INFORME DE SEGUIMIENTO A LOS SISTEMAS DE INFORMACIÓN QUE SOPORTAN EL COMPONENTE FINANCIERO, VALIDANDO LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN, DESDE LO ESTABLECIDO EN LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL SNR

OBJETIVO

Evaluar la identificación, diseño y ejecución del control de los riesgos asociados con la confidencialidad, integridad y disponibilidad de los sistemas de Información SIR y REL que contienen el componente financiero en las Oficina De Registro de Instrumentos Públicos de Manizales, Bucaramanga y Popayán, conforme a la muestra seleccionada.

ALCANCE DEL SEGUIMIENTO

Comprende la verificación de la identificación, diseño y ejecución del control de los riesgos asociados con la confidencialidad, integridad y disponibilidad de los sistemas de Información misionales SIR y REL que contienen el componente financiero de la Superintendencia de Notariado y Registro, de acuerdo con la lista de chequeo elaborada en términos del cumplimiento de los lineamientos establecidos en la entidad frente a seguridad de la información; a través del análisis de controles de seguridad implementados con corte al 25 de Noviembre del 2022, asociados a los procesos: Gestión de Tecnologías de la Información, Gestión Administrativa y Financiera, Dirección Técnica de Registro y las Oficinas de Registro de Instrumentos Públicos de Manizales, Popayán y Bucaramanga, seleccionadas en la muestra; adicionalmente, evaluar la efectividad de los planes de mejoramiento asociados al objeto auditar.

MARCO NORMATIVO

Los parámetros o criterios que se tuvieron en cuenta para el presente informe de seguimiento son:

Ley 23 de 1982 sobre Derechos de Autor.
Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 767 de 2022, "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
Decreto 2723 de 2014 - "Por el cual se modifica la estructura de la Superintendencia de Notariado y Registro"
Artículo 11. Funciones de la Superintendencia. *14. Ejercer la inspección, vigilancia y control de las Oficinas de Registro de Instrumentos Públicos, en los términos establecidos en las normas vigentes.*
Artículo 17. Funciones de la Oficina de Tecnologías de la Información*. Función de la Oficina de Tecnologías de la Información: 18. Atender, proponer e implementar las políticas y acciones relativas a la seguridad de la información y de la plataforma tecnológica de la Superintendencia.*
Guía para la Administración del Riesgo para las Entidades Públicas del Departamento Administrativo de Función Pública -DAFP.
Guía 18: Lineamientos: Terminales de áreas financieras entidades públicas. Modelo de Seguridad y Privacidad de la Información de MINTIC.

Resolución 193 de 2016, CONTADURÍA GENERAL DE LA NACIÓN, por la cual se determinan los elementos y actividades de control interno para gestionar el riesgo contable, que señala:

Numeral 3.2.3.1 Soportes documentales. – *"La totalidad de las operaciones realizadas por la entidad deberá estar respaldada en documentos idóneos, de manera que la información registrada sea susceptible de verificación y comprobación exhaustiva o aleatoria; por lo cual, no podrán registrarse contablemente los hechos económicos que no se encuentren debidamente soportados. (…) De conformidad con el desarrollo de la gestión contable por procesos y los manuales de procedimientos implementados en las entidades, se deberá hacer un análisis y evaluación de los diferentes tipos de documentos que sirven de soporte a las operaciones llevadas a cabo, así como de la forma y eficiencia de su circulación entre las dependencias, y entre la entidad y los usuarios externos, con el propósito de tomar las medidas que sean necesarias para garantizar un eficiente flujo de documentos."*

Numeral 3.2.8 Eficiencia de los sistemas de información. – *"Con independencia de la forma que utilicen las entidades para procesar la información, el diseño del sistema implementado deberá garantizar eficiencia y eficacia en el procesamiento y generación de la información financiera. Para la implementación y puesta en marcha de sistemas automatizados, las entidades observarán criterios de eficiencia en la adquisición de equipos y programas que contribuyan a satisfacer sus necesidades de información, atendiendo la naturaleza y complejidad de la entidad de que se trate; además, se deberá procurar que los sistemas implementados integren adecuadamente los principales procesos que tienen a su cargo las dependencias.".*

Resolución No. 02170 de 2022 Por la cual se actualizan las tarifas por concepto del ejercicio de la función registral.
Resolución 06387 del 3 junio del 2022. Devolución de Dinero mayores valores.
Política General y políticas específicas del Sistema de Seguridad de la Información de la SNR. - Código: MP - GNTI - PL - 01 Versión: 02 Fecha: 19/08/2021.
Norma internacional ISO / IEC 27001 - Sistema de gestión de seguridad de la información.
Procedimiento: RECAUDOS POR LA PRESTACIÓN DEL SERVICIO PÚBLICO REGISTRAL - Código: MP - GNFA- PO - 02 - PR – 02 - Versión: 01.
Procedimiento: CONCILIACIONES CONVENIOS DE RECAUDO - Código: GF - CI - PR – 02 - Versión: 01.
Manual de Políticas de Operación Proceso Estados Financieros Procedimiento Estados Financieros.

METODOLOGÍA

La Oficina de Control Interno, adelantó la verificación de la identificación, diseño y ejecución del control de los riesgos asociados con la confidencialidad, integridad y disponibilidad de los sistemas de Información misionales SIR y REL, que contienen el componente financiero de la Superintendencia de Notariado y Registro, con el fin de verificar su cumplimiento y la efectividad de sus controles.

Para realizar el presente seguimiento, se verificaron los diferentes soportes y evidencias con corte al 25 de noviembre de 2022, ejecutando las siguientes actividades:

La revisión a la documentación entregada por las Oficinas de Registro de Manizales, Popayán y Bucaramanga, de acuerdo con los ítems verificados.

Entrevistas con el sujeto objeto de seguimiento, validando la aplicación de los controles ejecutados por parte de los sujetos objeto del seguimiento, y de las dependencias que aportaron soportes, como responsables del contenido de la información suministrada.
Observación por parte del Equipo Auditor, a la aplicación de protocolos de seguridad de la información, según los roles y responsabilidades de cada usuario, respecto a la data.
Se verificaron los soportes documentales tomados de las reuniones realizadas con algunos de los responsables de operar la información de los aplicativos SIR y REL, validando tanto el cumplimiento a las políticas de seguridad de la información en los temas tecnológicos, como a la gestión técnico-administrativa adelantada por cada una de las Oficinas de Registro tomadas como muestra.
Se verificaron aspectos relacionados con la identificación, diseño y ejecución del control de los riesgos asociados con la confidencialidad, integridad y disponibilidad de los sistemas de Información misionales SIR y REL, en lo concerniente al componente financiero de la Superintendencia de Notariado y Registro.
Verificación a las actividades de control asociadas al Procedimiento: Recaudos por la Prestación del Servicio Público Registral, Código: MP-GNFA-PO-02-PR–02-Versión: 01.
La validación a la aplicación de los controles, según los riesgos identificados por las oficinas de Registro de Instrumentos Públicos de Manizales, Popayán y Bucaramanga.
La verificación a la suscripción de plan de mejoramiento producto de auditorías anteriores realizadas por la Oficina de Control Interno.
Pruebas de recorrido y de efectividad de controles físicas.

LIMITACIONES

En la realización del seguimiento, no se presentó ningún tipo de inconveniente, se contó con la colaboración y la buena disposición de los funcionarios de las oficinas de Registro de Instrumentos Públicos – Oficinas de Registro de Instrumentos Públicos, tomadas como muestra.

DESARROLLO DEL SEGUIMIENTO

De conformidad al Plan Anual de Auditoria aprobado para la vigencia 2022; en cumplimiento al Procedimiento de Informes de Ley, Seguimiento y/o Evaluación, el Equipo Auditor, llevó a cabo el ejercicio de seguimiento teniendo en cuenta lo señalado en la Política General y específicas del Sistema de Seguridad de la Información de la SNR, de conformidad con lo definido en la Guía 18: Lineamientos: Terminales de áreas financieras entidades públicas. Modelo de Seguridad y Privacidad de la Información de MINTIC. Así mismo, se tuvo en cuenta la información suministrada por la Oficina de Tecnologías de la Información, la Dirección Técnica de Registro, la Dirección Administrativa y Financiera y las oficinas de Registro de Instrumentos Públicos de Manizales, Popayán y Bucaramanga, como actores participes en la operación y soporte de los sistemas de Información SIR y REL que contienen el componente financiero.

1. **Verificación de la aplicación de la Guía 18: Lineamientos: Terminales de áreas financieras entidades públicas. Modelo de Seguridad y Privacidad de la Información de MINTIC, como control para gestionar los riesgos de confidencialidad, integridad y disponibilidad de las estaciones de trabajo desde las cuales se acceden a las cuentas bancarias que registran los recaudos con el apoyo de los sistemas de Información SIR y REL que contienen el componente financiero.**

Para la validación de los Lineamientos establecidos en la *Guía 18: Lineamientos: Terminales de áreas financieras entidades públicas. Modelo de Seguridad y Privacidad de la Información de MINTIC)*, la OCI realizó pruebas y recorridos físicos a las Oficinas de Registro de Instrumentos Públicos de Manizales, Popayán y Bucaramanga, entre los meses de octubre y noviembre del 2022; se verificó la aplicación de los lineamientos que la SNR debe implementar para elevar el aseguramiento de los equipos de cómputo tanto en su hardware como en el software, asignados por la entidad y desde los cuales se ingresa a una plataforma bancaria, para consultar y descargar los extractos bancarios de los ingresos recaudados desde los roles de contador y Coordinador Grupo Tecnológico y Administrativo.

El alcance de la presente verificación, solo aplica para las Oficinas de Registro de Instrumentos Públicos de Manizales y Bucaramanga, dado que tienen una cuenta producto y desde éstas, se accede a un portal bancario.

1.1. <u>Riesgo evaluado:</u> "Pérdida de Confidencialidad de la Información del recaudo y pérdida de integridad de las estaciones de trabajo"

En la validación realizada por la OCI al cumplimiento de los Lineamiento de seguridad lógica *(numeral 5.1 de la Guía 18: Lineamientos Terminales de áreas financieras entidades públicas, Modelo de Seguridad y Privacidad de la Información de MINTIC)*, se evidenció lo siguiente:

a) Requerir credenciales de autenticación para el ingreso y/o uso, las cuales deberán estar obligadas a cambiarse periódicamente y tener especificaciones mayores de seguridad (longitud mínima de ocho caracteres alfanúmeros y caracteres especiales) de conformidad con la tecnología y mecanismos técnicos que dispongan las instituciones financieras para este fin.

