020*." y "*Porcentaje de Mantenimientos preventivos realizados;* En relación con el primer y segundo indicador, se observó incumplimiento a los lineamientos emitidos por la Entidad - Procedimiento de Medición de la Gestión de los Procesos y Guía Metodológica para la Construcción de Indicadores de seguimiento a los procesos, generado por la ausencia de soporte de reporte de datos, para el primer indicador y para los meses de julio, agosto y septiembre de 2020, en relación con los equipos con instalación de la protección de antivirus; Igualmente, se observan diferencias de la información reportada entre el número de equipos existentes en la entidad (4273- último reporte a Derechos de Autor) con respecto a la cantidad de equipos reportados en el Directorio Activo y programados para la instalación del antivirus (3000). En cuanto al segundo indicador "*Porcentaje de Mantenimientos preventivos realizados;* Se observó que de acuerdo con las evidencias presentadas: Cronograma de actividades para los mantenimientos preventivos a realizarse en el mes de Jul/2020, que los datos de origen reportados inicialmente, difieren de los datos consignados en el reporte de datos del indicador, -soportes de consolidado y seguimiento presentado por la Mesa de Ayuda. -También se encontró que los indicadores del sistema de gestión de seguridad y privacidad de la información, aunque fueron incluidos en el formato establecido, no están siendo gestionados, toda vez que no se están haciendo los análisis cuantitativos o cualitativos de datos y no se encuentran aprobados por el Comité de Gestión y Desempeño Institucional. Estas situaciones conllevan a generar varios riesgos como son: -Dejar sin protección mensual de antivirus un total de 1.273 equipos. -No contar con los soportes del reporte realizado mensualmente, es decir no se cuenta con la trazabilidad del dato consignado en el indicador, con el fin de tener un conocimiento documentado del grado de avance, o el logro de los objetivos y resultados esperados, a fin de tomar decisiones oportunas.	NC	Se recomienda aprovechar la información generada en el proceso de seguimiento y evaluación (trazabilidad) para responder ante requerimientos externos y / o toma de decisiones; máxime si se tiene en cuenta la actual situación de pandemia, donde puede ocurrir que no se visualicen los equipos que llevan días sin encenderse, o que fueron llevados a casa de los funcionarios. Así mismo, es necesario realizar la verificación a los datos consignados como base, con el fin de contar con datos reales para la toma de decisiones. Ejecutar acciones de mejora y transformación a partir de los resultados obtenidos. Así mismo, se recomienda revisar y tener como referente, en uso de las buenas prácticas, indicadores utilizados por otras entidades líderes de políticas y órganos de control para medir el desempeño de la entidad. De esta manera, se podrá aprovechar la información generada en el proceso de seguimiento y evaluación para responder a requerimientos externos.	**Lidera:** 1**ra. Línea de Defensa:** Oficina Tecnologías de la Información. **Apoyo: 2da. Línea Defensa:** Oficina Asesora de Planeación
9	Se encontró que el catálogo de Componentes de la Información y el de Sistemas de Información, no cuentan con fechas de las actualizaciones realizadas o control de versiones, que permita determinar su estado de actualización. Para el de componentes de información se encontró desactualización respecto a la totalidad de los componentes de información	NC	Identificar los componentes de información que posee la entidad y sus características con el fin de proyectar la totalidad de los servicios de información, identificar fuentes	**Lidera:** 1**ra. Línea de Defensa:** Oficina Tecnologías de la Información. **Apoyo: 2da. Línea**