Al verificar el lineamiento anterior en la Oficina de Registro de Instrumentos Públicos de Manizales, se evidenció el cumplimiento de este criterio descrito en este literal, por cuanto se está realizando el cambio periódico de la autenticación para el ingreso a la plataforma bancaria; no obstante, se observó que la Contadora accede al portal del Banco, realizando la autenticación con el usuario (cédula coordinador) y contraseña asignada al Coordinador Grupo Tecnológico y Administrativo, con la aprobación tácita del Coordinador. Así mismo, el Contador solicita el cambio de contraseña a través del portal bancario de forma manual y/o cuando lo requiera el portal bancario; después de esta modificación exitosa, reporta al Coordinador Grupo Tecnológico y Administrativo sobre la nueva contraseña.

Con lo anterior, se estaría causando una suplantación de identidad y una inadecuada segregación de funciones, dado que la cuenta de usuario para ingresar al Banco, se encuentra asignada al Coordinador Grupo Tecnológico y Administrativo y ésta es usada por el Contador de la Oficina de Registro de

Instrumentos Públicos; situaciones asociadas al riesgo 1.1 Pérdida de Confidencialidad de la Información del recaudo. Se evidencia igualmente; en consecuencia, se está **incumpliendo** el presente lineamiento.

b) *Controlar el tiempo de inactividad del usuario a través de bloqueo automático del equipo o terminal móvil (se sugiere máximo cinco minutos). Implementar políticas en el directorio activo de la entidad o mecanismo y/o solución equivalente, que exija la autenticación y controle el tiempo de inactividad del usuario."*

En este punto, se observó que las terminales asignadas a los roles de Contador y Coordinador Grupo Tecnológico y Administrativo, no controlan el tiempo de inactividad del usuario a través del bloqueo automático del equipo o terminal móvil, tampoco se evidenció la configuración de una Política a través del directorio activo desde el Nivel Central, que permita bloquear el equipo de cómputo por inactividad; situación que puede causar acciones no autorizadas y comprometer las funciones que son desempeñadas por estos dos roles en la entidad.; Por consiguiente se observó el **incumplimiento** del presente literal.

c) *Limitar los privilegios de la(s) cuenta(s) de usuario(s) utilizada(s) para realizar transacciones financieras en los equipos y/o terminales para este fin, a efecto de reducir el riesgo de que con la misma sea posible la instalación de software malintencionado o controladores de dispositivos no autorizados. Implementar una política en el Directorio Activo o mecanismo y/o solución equivalente, que restrinja los permisos de administración local sobre el equipo o terminal móvil, de los usuarios que realicen transacciones financieras en éste.*

Se observó que el perfil del usuario con el cual se ingresa al portal bancario para la Oficina de Registro de Instrumentos Públicos de Manizales, cuenta con un perfil de solo consulta, lo cual limita los privilegios asociados a la cuenta de usuario.

Así mismo, los equipos de cómputo asignados a los roles de Contador y Coordinador Grupo Tecnológico y Administrativo, se encuentran integrados al directorio activo a fin de reducir el riesgo de pérdida de integridad de las estaciones de trabajo dada la instalación de software malintencionado o controladores de dispositivos no autorizados; por lo que **se da cumplimiento** al presente literal.

d) *Restringir en lo posible la ejecución de archivos como (.exe, .vbs, .com .scr, etc.) que no hagan parte de los sistemas necesarios para la elaboración de las actividades propias del cargo y que hayan sido descargados de sitios web o recibidos vía correo por parte del usuario del equipo por medio del cual se realizan las transacciones financieras.*

Resultado de la verificación, se observó que no es posible la ejecución de archivos como (.exe, .vbs, .com. scr, etc.), dado que tanto el directorio activo como el antivirus instalado en cada estación de trabajo realiza los bloqueos necesarios, con lo cual se minimiza el riesgo de pérdida de integridad de las estaciones de trabajo.; por lo anterior **se da cumplimiento** al presente literal.

e) Establecer procedimientos automatizados o por medio del soporte técnico que disponga la entidad, para efectuar el borrado regular de: archivos temporales del sistema operativo, archivos temporales de Internet, cookies, historial de navegación y descargas (se sugiere mínimo una vez a la semana).

De acuerdo con lo evidenciado, no se observaron procedimientos automatizados, o ejecutados por medio del soporte técnico o mesa de ayuda, para efectuar el borrado **regular** de: archivos temporales del sistema operativo, archivos temporales de Internet, cookies, historial de navegación y descargas en los equipos de cómputo asignados al Contador y al Coordinador Grupo Tecnológico y Administrativo; situación, con probabilidad de materializarse el riesgo de pérdida de integridad de las estaciones de trabajo; por lo anterior se está **incumpliendo** el presente literal.

f) Establecer los mecanismos necesarios para que la instalación, actualización o desinstalación de programas o dispositivos en el equipo o terminal móvil, sea realizada únicamente por los funcionarios del área de sistemas o tecnología, o el personal designado por la Entidad para este tipo de requerimientos, adicionalmente, estas actividades deben ser revisadas y aprobadas por el funcionario que desempeñe el rol de oficial de seguridad de la información, y/o las áreas responsables de la seguridad de la información y/o los designados por la entidad para efectuar este tipo de aprobaciones.

Se observó que en las Oficinas de Registro de Instrumentos Públicos, se encuentran establecidos controles para que la instalación, actualización o desinstalación de programas o dispositivos en los equipos de cómputo, sea realizada únicamente por el personal designando; dando **cumplimiento** al presente literal.

g) Restringir la instalación de software que permita conexión remota (TeamViewer, LogMeIn, Hamachi, VCN, entre otros) evitando con esto que personas externas se puedan conectar fácilmente al equipo o terminal desde el cual se realizan las transacciones. – Restringir el software de acceso remoto al equipo que pueda ofrecer o tener preinstalado el Sistema Operativo del respectivo equipo o terminal.

Conforme a la revisión y análisis se verificó desde algunas estaciones de trabajo de las Oficinas de Registro de Instrumentos Públicos de Manizales y Popayán que son asignadas a los roles del Contador y el Coordinador Grupo Tecnológico y Administrativo, encontrando que se encuentra restringida la instalación, más no la ejecución de software que permita conexión remota (TeamViewer, LogMeIn, Hamachi, VCN, entre otros); situación que podría originar la materialización del riesgo de pérdida de confidencialidad de la información de recaudo, de forma que personas externas a la entidad puedan conectarse a las estaciones de trabajo asociadas a los roles de Contador y Coordinador Grupo Tecnológico Financiero y realicen intrusiones no autorizadas y fuga de información. En consecuencia, con lo anteriormente descrito, se da **incumplimiento** al presente literal.

h) Asegurar que el equipo y/o terminal móvil cuente mínimo con: antivirus (con módulos de anti - keylogger, firewall personal, antispyware), software licenciado y actualizado de forma automática o supervisada. - Activar mecanismos para que el equipo o terminal pueda recibir las actualizaciones de seguridad de forma automática, cada vez que sean emitidas por el fabricante para el sistema operativo respectivo y aplicaciones.

Se observó que las estaciones de trabajo asignadas a los roles del Contador y el Coordinador Grupo Tecnológico y Administrativo, cuentan con el antivirus de la entidad; no obstante, no fue posible ejecutar el antivirus para validar si este contaba con las bases actualizadas y con los módulos: anti - keylogger, firewall personal, antispyware, dado que requería una contraseña.

Así mismo, se identificaron software no licenciados en las estaciones de trabajo; situación que podría dar origen a la materialización del riesgo de pérdida de integridad de las estaciones de trabajo causando a su vez un incumplimiento legal por parte de la entidad a las disposiciones dadas en materia de Protección de Propiedad Intelectual y Derechos de Autor de programas de software informático, sujetas de revisión y vigilancia por parte de la Dirección Nacional de Derechos de Autor, que son objeto de seguimiento y reporte de esta Oficina en cumplimiento de la Circular 017 de 2011 de la Unidad Administrativa Especial Dirección Nacional de Derecho de Autor y la Directiva Presidencial 02 de 2002.

En consecuencia, con lo anteriormente descrito, se da el **incumplimiento** al presente literal.

i) Restringir los puertos que permitan la conexión y/o acceso a dispositivos de almacenamiento extraíbles (CD, USB, SD Card, etc.).

Se evidenció que es posible el acceso y uso de los puertos que permitan la conexión y/o acceso a dispositivos de almacenamiento extraíbles (CD, USB, SD Card, etc.), situación que puede generar la materialización del riesgo de pérdida de confidencialidad de la información del recaudo por una posible fuga de información, haciendo uso de estos puertos y/o una pérdida de integridad de la estación de trabajo por una posible infección por virus o puertas traseras que puedan obtener información confidencial o monitorizar las acciones de los roles Contador y Coordinador Grupo Tecnológico Administrativo; por lo anterior se confirma el **incumplimiento** al presente literal.

j) Procurar tener instalado un solo navegador, en el que esté comprobada la adecuada compatibilidad y operación de servicios en línea de las instituciones financieras con las que tenga relación, con mejores mecanismos de seguridad posibles debidamente configurados y el cual deberá estar permanentemente actualizado a efecto de garantizar la disposición.

Se identificó la instalación de al menos dos navegadores tales como Google Chrome e Internet Explorer, así mismo se observa que no cuentan con la última actualización de la versión, en consecuencia, se generó el **incumplimiento** al presente literal.

k) En lo posible, el equipo o terminal deberá ser destinado de manera exclusiva para la realización de las transacciones financieras. Verificar que la utilización del equipo o terminal móvil sea realizada solo por el personal autorizado y para las actividades definidas.

Se observó que las estaciones de trabajo asignadas a los roles del Contador y el Coordinador Grupo Tecnológico y Administrativo son usadas para los fines dispuestos; no obstante, el dejar las sesiones abiertas y desatendidas, pueden ser usadas por otros usuarios diferentes a estos dos roles; situación que puede causar la posible materialización de pérdida de confidencialidad de la información de recaudo a

través de un acceso no autorizado a los recursos de información; dando un **incumplimiento** al presente literal.

l) En lo posible, apagar el equipo o terminal cuando no se esté utilizando, sobre todo si dispone de una conexión permanente a Internet. Habilitar opciones de hibernación y/o suspensión automática.

De conformidad con la validación del presente lineamiento, se evidenció que no existe una directriz clara con respecto a la obligación de apagar los equipos en las Oficinas de Registro de Instrumentos Públicos; no obstante, ante la validación realizada con el rol Contador de la Oficina de Registro de Instrumentos Públicos de Manizales, informó lo siguiente: "*Desde la OTI nos indicaron dejar prendidos los equipos para mantener las configuraciones de los sistemas operativas*"; consecuente con lo anterior, se evidencia el **incumplimiento** al presente literal.

Conclusión: Incumplimiento de los *Lineamientos de seguridad lógica (numeral 5.1 de la Guía 18: Lineamientos Terminales de áreas financieras entidades públicas, Modelo de Seguridad y Privacidad de la Información de MINTIC),* establecidos para mitigar el riesgo: **Pérdida de Confidencialidad de la Información del recaudo y pérdida de integridad de las estaciones de trabajo**, por cuanto se observó la posibilidad de ocurrencia de situaciones asociadas a suplantación de identidad, inadecuada segregación de funciones, instalación de software malintencionado, no licenciado o controladores de dispositivos no autorizados y conexión desde el exterior de la entidad a las estaciones de trabajo asociadas a los roles de Contador y Coordinador Grupo Tecnológico Financiero; razón por la que se hace necesario realizar seguimiento y control permanente sobre la ejecución de los controles establecidos, teniendo en cuenta los compromisos y responsabilidades adquiridas por los usuarios.

Recomendación:
Implementar la ejecución de los controles que dan cumplimiento a los lineamientos, tales como:

- Fortalecer las políticas en el directorio activo de la SNR, que exija la autenticación y controle el tiempo de inactividad del usuario, así como restricción de los permisos de administración local sobre la estación de trabajo, de los usuarios que realicen transacciones financieras en ellos.
- Establecer un procedimiento periódico en el cual se definan las actividades necesarias para que sean desarrolladas por la mesa de servicio y/o quien disponga la Oficina de Tecnología de la Información, para que las estaciones de trabajo, se mantengan depuradas de archivos innecesarios.
- Definir una lista de software base con el que debe contar cada estación de trabajo financiera, que incluya como mínimo un programa antivirus institucional, listado de parches de seguridad del sistema operativo y de los programas instalados, un único navegador y el desbloqueo de periféricos tales como unidades de CD/DVD, USB entre otros.
- Implementar un servidor de WSUS con el cuál se gestionen las vulnerabilidades de las estaciones de trabajo, con base en las mejores prácticas y estándares de seguridad informática.

En la validación realizada por la OCI al cumplimiento de los Lineamiento de seguridad física *(numeral 5.2 de la Guía 18: Lineamientos Terminales de áreas financieras entidades públicas, Modelo de Seguridad y Privacidad de la Información de MINTIC)*, se encontraron las siguientes situaciones:

a) *Restringir el acceso al área física desde donde se realizan transacciones financieras sólo para personal autorizado. Mantener el seguro de las cerraduras y/o puertas activos y disponibles para acceso solo al personal autorizado para utilizar el equipo o terminal móvil. Contar con guardas de seguridad, que registren y evalúen los ingresos al área física donde se encuentra el equipo o terminal móvil.*

Se observó que el acceso al área física desde donde se realizan transacciones financieras; no es solo para personal autorizado dada la situación presentada en la Oficina de Registro de Instrumentos Públicos de Manizales, donde la puerta permanece abierta y el acceso no es custodiado por un guarda de seguridad. No obstante, no se observó que se registraran los ingresos a las áreas físicas donde se encuentran las estaciones de trabajo en mención; situaciones que pueden generar la materialización del riesgo de pérdida de confidencialidad de la información de recaudo por un acceso físico no autorizado y/o robo de información; en consecuencia, se evidenció el **incumplimiento** al presente literal.

b) *En lo posible, contar con cámaras de video, las cuales deben cubrir al menos el acceso principal al área y el funcionario que utilice el equipo o* terminal móvil.

Conforme a la inspección visual, se observó que las Oficinas de Registro de Instrumentos Públicos cuentan con cámaras de video administradas por el Nivel Central; sin embargo, no están ubicadas de tal forma que se pueda cubrir al menos el acceso principal al área y el funcionario que utilice la estación de trabajo; en consecuencia, se materializa el **incumplimiento** al lineamiento.

Conclusión: Incumplimiento de los *Lineamientos de seguridad física (numeral 5.2 de la Guía 18: Lineamientos Terminales de áreas financieras entidades públicas, Modelo de Seguridad y Privacidad de la Información de MINTIC),* establecidos para mitigar el riesgo: **Pérdida de Confidencialidad de la Información del recaudo y pérdida de integridad de las estaciones de trabajo**, por cuanto se observó la probabilidad de ocurrencia de situaciones asociadas con el acceso físico no autorizado y/o robo de información por personas no autorizadas, así como la ausencia de cámaras de video que cubran al menos el acceso principal al área y el funcionario que utiliza la estación de trabajo asociadas a los roles de Contador y Coordinador Grupo Tecnológico Financiero; razón por la que se hace necesario implementar controles compensatorios de acuerdo con las limitaciones locativas existentes en la Oficina de Registro de Instrumentos Públicos.

Recomendación:
Realizar un análisis de riesgos para identificar posibles causas y limitaciones encontradas y establecer posibles controles para minimizar la materialización de los riesgos identificados.

- En la validación realizada por la OCI al cumplimiento de los Lineamiento de seguridad de la red *(numeral 5.3 de la Guía 18: Lineamientos Terminales de áreas financieras entidades públicas, Modelo de Seguridad y Privacidad de la Información de MINTIC)*, se encontraron las siguientes situaciones:

a) *Restringir el acceso a correos personales, redes sociales, y en general a otros sitios no asociados con las funciones del operador, desde el equipo y/o terminal.*

Conforme a la verificación realizada; se observó que desde las estaciones de trabajo asignadas a los roles del Contador y el Coordinador Grupo Tecnológico y Administrativo, se puede acceder a redes sociales y correos electrónicos personales; situación que puede materializar el riesgo de pérdida de confidencialidad de la información del recaudo, dada la posibilidad de fuga de información. En consecuencia, se evidenció el **incumplimiento** del presente lineamiento.

b) *Implementar mecanismos de autenticación que permitan confirmar que el equipo o terminal móvil es un dispositivo autorizado dentro de la red de la entidad.*

Se evidenció que las estaciones de trabajo asignadas a los roles del Contador y el Coordinador Grupo Tecnológico y Administrativo, hacen uso de mecanismos de autenticación para confirmar que el equipo es un dispositivo autorizado a través de la adición de este al directorio activo de la entidad; consecuentemente con lo anterior, se da **cumplimiento** a este lineamiento.

Conclusión: Incumplimiento de los *Lineamientos de seguridad de la red (numeral 5.3 de la Guía 18: Lineamientos Terminales de áreas financieras entidades públicas, Modelo de Seguridad y Privacidad de la Información de MINTIC),* establecidos para mitigar el riesgo: **Pérdida de Confidencialidad de la Información del recaudo y pérdida de integridad de las estaciones de trabajo**, por cuanto se observó la posibilidad de acceso a correos personales, redes sociales, y en general a otros sitios no asociados con las funciones asignadas a los roles de Contador y Coordinador Grupo Tecnológico Financiero; razón por la que se hace necesario fortalecer desde la Oficina de Tecnologías de la Información del Nivel Central, la implantación de controles de seguridad informática en las Oficinas de Registro de Instrumentos Públicos.

Recomendación:
Implementar la ejecución de los controles que dan cumplimiento a los lineamientos, tales como:

- Verificar y extender la aplicación de la política para filtrado de contenido o servidor proxy establecida desde la Oficina de Tecnologías de la Información, con el fin de restringir el acceso a contenidos y portales de internet no autorizados.
- Definir un listado de estaciones de trabajo las cuáles serán las únicas autorizadas para la ingresar a los portales bancarios.

En la validación realizada por la OCIG, al cumplimiento de los Lineamiento de seguridad frente a la entidad financiera *(numeral 5.4 de la Guía 18: Lineamientos Terminales de áreas financieras entidades públicas, Modelo de Seguridad y Privacidad de la Información de MINTIC)*, se encontraron las siguientes situaciones:

a) *Asignar una dirección IP fija pública al equipo o terminal móvil, la cual debe ser informada a la(s) entidad(es) financiera(s), de forma que solo esta dirección IP fija sea la utilizada para realizar transacciones en los portales empresariales.*

Conforme a la revisión efectuada, se evidenció que en ninguna de las Oficinas de Registro de Instrumentos Públicos, se asignó una dirección IP fija pública a las estaciones de trabajo asignadas a los roles del contador y el Coordinador Grupo Tecnológico y Administrativo, lo cual **incumple** el literal.

b) Garantizar la protección de las claves y dispositivos de acceso al equipo o terminal móvil y al portal empresarial de la entidad financiera. En desarrollo de esta obligación, las entidades deberán evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en el equipo y/o terminal móvil de la entidad deberá ser única y personalizada. Emitir una política con el fin de asegurar la custodia de este tipo de claves y dispositivos de acceso a los sistemas de información. Crear usuarios personalizados en los sistemas de información que permitan identificar la trazabilidad de lo realizado por los funcionarios que utilizan el equipo o terminal móvil.

Se observó que en la entidad; se presenta el uso de claves compartidas, así como la no creación de usuarios personalizados en los sistemas de información que permitan identificar la trazabilidad de lo realizado por los funcionarios; situación que puede materializar el riesgo de pérdida de confidencialidad de la información de recaudo; en consecuencia, se presenta un **incumplimiento** al literal.

c) Utilizar las medidas de autenticación y control que le ofrecen la(s) entidad(es) financieras a través de la(s) cuales realizan transacciones.

Se observó que desde la Oficina de Registro de Instrumentos Públicos, se autentican en portal bancario solo con una cuenta de usuario con perfil de consulta, lo cual genera **cumplimiento** al presente literal.

Conclusión: Incumplimiento de los *Lineamientos de seguridad frente a la entidad financiera (numeral 5.4 de la Guía 18: Lineamientos Terminales de áreas financieras entidades públicas, Modelo de Seguridad y Privacidad de la Información de MINTIC),* establecidos para mitigar el riesgo: **Pérdida de Confidencialidad de la Información del recaudo y pérdida de integridad de las estaciones de trabajo**, por cuanto se observó la situación de préstamo de claves y posibilidad de negación de acciones que puede ocurrir por los usuarios que operan las estaciones de trabajo asignadas al contador y Coordinador Grupo Tecnológico y Administrativo; razón por la que se hace necesario gestionar la implantación de controles que preserven la propiedad de no repudio en la entidad.