	existentes en la entidad, toda vez que no se están relacionando los diferentes servicios que presta la Superintendencia. Por lo anterior, se establece un posible incumplimiento a lo señalado en la Guía de Mintic - G.INF.07- cómo construir el Catálogo de Componentes de Información, numeral 3.1, -Cuál es la información que se debe identificar para construir al catálogo; "*a. Identificar y reunir las fuentes de información: b. Identificar* ***a partir de las funciones y obligaciones legales de la entidad*** *que información debe producir.* *c. Realizar la* ***validación de la información identificada con todas las áreas****, con el fin de identificar información faltante."* En el Catálogo de los Sistemas de Información se observaron casillas sin diligenciar: "Sistema", la "ubicación de la documentación técnica", "la categoría", "el tipo", el "proveedor", el "licenciamiento", el "tipo de desarrollo", "vencimiento de la licencia", la "plataforma de aplicaciones", la "ubicación del servidor de aplicaciones", "lenguaje de programación", la "plataforma de base de datos", "ubicación del servidor de base de datos", entre otros. y faltan atributos como versión del sistema, tipo de desarrollo, fecha de vencimiento del soporte, sistema operativo; situación que incumple los lineamientos de la guía G.SIS.03, donde se describen los atributos para la construcción del catálogo de sistemas de información, así como el lineamiento LI.SIS.02- MINTIC – Catálogo de sistemas de información, que establece: "*es un instrumento base sobre el cual se inicia la documentación de una arquitectura de sistemas de información*".		únicas de información, oportunidades de mejora en seguridad y calidad de los datos e información, identificar datos maestros, datos abiertos, definir controles y mejorar el nivel de acceso a la información y demás actividades propias de la gestión de información, tal como lo señala la Guía G.INF.07- cómo construir el Catálogo de Componentes de Información.	**Defensa:** Oficina Asesora de Planeación
10	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.	NC	Se recomienda dar cumplimiento a la mencionada guía, contando con un plan de contingencia para mantener o recuperar las operaciones, asegurar la disponibilidad de la información en el grado y la escala del tiempo requerido por la Entidad, teniendo presente las siguientes características, dentro del plan: a) Una estructura organizacional adecuada para prepararse, mitigar y responder a un evento contingente, usando personal con la autoridad, experiencia y competencia necesarias. b) Personal formalmente asignado de respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para manejar un incidente y mantener la seguridad de la información. c) Planes aprobados, procedimientos de respuesta y recuperación documentados, en los que se especifique en detalle como la organización gestionará un evento contingente y mantendrá su seguridad de la información en un límite predeterminado, con base en los objetivos de continuidad de seguridad de la información aprobados por la Dirección.	**Lidera:** 1**ra. Línea de Defensa:** Oficina Tecnologías de la Información.
11	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.supernotariado.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, 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	NC	Se recomienda contar con un plan de acción y cronograma documentado para aquellos aplicativos que no soportan el protocolo IPv6. Tener presente los planes de capacitación para los diferentes funcionarios, y contar con los soportes documentales y en firme, para cada una de las fases (Planeación- plan de diagnóstico - Plan detallado del proceso de transición - Plan de direccionamiento IPv6 - Plan de contingencias para IPv6; Implementación - Documento de diseño detallado de la implementación de IPv6- Informe de activación de políticas de seguridad	**Lidera:** 1**ra. Línea de Defensa:** Oficina Tecnologías de la Información.