Recomendación:
Implementar la ejecución de los controles que dan cumplimiento a los lineamientos, como:

- Emitir una directriz desde la alta gerencia, con el fin de fortalecer la custodia de claves y dispositivos de acceso a los sistemas de información.
- Crear usuarios personalizados en los sistemas de información que permitan identificar la trazabilidad de lo realizado por los usuarios que cuentan con un rol de contador y Coordinador Grupo Tecnológico y Administrativo.

En la validación realizada por la OCG,I al cumplimiento de los Lineamiento de *seguimiento y monitoreo de controles (numeral 5.5 de la Guía 18: Lineamientos Terminales de áreas financieras entidades públicas, Modelo de Seguridad y Privacidad de la Información de MINTIC)*, se encontraron las siguientes situaciones:

a) *Llevar un adecuado control de los usuarios y perfiles del equipo. Estos deben ser personalizados y de uso restringido al funcionario asignado (debe prohibirse el uso de usuarios y claves por parte de personas diferentes a la que asignaron).*

Conforme a la verificación realizada, se observó que no se lleva un adecuado control de los usuarios y perfiles del equipo. Si bien es cierto; éstos son personalizados, no son de uso restringido al funcionario asignado, dado que se presenta la situación de préstamo de los mismos; en consecuencia, se **incumple** este literal.

b) *Asegurar que las personas que realizan transacciones financieras con los recursos de la entidad cuentan con capacitación en relación con la seguridad de la información y de las medidas que debe adoptar para mitigar los riesgos de fraude financiero.*

Se evidenció que las personas que realizan transacciones financieras con los recursos de la entidad, cuentan con capacitación en relación con la seguridad de la información; lo que denota **cumplimiento** de este literal; no obstante, y pese a que la Oficina de Tecnologías de la Información, ha realizado la divulgación de las políticas de seguridad de la Información, se observaron comportamientos inseguros.

Conclusión: Incumplimiento de los *Lineamientos de seguridad de seguimiento y monitoreo de controles (numeral 5.5 de la Guía 18: Lineamientos Terminales de áreas financieras entidades públicas, Modelo de Seguridad y Privacidad de la Información de MINTIC),* establecidos para mitigar el riesgo: **Pérdida de Confidencialidad de la Información del recaudo y pérdida de integridad de las estaciones de trabajo**, por cuanto se observó la probabilidad de ocurrencia de situaciones asociadas a la ejecución de inadecuados controles para proteger los usuarios y perfiles; razón por la que se hace necesario continuar con la ejecución de actividades de sensibilización para generar una cultura de seguridad y fortalecer las actividades de seguimiento y control permanente sobre la ejecución de los controles implementados, alineado con los compromisos y responsabilidades adquiridas por los usuarios.

Recomendación:
Implementar la ejecución de los controles que dan cumplimiento a los lineamientos, tales como:

- Llevar un adecuado control de los usuarios y perfiles que trabajan en las estaciones de trabajo financieras. (debe prohibirse el uso de usuarios y claves por parte de personas diferentes a la que asignaron).
- Capacitar sobre la seguridad de la información y las medidas que deben adoptar los roles de Contador y Coordinador del Grupo Tecnológico y Financiero, para mitigar los riesgos de fraude financiero.

2. Validación de los controles establecidos en la Política General y políticas específicas del Sistema de Seguridad de la Información de la SNR. - Código: MP - GNTI - PL - 01 Versión: 02 Fecha: 19/08/2021, que salvaguardan la seguridad de la información operada por los sistemas de Información SIR y REL que contienen el componente financiero.

Conforme a lo establecido en la Política General y Políticas Específicas del Sistema de Seguridad de la Información de la SNR: “Todos los usuarios de los sistemas de información y telecomunicaciones de la

Superintendencia de Notariado y Registro, tienen la responsabilidad y obligación de cumplir con la Política General y Políticas Específicas, normas, procedimientos y buenas prácticas de seguridad de la información", se identificaron y verificaron las políticas más relevantes que dictan controles para salvaguardar los sistemas de información misional SIR y REL que contienen el componente financiero.

2.1. <u>Riesgo evaluado</u>: "Afectación de la integridad, disponibilidad y/o confidencialidad de la información financiera gestionada con los Sistemas de Información misionales SIR y REL en cumplimiento de la Política General y políticas específicas del Sistema de Seguridad de la Información de la SNR."

En el marco de la verificación realizada por la OCIG a las: "*Políticas de uso de estaciones cliente", "Política de controles criptográficos", "Política de manejo, disposición de información, medios y equipos" y "Política de escritorio y pantalla limpia", incluidas en el documento*: *Política General y políticas específicas del Sistema de Seguridad de la Información de la SNR*, (CAPITULO II. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN), se observaron las siguientes situaciones:

a) *<u>Políticas de uso de estaciones cliente</u> - Los usuarios no podrán realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo.*

Conforme con la verificación ejecutada, se evidencia que los usuarios pueden realizar cambios en las estaciones de trabajo cuando éstas no están integradas al directorio activo; situación que puede materializar el riesgo de afectación de la confidencialidad de la información financiera gestionada con los Sistemas de Información misionales SIR y REL en cumplimiento de la Política de uso de estaciones de cliente a causa una modificación no autorizada sobre las configuraciones e instalaciones de los equipos de cómputo de la entidad; en consecuencia se presenta un **<u>incumplimiento</u>** del presente literal.

b) *<u>Políticas de uso de estaciones cliente</u> - La información almacenada en los equipos de cómputo de la Superintendencia de Notariado y Registro es de su propiedad y cada usuario es responsable por proteger su integridad, confidencialidad y disponibilidad.*

Se evidenció que los usuarios no asumen la responsabilidad por la información almacenada en los equipos frente a la protección de la integridad, confidencialidad y disponibilidad de la información al presentarse comportamientos inseguros como: el dejar las sesiones abiertas en las estaciones de trabajo cuando se apartan de éstas; situación que puede materializar el riesgo de afectación de la confidencialidad, integridad y disponibilidad de la información a causa un error en el uso en el uso de la información o un entrenamiento insuficiente en seguridad, en consecuencia se observó un **<u>incumplimiento</u>** de este literal.

c) *<u>Política de controles criptográficos</u> - Toda información que se extraiga de los aplicativos misionales debe estar cifrada para evitar que la misma pierda su confidencialidad.*

Conforme a lo evidenciado en las Oficina de Registro de Instrumentos Públicos, se observa **<u>incumplimiento</u>** de este literal, toda vez que al generar los reportes del Sistema misional SIR y REL, no se presenta algún

tipo de cifrado; situación que denota la posible materialización del riesgo de afectación de la confidencialidad de la información de los sistemas misionales SIR y REL.

d) *Política de manejo, disposición de información, medios y equipos - La Superintendencia de Notariado y Registro establece directrices para evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada en los medios proporcionados, velando por la disponibilidad y confidencialidad de la información.*

Conforme a la revisión ejecutada, se observó la ausencia de directrices para evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada; situación que causa una probabilidad de materialización del riesgo de afectación de la confidencialidad de la información financiera gestionada con los Sistemas de Información misionales SIR y REL, dado que no se cuenta con un mecanismo de control efectivo con el cual la entidad evite la divulgación de información al momento de dar de baja los equipos. (Destrucción, borrado seguro, incineración entre otros); por consiguiente, se da un **incumplimiento** al presente literal.

e) *Política de manejo, disposición de información, medios y equipos - Los medios y equipos donde se almacena procesan o comunica la información deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos cada vez que se requiera, para lo cual se le avisará al usuario sobre la realización de estas actividades con anterioridad.*

Conforme a la revisión efectuada, se observaron algunas situaciones que bridan protección física y lógicas para los medios y equipos donde se almacena procesa o comunica la información de la entidad, tales como barreras físicas, guardas de seguridad, video vigilancia, controles de acceso de forma inefectiva; como es el caso de la falta de contingencias de fluido eléctrico de la Oficina de Registro de Instrumentos Públicos de Popayán, dado que la planta eléctrica, la UPS y el tablero de transferencia presentan fallas sin solución; lo cual puede generar la materialización del riesgo de afectación de la disponibilidad e integridad de la información financiera, gestionada con los Sistemas de Información misionales SIR y REL ante la inoportunidad de mantenimiento y/o ausencia del mismo en los medios donde se almacena o procesa la información, lo que denota un **incumplimiento** al literal.

Así mismo se evidenciaron situaciones inadecuadas que son fuentes generadoras de riesgo, en donde se puede presentar una posible afectación de vidas humanas, por las fallas presentadas por el tablero de transferencia y su desacierto en su ubicación (Se encuentra ubicado a menos de un metro de la atención de los ciudadanos en la Oficina de Registro de Instrumentos Públicos de Popayán).

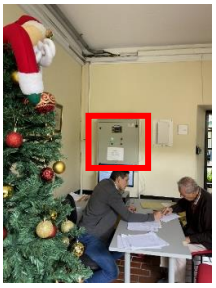

Ilustración 1: Tablero de Transferencia ORIP de Popayán.

f) *Política de escritorio y pantalla limpia - Los funcionarios, servidores públicos, contratistas, personas en comisión, pasantes y terceros que tienen algún vínculo con la Superintendencia de Notariado y Registro, deben conservar su escritorio libre de información, propia de la entidad que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.*

Al validar las estaciones de trabajo en las Oficinas de Registro de Instrumentos Públicos, se observó que el escritorio no permanece libre de información; dado que existen puestos de trabajo con exceso de documentos, así mismo, se observó que en el área de cajeros y correspondencia, se encuentra un gran volumen de documentos sin organizar; situación que puede materializar el riesgo el riesgo de afectación de la disponibilidad, confidencialidad y/o integridad de la información financiera gestionada con los Sistemas de Información misionales SIR y REL; lo que denota un **incumplimiento** del presente literal.

g) *Política de escritorio y pantalla limpia - Los usuarios de la entidad deben bloquear la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo y cerrar las aplicaciones y servicios de red cuando ya no los necesiten.*

Se evidencio que la mayoría de los usuarios, no bloquean la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo se deje desatendido el puesto de trabajo, por consiguiente, tampoco se cierra sesión en los sistemas de información, como es el caso del Sistema Misional SIR, REL y el portal de recaudo WOMPI; situación que podría generar la materialización del riesgo de afectación de la confidencialidad, disponibilidad y/o integridad de la información financiera gestionada con los Sistemas de Información misionales SIR y REL; en consecuencia se presenta un **incumplimiento** al lineamiento de política.

h) *Política de escritorio y pantalla limpia - Al imprimir documentos con información pública reservada y/o pública clasificada (semiprivada o privada), deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.*

Se evidenció la existencia de documentos impresos en las impresoras con reportes generados con el Sistema de Información misional SIR y REL; lo cual denota ausencia de procedimientos para el manejo de información clasificada, lo cual puede causar la materialización del riesgo de afectación de la disponibilidad y confidencialidad de la información financiera gestionada con los Sistemas de Información misionales SIR y REL, generando un **incumplimiento** a los lineamientos del presente literal.

Conclusión: Incumplimiento de las: "*Políticas de uso de estaciones cliente", "Política de controles criptográficos", "Política de manejo, disposición de información, medios y equipos" y "Política de escritorio y pantalla limpia", incluidas en el documento*: *Política General y políticas específicas del Sistema de Seguridad de la Información de la SNR*, (CAPITULO II. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN), que establecen directrices para mitigar el riesgo: **"Afectación de la integridad, disponibilidad y/o confidencialidad de la información financiera gestionada con los Sistemas de Información misionales SIR y REL en cumplimiento de la Política General y políticas específicas del Sistema de Seguridad de la Información de la SNR"**, por cuanto se evidenciaron situaciones asociadas a la posibilidad de realizar cambios en las estaciones de trabajo cuando éstas no están integradas al directorio activo a causa de una modificación no autorizada sobre las configuraciones e instalaciones de los equipos de cómputo de la entidad; así como el hecho de dejar las sesiones abiertas en las estaciones de trabajo cuando los usuarios se ausentan de estas; razón por la que se deben implementar las acciones y controles requeridos con el ámbito de minimizar el impacto negativo por una ejecución inexacta de estos.

Recomendación:

Implementar la ejecución de los controles que dan cumplimiento a los lineamientos, como:

- Definir y asignar todas las responsabilidades de la seguridad de la información, donde los roles sean establecidos, coordinados y alineados con los roles internos de la SNR y las partes externas y comunicados a todas las partes interesadas para que éstas conozcan sus responsabilidades y participen de las concientizaciones que lidera la Oficina de Tecnologías de la información frente a la protección de la información.
- Liderar de forma efectiva, la implementación de los controles de seguridad de la información por la Oficina de Tecnologías de la Información y las Telecomunicaciones dando cumplimiento al Decreto 2723 de 2014 - "Por el cual se modifica la estructura de la Superintendencia de Notariado y Registro", ARTÍCULO 17. Funciones de la Oficina de Tecnologías de la Información. Función de la Oficina de Tecnologías de la Información: 18. Atender, proponer e implementar las políticas y acciones relativas a la seguridad de la información y de la plataforma tecnológica de la Superintendencia
- Realizar una revisión de los riesgos de seguridad de la información, junto con los controles que mitigan la materialización de los riesgos en concordancia con la clasificación de los activos de información, a fin de fortalecer los controles en cumplimiento de las políticas específicas: "Políticas de uso de estaciones cliente", "Política de controles criptográficos", "Política de manejo, disposición de información, medios y equipos" y "Política de escritorio y pantalla limpia".

En el marco de la verificación realizada a las: "*Política de control de acceso" y "Política de establecimiento, uso y protección de claves de acceso", incluida en el documento*: *Política General y políticas específicas del Sistema de Seguridad de la Información de la SNR*, (CAPITULO II. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN), se observaron las siguientes situaciones:

a) *Política de control de acceso - El acceso a los activos de información de la Superintendencia de Notariado y Registro está permitido únicamente a los usuarios autorizados.*

Conforme con lo verificado, se observó que los sistemas misionales SIR y REL, no se encuentran identificados como un activo de información en el link de transparencia: https://www.supernotariado.gov.co/transparencia/ley-de-transparencia/; no obstante, al validar que el acceso a estos sistemas misionales, este permitido únicamente por usuarios autorizados; se evidencio la existencia de usuarios activos en el sistema que se encuentran en periodo de vacaciones; situación que puede materializar el riesgo de afectación de la integridad, disponibilidad y/o confidencialidad de la información financiera gestionada con los Sistemas de Información misionales SIR y REL; en consecuencia, se denota un **incumplimiento** al presente literal.

b) *Política de control de acceso - El funcionario que disponga de claves de acceso a los activos de información será responsable de su uso, esta clave es personal e intransferible y la debe usar durante el proceso de autenticación. Y Política de establecimiento, uso y protección de claves de acceso - La Superintendencia de Notariado y Registro suministra a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible.*

Se observó en las Oficinas de Registro de Instrumentos públicos, que las claves de acceso a los activos de información, no son personales e intransferibles dado que se evidenció el uso compartido de éstas; situación que puede materializar el riesgo de afectación de la integridad, disponibilidad y/o confidencialidad de la información financiera gestionada con los Sistemas de Información misionales SIR y REL; lo que denota un **incumplimiento** al presente literal.

Así mismo, se observó un mal uso de las claves al ser escritas en papeles a la vista de cualquiera.

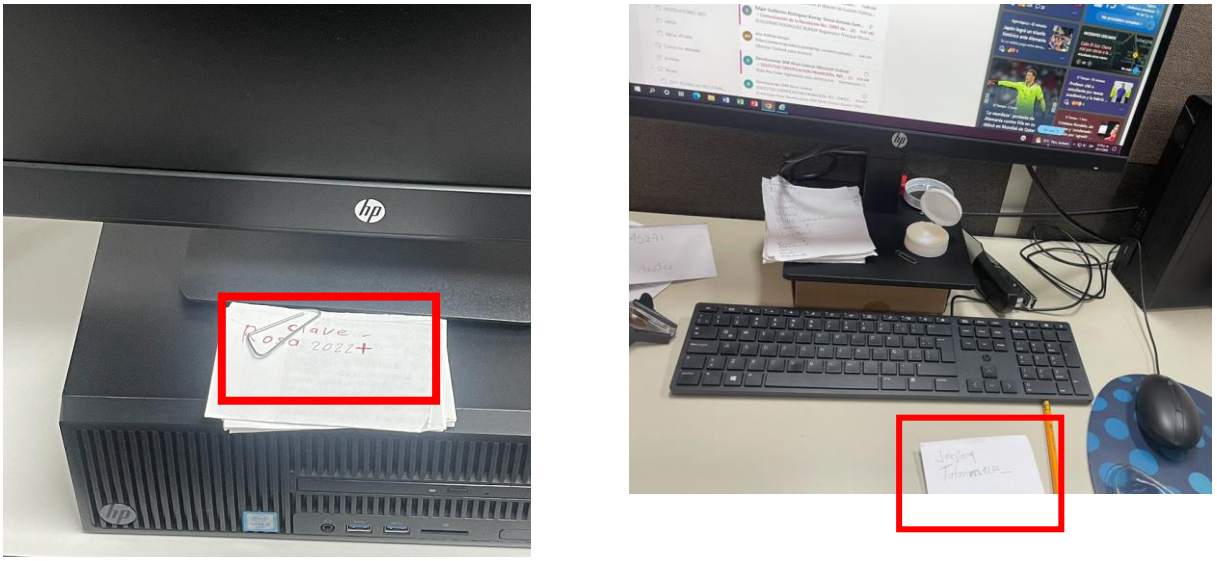

Ilustración 2: Claves escritas en papeles.

c) *Política de establecimiento, uso y protección de claves de acceso - Ningún usuario debe acceder a la red o a los servicios TIC de la Superintendencia de Notariado y Registro, utilizando una cuenta de usuario o clave de otro usuario.*

Tras verificar el uso de claves en las Oficinas de Registro de Instrumentos Públicos, se observó que el acceso a la red y los servicios TIC, en ocasiones, es realizado al hacer uso de una cuenta de usuario de otro usuario, conforme a lo identificado en la plataforma WOMPI, donde los usuarios con el rol Cajero, Coordinador Grupo Tecnológico Administrativo, conocen y acceden con el mismo usuario y contraseña; lo que denota un **incumplimiento** al presente literal.

Conclusión: Incumplimiento de las: "*Política de control de acceso" y "Política de establecimiento, uso y protección de claves de acceso"*, *incluidas en el documento*: *Política General y políticas específicas del Sistema de Seguridad de la Información de la SNR*, (CAPITULO II. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN), que establecen directrices para mitigar el riesgo: **"Afectación de la integridad y/o confidencialidad de la información financiera gestionada con los Sistemas de Información misionales SIR y REL en cumplimiento de la Política General y políticas específicas del Sistema de Seguridad de la Información de la SNR"**, por cuanto se observó un manejo de los usuarios y contraseñas inseguro, con las cuales se accede a la información lo que podría conllevar a inexactitudes, fraude o decisiones erróneas por la modificación no autorizada de los datos y los sistemas bien sea de manera accidental o intencional.

Recomendación:
Implementar la ejecución de los controles que dan cumplimiento a los lineamientos, como:

- Fortalecer y complementar la identificación de activos de información en donde se valide la pertinencia de referenciar los sistemas de información en donde se registra información de la entidad, sin embargo, no son propiedad de la SNR como es el caso de Wompi, y los portales bancarios los cuáles se acceden a través de un usuario y contraseña propiedad de la SNR.
- Establecer procedimientos de aprovisionamiento y des aprovisionamiento de usuarios cuando ocurran situaciones que implican cambios o terminación de perfiles de acceso de los usuarios.
- Desarrollar acciones para restringir y controlar la asignación y uso de derechos de acceso privilegiado para los sistemas información misional SIR y REL.
- Revisar los derechos de acceso periódicamente y después de cualquier cambio, promoción, cambio a un cargo a un nivel inferior, o terminación del empleo.