	para Colombia.-numeral 7.1 Fase I. Planeación de IPv6.		en IPv6; Pruebas de funcionalidad - Documento de pruebas de funcionalidad en IPv6 - Acta de cumplimiento a satisfacción de la entidad sobre el funcionamiento de los elementos - intervenidos en la fase de implementación; y adopción del protocolo), de acuerdo a la Guía de Transición de IPv4 a IPv6 para Colombia.	
12	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.	NC	Procurar formalizar convenios orientados a garantizar el cumplimiento del objetivo trazado en el Decreto 1008 de 2018 "*Por el cual se establecen los lineamientos generales de la política de Gobierno Digital*" en su Artículo 2.2.9.1.2.2. "*Manual de Gobierno Digital*, en el marco de interoperabilidad que señala el deber de apoyar a las entidades públicas en sus esfuerzos por diseñar y ofrecer trámites y servicios en línea a otras entidades púbicas, ciudadanos y empresas que son digitales por defecto Se recomienda ademàs, dejar soportado con la documentación pertinente, cada una de las fases que sean gestionadas (Actas de reunión, Actas de aprobación, pruebas desarrolladas, etc), por cuanto las situaciones descritas en el informe denotan la necesidad de contar con registros documentales que soporten las decisiones tomadas de cada una de las actividades programadas, así como lo contemplado en cada una de las fases establecidas, dejando la trazabilidad de la ejecución de interoperabilidad.	**Lidera:** 1**ra. Línea de Defensa:** Oficina Tecnologías de la Información.
13	Se evidenció que de acuerdo con el formato de matriz de riesgos del Macroproceso de Tecnologías de la Información, en la redacción de los controles se obtuvo una calificación de 35 puntos, encontrándose en un rango entre 0 y 85; lo que significa conforme a la -Guía de Administración de Riesgos vigente, que la solidez del conjunto de controles en los procesos adscritos al mismo, es débil, y la ejecución del control no es suficiente para evitar la materialización de los riesgos. Con respecto a los soportes documentales de ejecución de controles existentes en la One Drive, se evidenció que estos se encontraron incompletos. Con respecto a los riesgos de seguridad y privacidad de la información, se encontró que no se está utilizando la metodología para la identificación, tratamiento, valoración de los riesgos identificados, por lo que no se están gestionando; no han sido caracterizados los riesgos cibernéticos, no se han identificado los supuestos, ni se ha logrado analizar el impacto que podría ocasionarse en caso de tener afectaciones de este tipo. También se evidencia que no han sido aprobados por el Comité de Gestión y Desempeño Institucional, incumpliendo lo establecido en la *Política General para la Administración de Riesgos y Oportunidades Código: DE - SOGI - POL - 01 Versión: 03 Fecha: 24 de abril del 2020. Guía para la identificación de riesgos, oportunidades, evaluación del diseño y efectividad de controles Código: DE - SOGI – PR – 07 -GI - 01 Versión: 03 Fecha: 06 de febrero de 2020. Así como* 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 para la implementación de la Política de Gobierno Digital, las entidades públicas deberán aplicar el Manual de Gobierno Digital que define los lineamientos,	NC	Establecer controles sólidos para fortalecer la ejecución de estos, evitando la materialización de los riesgos identificados. Se recomienda seleccionar actividades de control preventivas que por sí solas ayuden a la mitigación de las causas que puedan originar los riesgos. Gestionar los riesgos de Seguridad y Privacidad de la Información conforme a la metodología implementada por la entidad. De igual manera, se considera indispensable y oportuno recomendar fortalecer la identificación de los riesgos y diseño de los controles del Macroproceso de Tecnologías de la Información, tomando en cuenta, las advertencias identificadas en el desarrollo de esta auditoría y las oportunidades de mejora que se han recomendado por parte del Equipo Auditor, a fin de	**Lidera:** 1**ra. Línea de Defensa:** Oficina Tecnologías de la Información.