En el marco de la verificación realizada a la: "*Política de seguridad del centro de datos y centros de cableado" y "Política de Seguridad Física", incluida en el documento*: *Política General y políticas específicas del Sistema de Seguridad de la Información de la SNR*, (CAPITULO II. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN), se observaron las siguientes situaciones:

a) *Políticas de seguridad del centro de datos y centros de cableado - Los centros de cómputo deben mantener las condiciones físicas y ambientales óptimas recomendadas, así como controles automáticos para incendio, temperatura y cuando sea posible monitoreo por Circuito Cerrado de Televisión.*

Una vez revisado los centros de cableado de cada Oficina de Registro de Instrumentos Públicos, se evidenció que no se mantienen las condiciones físicas y ambientales óptimas recomendadas, con base en los

siguientes eventos evidenciados, que pueden materializar el riesgo de afectación de la disponibilidad de la información financiera gestionada con los Sistemas de Información misionales SIR y REL:

- Administración autónoma de cámaras pertenecientes a la Oficina de Registro de Instrumentos Públicos de Popayán, las cuales estaban ubicadas en los corredores de las áreas comunes, sin embargo, el cuarto del centro de control de monitoreo permanece desatendido.
- Ausencia en el seguimiento y monitoreo de las condiciones ambientales tales como temperatura y humedad, para determinar las condiciones que puedan afectar adversamente las instalaciones de procesamiento de información.
- Desconocimiento por parte de los usuarios finales, las directrices acerca de comer, consumir líquidos y fumar en cercanías de las instalaciones de procesamiento de información.
- Probabilidad de afectación a los centros de cableado por amenazas físicas y ambientales de acuerdo con la ubicación y la localización de cada Oficina de Registro de Instrumentos Públicos, tales como conato de incendio, polvo, corrosión, eventos naturales, perdida de los servicios esenciales por fallas en el sistema de suministro de agua o aire acondicionado, perdida de suministro de energía, y/o falla en los equipos de telecomunicaciones.
- Ausencia de controles de acceso a los centros de cableado y a los gabinetes de control, lo cual causa la probabilidad de acceso no autorizado y daño en componentes tecnológicos.
- Falta de señalización de áreas con riesgo eléctrico (cuarto de ubicación de UPS y planta)
- Falta de estandarización y debilidades en el etiquetado de cableado y equipos.
- Presencia de objetos inadecuados en los centros de cómputo y de cableado
- Falla en el sistema de detección de incendios de la Oficina de Registro de Instrumentos Públicos de Bucaramanga.

Conforme con lo anterior, se denota un **incumplimiento** al presente literal.

b) Política de Seguridad Física - La OTI debe tener implementadas, alarmas de detección de intrusos en los centros de datos y centros de cableado de la Superintendencia de Notariado y Registro.

Se observó la inexistencia de alarmas de detección de intrusos en el centro de datos y de cableado de las Oficinas de Registro de Instrumentos Públicos de Manizales, Bucaramanga y Popayán, lo que denota un **incumplimiento** del presente literal.

c) Todas las áreas destinadas al procesamiento, almacenamiento de documentos o información, así como aquellas en las que se encuentren los equipos de cómputo y demás infraestructura de los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. Por tanto, contarán con medidas de control de acceso físico en el perímetro, de tal forma que puedan ser auditadas con procedimientos de seguridad operacionales, que permitan proteger la información.

Se observó que las áreas consideradas con acceso restringido, cuentan con controles de acceso físico con ciertas limitantes en su implementación lo cual puede materializar el riesgo de afectación de la confidencialidad de la información financiera gestionada con los Sistemas de Información misionales SIR y REL, conforme a las siguientes situaciones observadas:

- Debilidad en los controles de seguridad física en las instalaciones de almacenamiento de información para evitar el acceso no autorizado.
- Ausencia de una puerta para restringir el acceso al centro de datos de la Oficina de Registro de Instrumentos Públicos de Manizales.
- Control de acceso biométrico con fallas al ingreso al área administrativa de la Oficina de Registro de Instrumentos Públicos de Popayán.
- Control de acceso biométrico en funcionamiento para ingresar al centro de datos de la Oficina de Registro De Instrumentos Públicos de Bucaramanga.

Conforme con lo anterior, se denota un **incumplimiento** al presente literal.

Conclusión: Incumplimiento de las: "*Política de seguridad del centro de datos y centros de cableado" y "Política de Seguridad Física"*, *incluidas en el documento*: *Política General y políticas específicas del Sistema de Seguridad de la Información de la SNR*, (CAPITULO II. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN), que establecen directrices para mitigar el riesgo: **"Afectación de la integridad y/o confidencialidad de la información financiera gestionada con los Sistemas de Información misionales SIR y REL en cumplimiento de la Política General y políticas específicas del Sistema de Seguridad de la Información de la SNR"**, al encontrar condiciones de seguridad de instalaciones físicas y del cableado inadecuadas como: daño de los equipos a causa de factores físicos y medio ambientales, daño o afectación a la infraestructura de la edificación y posible afectación de la vida y salud de las personas (funcionarios, contratistas y/o visitantes de la Oficinas de Registro de Instrumentos Públicos).

Así mismo, se identificó la falta de mantenimiento de equipos e instalaciones físicas y eléctricas, en la demarcación de zonas seguras asociadas al procesamiento de información y/o resguardo y protección de equipos de soporte energético de respaldo y en la estandarización del etiquetado y condiciones de instalación del cableado estructurado.

Recomendación:

Implementar la ejecución de los controles que dan cumplimiento a los lineamientos, como:

- Fortalecer la cultura de gestión de seguridad de la información que es visibilizada a través de la concientización del personal frente a la protección de la información.
- Subsanar las limitaciones locativas y físicas para implementar controles que preserven la seguridad de la información.
- Potencializar las acciones que llevan a construir un control Interno eficaz en la aplicación de controles y procedimientos que dan cumplimiento a las políticas específicas de seguridad de la información.
- Establecer actividades de monitoreo y control a las situaciones de advertencia que pueden materializar riesgos que afecten la seguridad de la información.

3. Identificación de situaciones que afectan la seguridad de la información de los Sistemas de Información misionales SIR y REL que contienen el componente financiero relacionados en las actividades del Procedimiento -Recaudos por la Prestación del Servicio Público Registral - Código: MP - GNFA- PO - 02 - PR – 02 - Versión: 01, en cumplimiento de la Resolución 193 de 2016, CONTADURÍA GENERAL DE LA NACIÓN, Numeral 3.2.3.1 SOPORTES DOCUMENTALES. – Numeral 3.2.8 -EFICIENCIA DE LOS SISTEMAS DE INFORMACIÓN 193 de 2016.

Para la validación del cumplimiento de la Resolución 193 de 2016, CONTADURÍA GENERAL DE LA NACIÓN, Numeral 3.2.3.1 SOPORTES DOCUMENTALES. – Numeral 3.2.8 EFICIENCIA DE LOS SISTEMAS DE INFORMACIÓN 193 de 2016, a través de la identificación de situaciones que afectan la seguridad de la información de los Sistemas de Información misionales SIR y REL que contienen el componente financiero relacionados en las actividades del Procedimiento -Recaudos por la Prestación del Servicio Público Registral - Código: MP - GNFA- PO - 02 - PR – 02 - Versión: 01, la OCIG realizó prueba de recorrido en las tres Oficinas de Registro de Instrumentos Públicos donde se identificaron situaciones que afectan la seguridad de la información de los Sistemas de Información misionales SIR y REL que contienen el componente financiero relacionados en las actividades del Procedimiento Recaudos por la Prestación del Servicio Público Registral.

3.1. <u>Riesgo evaluado</u>: "Incumplimiento de la Resolución 193 de 2016, CONTADURÍA GENERAL DE LA NACIÓN, Numeral 3.2.3.1 SOPORTES DOCUMENTALES. – Numeral 3.2.8 -EFICIENCIA DE LOS SISTEMAS DE INFORMACIÓN 193 de 2016, a través de la identificación de situaciones que afectan la seguridad de la información de los Sistemas de Información misionales SIR y REL que contienen el componente financiero relacionados en las actividades del Procedimiento -Recaudos por la Prestación del Servicio Público Registral - Código: MP - GNFA- PO - 02 - PR – 02 - Versión: 01

Conforme a lo establecido en la *Resolución 193 de 2016, CONTADURÍA GENERAL DE LA NACIÓN*, por la cual se determinan los elementos y actividades de control interno para gestionar el riesgo contable, se encontraron las siguientes situaciones:

- *Numeral 3.2.3.1 SOPORTES DOCUMENTALES. – "La totalidad de las operaciones realizadas por la entidad deberá estar respaldada en documentos idóneos, de manera que la información registrada sea susceptible de verificación y comprobación exhaustiva o aleatoria; por lo cual, no podrán registrarse contablemente los hechos económicos que no se encuentren debidamente soportados. (…) De conformidad con el desarrollo de la gestión contable por procesos y los manuales de procedimientos implementados en las entidades, se deberá hacer un análisis y evaluación de los diferentes tipos de documentos que sirven de soporte a las operaciones llevadas a cabo, así como de la forma y eficiencia de su circulación entre las dependencias, y entre la entidad y los usuarios externos, con el propósito de tomar las medidas que sean necesarias para garantizar un eficiente flujo de documentos."*

Se observó que las operaciones realizadas por la entidad, se encuentran respaldadas en documentos idóneos, de manera que la información registrada sea susceptible de verificación y comprobación exhaustiva; no obstante, se evidenció una situación que afecta la integridad de la información para la actividad de preliquidación realizada en ventanilla, donde se evidenció que no hay claridad en cuanto a qué soporte se debe entregar al Ciudadano para que conozca el valor a pagar, dado que en una Oficina de Registro de Instrumentos Públicos, se entrega la información a través de copia impresa desde la plataforma WOMPI, que genera un número de referencia, mientras que en otra Oficina de Registro de Instrumentos Públicos, se entrega desde el aplicativo SIR, a través de tres copias impresas (predefinidas), donde dos copias se

entregan al Ciudadano y una tercera es reciclada. En la última Oficina de Registro de Instrumentos Públicos, se entrega al ciudadano, un papel con los datos del valor a cancelar.

Con respecto a las trasferencias electrónicas como otro medio de recaudo, no se evidenciaron actividades de control documentadas a través del procedimiento, para realizar la verificación y validación de este ingreso, solo se menciona a través del procedimiento que: "*por transferencia de fondos o consignación en efectivo; él usuario debe presentar el original de la consignación o la prueba de la transferencia".* Similar situación, se identificó con los pagos realizados a través del medio de recaudo REL, dado que, desde las Oficinas de Registro, no se cuenta con acceso a la cuenta bancaria nacional, puesto que no se tiene usuario, ni contraseña, para realizar su validación y en algunos casos, se desconoce la cuenta de destino; con lo cual no se podría establecer la veracidad del pago, a fin de evitar fraudes, y garantizar el pago de los derechos del registro.
Al realizar estas actividades se puede determinar que conllevan a **generar mayor consumo de papel** y en volumen de impresiones, acarreando mayores costos para la operación en la entidad.