	estándares y acciones a ejecutar por parte de los sujetos obligados de esta Política de Gobierno Digital", y en el Lineamiento LI: ST.14- MINTIC –"…*debe realizar el análisis y gestión de los riegos asociados a su infraestructura tecnológica haciendo énfasis en aquellos que puedan comprometer la seguridad de la información o que puedan afectar la prestación de un servicio de TI.*"		prevenir, mitigar y evitar la materialización de situaciones críticas o desviaciones que pongan en riesgo el cumplimiento del objetivo de sus procesos.	
14	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.	OBS	Se recomienda realizar los convenios a que haya lugar, con el fin de documentar la cooperación y compromiso por parte de las entidades.	**Lidera:** 1r**a. Línea de Defensa:** Oficina Tecnologías de la Información.
15	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*."	OBS	Se recomienda avanzar con las gestiones necesarias a fin de documentar e implementar el conjunto de controles y procedimientos para alcanzar un correcto nivel de seguridad en el manejo, transformación y operación de la información y de igual forma administrar estos controles para mantener este nivel a lo largo del tiempo, el cual ayudará a centrar los esfuerzos y recursos en la mitigación de los riesgos que sean identificados como de mayor impacto y/o probabilidad conforme al análisis y evaluación de éstos y para dar cumplimiento a los lineamientos establecidos a través del CONPES 3854 POLÍTICA NACIONAL DE SEGURIDAD DIGITAL", en lo relacionado con la gestión del riesgo de seguridad digital.	**Lidera:** 1r**a. Línea de Defensa:** Oficina Tecnologías de la Información.
16	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 Critico*" 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, 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.	NC	Se recomienda establecer un plan de trabajo para determinar las acciones tendientes a solucionar o corregir las vulnerabilidades presentadas y que a la fecha se encuentran sin un tratamiento efectivo de mitigación, de acuerdo con el comportamiento de las amenazas registradas mes a mes, practicas orientadas a garantizar la seguridad, la integridad y la confidencialidad de los datos de la entidad.	**Lidera:** 1r**a. Línea de Defensa:** Oficina Tecnologías de la Información.
17	Revisados los Planes de Mejoramiento suscritos con la CGR y el Institucional se encontró que, para los hallazgos tomados en la muestra y descritos en el numeral 7 del presente informe, se encuentran vencidas e incumplidas las acciones propuestas, a la fecha de la auditoria. Esta situación genera incumplimiento a lo establecido en el Modelo Integral de Planeación y Gestión –MIPG, establecido mediante Decreto 1499/2017, en su 7ª. Dimensión: Evaluación de Resultados, Actividades de Monitoreo, y respecto al numeral -7.2.1 Diseñar y mantener de manera adecuada y efectiva el MECI, desarrollando las siguientes actividades: Cuarto componente: -Implementar las actividades de monitoreo y supervisión continua en el proceso que lidera, a fin de asegurar o garantizar el cumplimiento de los objetivos trazados en los mismos: … "- La evaluación continua o autoevaluación lleva a cabo el monitoreo a la operación de la entidad a través de la medición de los resultados generados en cada proceso, procedimiento, proyecto, plan y/o	NC	–Verificar el desarrollo y cumplimiento de sus acciones, que contribuyan al cumplimiento de los objetivos institucionales, de tal forma que se convierte, entonces, la autoevaluación en el mecanismo de verificación y evaluación, que le permita a la entidad medirse a sí misma, al proveer la información necesaria para establecer si ésta funciona efectivamente o si existen desviaciones en su operación, que afecten su propósito fundamental. – La autoevaluación se convierte en	**Lidera:** 1r**a. Línea de Defensa:** Oficina Tecnologías de la Información.

	programa, teniendo en cuenta los indicadores de gestión, el manejo de los riesgos, **los planes de mejoramiento**, entre otros. De esta manera, se evalúa su diseño y operación en un período de tiempo determinado, por medio de la medición y el análisis de los indicadores, cuyo propósito fundamental será tomar las decisiones relacionadas con la corrección o el mejoramiento del desempeño.		un proceso periódico, en el cual participan los servidores que dirigen y ejecutan los procesos, programas y/o proyectos, según el grado de responsabilidad y autoridad para su operación. Toma como base los criterios de evaluación incluidos en la definición de cada uno de los elementos del control interno, así como la existencia de controles que se dan en forma espontánea en la ejecución de las operaciones y en la toma de decisiones."	

No Conformidad (NC): Incumplimiento de una norma o requisito.
Observación (OBS): Situación identificada, que puede dar lugar al incumplimiento de una norma o a la materialización de un riesgo.

10. RESPUESTA Y ARGUMENTACIÓN A LAS OBSERVACIONES PRESENTADAS POR LA OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN: Mediante correo electrónico de fecha 22 de Enero de 2021, la Oficina de Tecnologías de la Información envió respuesta sobre los hallazgos evidenciados, encontrando que para algunos casos, fueron enviados los soportes que avalan las acciones adelantadas, tendientes a subsanar las causas que los originaron; en otros casos han manifestado que se requiere del apoyo de otras dependencias para subsanarlos; por lo tanto se evidencia la voluntad y disposición de los funcionarios para corregir o dar cumplimiento a la normatividad vigente; sin embargo, dado que las evidencias aportadas no subsanan las causas generadoras de los hallazgos, y teniendo en cuenta que la auditoría se plantea con un enfoque basado en procesos, donde es necesario ir más allá de las gestiones que se puedan realizar por la Oficina de Tecnologías, se requiere que el análisis de causa raíz, sea realizado de manera integral y coordinado con los diferentes responsables, identificando las acciones que sean necesarias para eliminarlas, en aras de optimizar los procedimientos de la Superintendencia, buscando ser más eficientes a Nivel Nacional.