Ahora bien, según lo evidenciado en las tres Oficinas de Registro de Instrumentos Públicos, y frente a los soportes de pago que son requeridos por el cajero al ciudadano para respaldar la información de ingresos, se evidenció que en dos Oficinas de Registro de Instrumentos Públicos solicitan el boucher de pago y una fotocopia del mismo, mientras que, en otra, se solicitan las dos copias del baucher que es entregada por el operador al ciudadano. Esta situación permitió determinar que **no hay claridad de cuál es el soporte que debe ser requerido al ciudadano y en qué cantidad**, conllevando a incurrir en más gastos para el ciudadano.

Así mismo, se identifica la situación de afectación de la integridad de la información frente a la conservación documental de los soportes correspondientes a recibos de caja y documentos registrales, dado que la Oficina de Registro de Instrumentos Públicos de Popayán, no cuenta con el apoyo de la plataforma IRIS-DOCUMENTAL, lo cual demuestra una inefectividad en la acción de garantizar un eficiente flujo de documentos; más aún, cuando se cobra a los ciudadanos una tarifa de conservación documental. Ahora bien, respecto a la entrega de los documentos registrales al abogado, se observó que existe una ausencia de control frente a los soportes documentales entregados con el fin de mantener la integridad del expediente entregado, situación que fue informada al momento del seguimiento para establecer el control correspondiente. Adicionalmente, se evidenciaron notas devolutivas tramitadas de forma manual, con archivos desde la vigencia 2016, donde su control se realiza a través de un archivo en Word, el cual no permite tener presente las fechas límites de notificación, entre otros aspectos importantes, esta situación puede generar el riesgo de la perdida de integridad y disponibilidad de la información relacionada con las notas devolutivas.

Conforme con lo anterior, se denota un **incumplimiento** al presente numeral.

- *Numeral 3.2.8 -EFICIENCIA DE LOS SISTEMAS DE INFORMACIÓN. – "Con independencia de la forma que utilicen las entidades para procesar la información, el diseño del sistema implementado deberá garantizar eficiencia y eficacia en el procesamiento y generación de la información financiera. Para la*

implementación y puesta en marcha de sistemas automatizados, las entidades observarán criterios de eficiencia en la adquisición de equipos y programas que contribuyan a satisfacer sus necesidades de información, atendiendo la naturaleza y complejidad de la entidad de que se trate; además, se deberá procurar que los sistemas implementados integren adecuadamente los principales procesos que tienen a su cargo las dependencias.".

Se evidenció que el sistema implementado por la entidad para procesar la información, presentó falencias al momento de garantizar eficiencia y eficacia en el procesamiento y generación de la información financiera dada la situación que afecta la integridad de la información, para la actividad observada frente a los pagos que son realizados en la ventanilla de la misma Oficina de Registro de Instrumentos Públicos, se evidenció que se están recibiendo los originales del boucher; sin embargo, se evidenciaron situaciones que no permiten al aplicativo SIR, realizar la validación que el PIN, solo se registre una vez en el sistema, toda vez que para generar el recibo de caja, en una Oficina de Registro de Instrumentos Públicos, al momento de ser registrado el PIN en el campo de consignación del aplicativo SIR, se debió anteponer dos ceros (00) al número completo que aparece en el boucher; y en otra Oficina de Registro de Instrumentos Públicos, debieron anteponer el año (2022) para lograr la inclusión del pago, de lo contrario, aparece un error indicando que el pin ya está en uso.
No obstante, se precisa que, en la validación del equipo auditor, se observó que el ciudadano solicitó la preliquidación del trámite, acto seguido realizó el pago e hizo entrega de los dos Boucher que lo soportan. En ese sentido, se determinó por el equipo auditor que **el control asignado a través del Sistema de Información misional SIR no está siendo eficiente**, por consiguiente, el riesgo de evitar fraudes, y garantizar el pago de los derechos del registro, continua sin ser controlado.

Ahora bien, con respecto a lo estipulado en la circular 414 de julio del 2022 con asunto: "*Datos Recibo de Caja"*, a fin de dar cumplimiento a esta circular, el cajero coloca los datos de los intervinientes en el campo "*Nombres / Razón Social",* digitando el nombre, cedula y teléfono de contacto del ciudadano, datos que no corresponde con el título del campo, situación que afecta la integridad y calidad de los datos ingresados al sistema de información misional SIR, dado que el campo refiere solo la digitación del nombre, mas no la cédula y el teléfono del ciudadano.

Por otro lado, en la Oficina de Registro de Instrumentos Públicos de Manizales se evidenció que se vienen presentando pequeñas diferencias en el valor de la conservación documental, confrontando los valores del Sistema de Información SIR, con los del REL, donde para los turnos 2022-100-6-20803 y 2022-100-6-20873, existio una diferencia de $100 cada uno. Así mismo, en el reporte consolidado del SIR con No.25-Informes Recaudo del Día (Tiracaja), confrontado con el reporte No.51B - Diario Radicador de Certificados, para el día 21 de enero de 2022, se evidenció que existe una diferencia por valor de $476.000, que corresponden a consignación "C_Reval"; cuando debieran coincidir estos reportes. Similar situación se evidenció con el reporte 51- Resumén Diario de Ingresos y Egresos del 21 de enero de 2022, que no consolida el valor de la conservación documental por $579.900, conllevando a que éste reporte no permita mostrar toda la información financiera procesada a través del aplicativo SIR, conllevando a que sea necesario imprimir diferentes reportes al momento de realizar el boletín diario por parte de la ORIP.

Conclusión: Incumplimiento de la Resolución 193 de 2016, CONTADURÍA GENERAL DE LA NACIÓN, Numeral 3.2.3.1 SOPORTES DOCUMENTALES. – Numeral 3.2.8 -EFICIENCIA DE LOS SISTEMAS DE INFORMACIÓN 193 de 2016, a través de la identificación de situaciones que afectan la seguridad de la información de los Sistemas de Información misionales SIR y REL que contienen el componente financiero relacionados en las actividades del Procedimiento -Recaudos por la Prestación del Servicio Público Registral - Código: MP - GNFA- PO - 02 - PR – 02 - Versión: 01, al encontrar situaciones que afectan la integridad de la información a causa del hecho de que no se cuenta con un procedimiento actualizado y estandarizado, acorde con las actividades desarrolladas en cada una de las oficinas de registro, identificando claramente los puntos de control para estas actividades y los responsables, con el fin de establecer controles efectivos, máxime cuando las Oficinas de Registro de Instrumentos Públicos son catalogadas como áreas proveedoras que intervienen en el suministro de información financiera, al contabilizar los ingresos mensuales.

Así mismo; el hecho de no contar con un análisis y evaluación de los diferentes tipos de documentos que sirven de soporte a las operaciones llevadas a cabo por la entidad; así como por la falta de eficiencia en el procesamiento y validación del soporte de pago asociado al PIN, como información financiera; conllevan a la afectación de los estados financieros, al materializarse los riesgos señalados por las debilidades y desactualizaciones identificadas en el procedimiento -Recaudos por la Prestación del Servicio Público Registral - Código: MP - GNFA- PO - 02 - PR – 02 - Versión: 01, en cuanto a las actividades necesarias para realizar las conciliaciones y cruces de información que garanticen el registro contable oportuno de los ingresos y su medición monetaria confiable.

Recomendación:

Implementar la ejecución de los controles que dan cumplimiento a los lineamientos, como:

- Actualizar el Procedimiento -Recaudos por la Prestación del Servicio Público Registral - Código: MP - GNFA- PO - 02 - PR – 02 y complementar las actividades allí descritas con la realidad de las Oficinas de Registro de Instrumentos Públicos.
- Desarrollar mesas de trabajo con Gestión Documental para que las Oficinas de Registro de Instrumentos Públicos que no cuentan con IRIS documental, puedan tener el beneficio la custodia de la información y la reducción del riesgo de corrupción que puede existir en cuanto al manejo de la información de manera manual.
- Establecer procedimientos de aprovisionamiento y des-aprovisionamiento de usuarios cuando ocurran situaciones que implican cambios o terminación de perfiles de acceso de los usuarios.
- Fomentar en la entidad, la formación de una cultura de control que contribuya at mejoramiento continuo para identificar oportunidades de mejora en los sistemas misionales de la entidad.
- Alinear las instrucciones dadas por el área misional junto con la preservación de la seguridad de la información que se encuentra en los sistemas de información misionales de la entidad.

4. MAPA DE RIESGOS

Matriz de Riesgos Institucional			
PROCESO	**NOMBRE DEL RIESGO**	**CONTROL**	**PRONUNCIAMIENTO DE EFECTIVIDAD OCIG**
GESTIÓN TECNOLOGICO Y ADMINISTRATIVO (ORIP MANIZALES – BUCARAMANGA Y POPAYÁN)	Desvío de recursos físicos o económicos durante la conciliación de ingresos y anticipados diarios en las Oficinas de Registro de Instrumentos Públicos	Verificar diariamente la conciliación de los ingresos y anticipados	Se advierte la presencia del mismo riesgo asociado a este proceso para las tres Oficinas De Registro de Instrumentos Públicos, cuyo control no responde de manera efectiva ante las situaciones de riesgo contempladas en el presente informe, por lo anterior, se recomienda estructurar una matriz de riesgos que incorpore todas aquellas acciones de control que considere necesario, en respuesta a un análisis de causa raíz exhaustivo que contemple todos aquellos posibles riesgos al cual este expuesto el proceso, teniendo en cuenta la recurrencia y su impacto frente al cumplimiento y desarrollo del mismo, aun mas cuando se asignan responsabilidades en los niveles descritos a continuación: *"…**ORIP Seccional:** El Registrador verifica y valida diario las conciliaciones. **ORIP Principal**: El Coordinador de Gestión Tecnológico y Administrativo y contador verifican diario. **Dirección Regional**: Contador Regional y Director Regional, verifican mensual…"* y se observó deficiencia en las actividades de inspección periódica como parte del monitoreo obligatorio al no ser realizadas. Así mismo, se observó que el responsable del monitoreo de riesgos para la Oficina de Registro de Instrumentos Públicos de Manizales, realizó el reporte a la Oficina Asesora de Planeación de acuerdo con los tiempos requeridos, mientras que las Oficinas de Registro de Instrumentos Públicos de Popayán y Bucaramanga no lo efectuaron; por lo que se recomienda fortalecer la cultura de seguimiento y reporte. Lo anterior, ha sido detectado por esta Oficina a través de los informes de seguimiento y evaluación de vigencias anteriores, así como los identificados por la Contraloría General de la Republica mediante los informes de auditoría financiera, hecho que contraviene los lineamientos emitidos en la Política de Administración de Riesgos de la Entidad.