Por lo anterior, estas situaciones se han reiterado, plasmándolas como observación y/o No Conformidad en la misma Matriz de Resultados del Seguimiento, dado el riesgo y/o incumplimiento a la normatividad vigente.
A continuación, se relaciona la situación final para cada hallazgo, luego del análisis efectuado a las evidencias aportadas para cada uno de ellos:

➢ **Hallazgos No. 2** (responsable Gestión Administrativa), **3, 5, 6, 7, 8, 9, 10, 11, 12, 13, 16, y 17:** Para estos hallazgos no se presentaron observaciones ni evidencias que permitan desvirtuar lo encontrado en el momento de la auditoría, por lo tanto, los mismos continúan en los términos descritos en el informe preliminar. A continuación, se describe la situación final para cada hallazgo que fue objeto de argumentación:

➢ **Hallazgo No.1:-OBS:** *"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.".

Argumento Oficina de Tecnologías: "*Conforme al informe de la auditoria de control interno, frente al punto uno (desarrollos realizados por la OTI para afrontar la pandemia ocasionada por el COVID-19), se indicó en la auditoria que se desarrollaron módulos en REL y el aplicativo Gestor Documental, se adjuntaron los manuales correspondientes en su momento. Igualmente se adjuntan al presente oficio, estos son:*
• Anexo 2 Manual de Usuario Gestor Documental
• Anexo 1 Finalización REL
Frente al formato de creación de usuarios, se creó uno con la Dirección Técnica de Registro para afrontar el tema de manera inmediata; no obstante, el formato actual de creación de usuarios de OTI y el de la DTR para REL serán los que se usen en adelante. Se adjuntan al presente oficio:
• Formato creación usuarios rel- Funcionarios SNR - ORIP (2).pdf
• Formato creación usuarios REL - NOTARIAS.pdf
• Formato creación usuarios REL- Funcionarios SNR - ORIP.xlsx
• Formato creación usuarios REL - NOTARIAS.xlsx
• Formato Administración de Usuarios
Adicionalmente se adjuntan como soporte los siguientes documentos:
• Actividades de apoyo Soporte Correo Covid 19 -2020
• Paso a paso –Instalación archivos Host –InstaladorV1.
• Manual de Instalación de Acceso remoto para equipo MAC"

Respuesta OCI: Verificados los Anexos señalados en la respuesta, se encuentra que anexaron evidencias de los manuales de usuario y gestor documental - GARC, donde se explica el uso de la plataforma de gestión de acceso y preservación de archivos y documentos SNR; el manual sobre la explicación de la descripción y el funcionamiento del módulo de finalización misional y consulta de finalizaciones de la plataforma REL (Radicación electrónica); Manual de Instalación de Acceso remoto para equipo MAC; Manual Paso a Paso Instalación; sin embargo, estos no han sido codificados, ni documentados a través del Sistema de Gestión Documental -SIC de la entidad; de otra parte, no se anexaron evidencias de los manuales de administrador de los sistemas.
Con respecto a los formatos de creación de usuarios, se observa que anexan como soportes los diferentes formatos de creación de usuario, los cuales tampoco están siendo codificados por el Sistema de Gestión de la entidad. Por lo anterior, la Observación se mantiene y se recomienda la estandarización de los formatos de creación de usuarios, toda vez que la Dirección Técnica de Registro está manejando formatos diferentes a la Oficina de Tecnologías de la Información.

➢ **Hallazgo No.4 - NC y 15 - OBS:** *""…Con estos documentos, se observa que la Oficina de Tecnologías de la Información pretende fortalecer las capacidades de respuesta de la entidad, ante un posible evento de riesgo que pueda ocurrir a los activos de información, de acuerdo con los lineamientos definidos por el Gobierno Nacional; sin embargo, se observó que estos documentos fueron presentados por la Empresa Alina Tech S.A.S, en la vigencia 2019 y a la fecha de la auditoría, no han sido gestionados en su actualización, aprobación y difusión para su aplicación al interior de la entidad."*

Argumento Oficina de Tecnologías: "*Es por esto, que la OTI informa que Sí se actualizó y ajustó según los lineamientos de la oficina de planeación, la "Política General y políticas específicas del Sistema de Seguridad de la Información" siendo este archivo enviado como evidencia el día 11 y el 26 de noviembre del 2020 al grupo auditor, así mismo se envió a la oficina de Planeación el formato de creación, modificación, para la aprobación, incluidas las firmas correspondientes:*

RV: Aprobación política general y políticas especificas SGSI

Responder | Responder a todos | Reenviar

Luis Emilio Romero Mogollon
Para Ceidy Ortiz Espitia; Juan Carlos Torres Rodriguez; Hadder Leonardo Aguirre Hernandez; Ariel Leonel Melo
CC Wilson Barrios Delgado; Yaneth Constanza Rincon Pulido; Sandra Rocio Castro Cruz; Dario David Peña Acuña; Proyecto de Seguridad SGSI SNR
mar 15/12/2020 01:12 p.m.

Haga clic aquí para descargar imágenes. Para ayudarle a proteger su confidencialidad, Outlook ha impedido la descarga automática de algunas imágenes en este mensaje.

Formato CREACION MODIFICACION PoliSGSI.pdf
330 KB

Buen dia,
Envío formato firmado por parte de la OTI.

Agradezo la gestión y atención a la presente comunicación.

Luis Emilio Romero Mogollón
Coordinador Grupo de Sistemas de Información

Superintendencia de Notariado y Registro
Calle 26 No 13-49 int. 201
Bogotá, Colombia

Fuente: Correo Electrónico SNR

Por tal motivo se solicita el favor que en lo posible se pueda unificar las observaciones 4 y 15 dejando también como responsables a la Oficina Asesora de Planeación, ya que se requiere del acompañamiento de ellos, para la aprobación final y su asesoría en cuanto a la elaboración de estos documentos o planes estratégicos mencionados en las presentes observaciones y finalmente diligenciar el plan de acciones de mejora."

Respuesta OCI: Verificados los argumentos enviados por la Oficina de Tecnologías de la Información, se encuentra que no es posible unificar los hallazgos, toda vez que en el No.4 se trata de una No Conformidad por el hecho de no contar con los Planes mencionados, debidamente aprobados por los responsables de los mismos (Comité); mientras que en el No.15 se trata del ajuste, aprobación y socialización de los diferentes 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,) los cuales para algunos casos deben ser ajustados por parte de la primera línea de defensa; y para la construcción de las acciones a suscribir en el Plan de Mejoramiento, pueden involucrar a los diferentes responsables como el caso de la Oficina Asesora de Planeación, y Divulgación, en las actividades que respecta a cada uno, a través de un trabajo colaborativo y por procesos.

- **Hallazgo No.14 - OBS:** *"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."*

Argumento Oficina de Tecnologías: "*La presente observación que hace referencia a que se soporte por medio de convenios, es necesario informar que para obtener contacto como es el caso con el CSIRT, no es necesario realizar convenios, sin embargo, se diligenciará el Formato de Suscripción de Acciones a Plan de Mejoramiento Integrado, de manera que se pueda interactuar con alguna de las entidades ya mencionadas y mitigar los riesgos de seguridad digital.*

Respuesta OCI: Verificados los argumentos enviados por la Oficina de Tecnologías de la Información se encuentra que el documento CONPES 3854 POLÍTICA NACIONAL DE SEGURIDAD DIGITAL, refiere la celebración de convenios entre entidades con el fin de que se intercambie voluntariamente información relativa a alertas, amenazas e incidentes de seguridad informática, informes o indicadores de compromiso que podrían prevenir los riesgos cibernéticos y novedades tecnológicas en el ámbito de la ciberseguridad, reportes de ciberseguridad y otros equivalentes. También se puede acordar sobre la cooperación en la prevención, detección, respuesta y recuperación de incidentes de ciberseguridad para minimizar el impacto en los servicios y operaciones o para recuperar infraestructuras críticas y servicios esenciales. Además, del resguardo -en conformidad a los estándares internacionales- en el envío de datos personales fuera del territorio colombiano. Por lo que se considera acertado que se suscriban acciones tendientes a subsanar la observación planteada. Se mantiene la Observación.

Cordialmente,

Equipo Auditor:

Luisa Barreto	*Stella Reyes*	*Hugo Alfonso*
Luisa Nayibe Barreto López	- María Stella Reyes Beltrán	- Hugo Alfonso Cepeda

Atentamente,

RITA CECILIA COTES COTES
Jefe Oficina Control Interno