Riesgos identificados en la ejecución de los contratos objeto de auditoria		
NOMBRE DEL RIESGO	**MACROPROCESO**	**PRONUNCIAMIENTO DE EFECTIVIDAD OCIG**
Pérdida de Confidencialidad de la Información del recaudo y pérdida de integridad de las estaciones de trabajo	Gestión de las tecnologías de la información Administración del servicio público Registral Gestión Financiera	Por deficiencias el incumplimiento de los Lineamientos de seguridad establecidos en la "*Guía 18: Lineamientos Terminales de áreas financieras entidades públicas, Modelo de Seguridad y Privacidad de la Información de MINTIC"*, se evidenció la posibilidad de materialización del riesgo: *"Pérdida de Confidencialidad de la Información del recaudo y pérdida de integridad de las estaciones de trabajo*", por cuanto se observó la posibilidad de ocurrencia de situaciones asociadas a: • Suplantación de identidad, inadecuada segregación de funciones, instalación de software malintencionado, no licenciado o controladores de dispositivos no autorizados y conexión desde el exterior de la entidad a las estaciones de trabajo asociadas a los roles de Contador y Coordinador Grupo Tecnológico Financiero. • Acceso físico no autorizado y/o robo de información por personas no autorizadas, así como la ausencia de cámaras de video que cubran al menos el acceso principal al área y el funcionario que utiliza la estación de trabajo asociadas a los roles de Contador y Coordinador Grupo Tecnológico Financiero. • Ejecución de inadecuados controles para proteger los usuarios y perfiles. Razón por la que se hace necesario continuar con la ejecución de actividades de sensibilización para generar una cultura de seguridad así como fortalecer desde la Oficina de Tecnologías de la Información del Nivel Central la implantación de controles de seguridad informática en las Oficinas de Registro de Instrumentos Públicos y las actividades de seguimiento y control permanente sobre la ejecución de los controles implementados, alineado con los compromisos y responsabilidades adquiridas por los usuarios.
Afectación de la integridad, disponibilidad y/o confidencialidad de la información financiera gestionada con los Sistemas de Información misionales SIR y REL en cumplimiento de la Política General y políticas específicas del Sistema de Seguridad de la Información de la SNR.	Gestión de las tecnologías de la información Administración del servicio público Registral Gestión Financiera	Se evidenció la posibilidad de materialización de este riesgo, "Afectación de la integridad, disponibilidad y/o confidencialidad de la información financiera gestionada con los Sistemas de Información misionales SIR y REL en cumplimiento de la Política General y políticas específicas del Sistema de Seguridad de la Información de la SNR", por cuanto se evidenciaron la ocurrencia de situaciones asociadas con: • La posibilidad de realizar cambios en las estaciones de trabajo cuando estas no están integradas al directorio activo a causa de una modificación no autorizada sobre las configuraciones e instalaciones de los equipos de cómputo de la entidad; así como el hecho de dejar las sesiones abiertas en las estaciones de trabajo cuando los usuarios se ausentan de estas. • El manejo de los usuarios y contraseñas inseguro, con las cuales se accede a la información lo que podría conllevar a inexactitudes, fraude o decisiones erróneas por la modificación no autorizada de los datos y los sistemas bien sea de manera accidental o intencional.

		• El daño de los equipos a causa de factores físicos y medio ambientales, daño o afectación a la infraestructura de la edificación y posible afectación de la vida y salud de las personas (funcionarios, contratistas y/o visitantes de la Oficinas de Registro de Instrumentos Públicos). • El mantenimiento de equipos e instalaciones físicas y eléctricas, en la demarcación de zonas seguras asociadas al procesamiento de información y/o resguardo y protección de equipos de soporte energético de respaldo y en la estandarización del etiquetado y condiciones de instalación del cableado estructurado. Razón por la que se deben implementar las acciones y controles requeridos con el ámbito de minimizar el impacto negativo por una ejecución inexacta de estas situaciones.
Incumplimiento de la Resolución 193 de 2016, CONTADURÍA GENERAL DE LA NACIÓN, Numeral 3.2.3.1 SOPORTES DOCUMENTALES. – Numeral 3.2.8 - EFICIENCIA DE LOS SISTEMAS DE INFORMACIÓN 193 de 2016, a través de la identificación de situaciones que afectan la seguridad de la información de los Sistemas de Información misionales SIR y REL que contienen el componente financiero relacionados en las actividades del Procedimiento -Recaudos por la Prestación del Servicio Público Registral - Código: MP - GNFA- PO - 02 - PR – 02 - Versión: 01	Gestión de las tecnologías de la información Administración del servicio público Registral Gestión Financiera	Ante la ausencia de controles que mitiguen la materialización del riesgo de "*Incumplimiento de la Resolución 193 de 2016, CONTADURÍA GENERAL DE LA NACIÓN, Numeral 3.2.3.1 SOPORTES DOCUMENTALES. – Numeral 3.2.8 -EFICIENCIA DE LOS SISTEMAS DE INFORMACIÓN 193 de 2016, a través de la identificación de situaciones que afectan la seguridad de la información de los Sistemas de Información misionales SIR y REL que contienen el componente financiero relacionados en las actividades del Procedimiento -Recaudos por la Prestación del Servicio Público Registral - Código: MP - GNFA- PO - 02 - PR – 02 - Versión: 01*" tras identificar situaciones que afectan la integridad de la información a causa de los siguientes hechos: • El no cotar con un procedimiento actualizado y estandarizado, acorde con las actividades desarrolladas en cada una de las oficinas de registro, identificando claramente los puntos de control para estas actividades y los responsables, con el fin de establecer controles efectivos, máxime cuando las Oficinas de Registro de Instrumentos Públicos son catalogadas como áreas proveedoras que intervienen en el suministro de información financiera, al contabilizar los ingresos mensuales. • El hecho de no contar con un análisis y evaluación de los diferentes tipos de documentos que sirven de soporte a las operaciones llevadas a cabo por la entidad; así como por la falta de eficiencia en el procesamiento y validación del soporte de pago asociado al PIN, como información financiera; conllevar a la afectación de los estados financieros, al materializarse los riesgos señalados por las debilidades y desactualizaciones identificadas en el procedimiento -Recaudos por la Prestación del Servicio Público Registral - Código: MP - GNFA- PO - 02 - PR – 02 - Versión: 01, en cuanto a las actividades necesarias para realizar las conciliaciones y cruces de información que garanticen el registro contable oportuno de los ingresos y su medición monetaria confiable.

5. EFECTIVIDAD DEL PLAN DE MEJORAMIENTO POR PROCESO Y CONTRALORIA GENERAL DE LA REPUBLICA

SEGUIMIENTO AL PLAN DE MEJORAMIENTO CONTRALORIA GENERAL		
CÓDIGO HALLAZGO	**DESCRIPCIÓN DE LOS HALLAZGOS**	**PRONUNCIAMIENTO OCIG**
202103AFE	H89. Consignaciones Trámites Derechos de Registro SIR y FOLIO (IP) (D) se evidencian deficiencias en la calidad de la información que se registra de las Bases de Datos de los sistemas misionales, en donde existe un procedimiento unificado para la incorporación de datos y revisión que garantice la calidad, seguridad y consistencia de la misma.	En el desarrollo del presente informe de seguimiento, se pudo evidenciar que persiste las deficiencias reportadas por contraloría en la calidad de la información que se registra en las bases de datos del sistema de información misional SIR, según lo señalado en el ítem 3 de este informe, conllevando a la afectación de la integridad y disponibilidad de la información existente en la entidad, por lo cual las acciones propuestas son inefectivas. El hallazgo persiste. Se debe reformular. La acción de mejora es **INEFECTIVA.**

SEGUIMIENTO AL PLAN DE MEJORAMIENTO INSTITUCIONAL		
CÓDIGO HALLAZGO	**DESCRIPCIÓN DE LOS HALLAZGOS**	**PRONUNCIAMIENTO OCIG**
2019204	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.	En el desarrollo del presente informe de seguimiento, se pudo evidenciar que persiste la inobservancia frente al no uso del formato: FORMULARIO PARA ADMINISTRACIÓN DE USUARIOS NUEVOS, ACTIVOS E INACTIVOS, situación por la que se advierte

		sobre la falta de cumplimiento en el procedimiento de gestión de usuarios. El hallazgo persiste. La acción de mejora es **INEFECTIVA**
2019201	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.	Se evidenció luego de la verificación del procedimiento de recaudo; que persiste la inobservancia a presuntas faltas relacionadas con manipulación, utilización y adulteración del aplicativo misional SIR. El hallazgo persiste. La acción de mejora es **INEFECTIVA**
2019201	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. Esta situación, podría conllevar a la materialización del riesgo de incendio por el recalentamiento de los equipos; lo que tendría como consecuencia la suspensión del servicio y/o pérdida de información. La situación anterior podría dar lugar al incumplimiento del numeral 7.1.3, que establece que la organización debe determinar, proporcionar y mantener la infraestructura necesaria para la operación de sus procesos y lograr la conformidad de los productos y servicios.	Resultado del presente informe de seguimiento, se pudo evidenciar que persisten, condiciones técnicas de instalación y/o mantenimiento inadecuadas (fuentes generadoras de riesgo) en los cuartos de cómputo y centros de cableado. El hallazgo persiste. La acción de mejora es **INEFECTIVA**
20220719	Una vez revisado los mecanismos de control, se observan debilidades en los controles preventivos, detectivos y correctivos que la Oficina de Tecnología de Información tiene establecido; incumpliendo con esto, lo establecido en la "Política general y políticas específicas del sistema de seguridad de la información de la SNR" - Política de cumplimiento de requisitos legales y contractuales.- La Superintendencia de Notariado y Registro respeta y acata las normas legales existentes relacionadas con seguridad de la información, para lo cual realizará una continua revisión, identificación, documentación y cumplimiento de la legislación y requisitos contractuales aplicables para la Superintendencia de Notariado y Registro, relacionada con la seguridad de la información", situación que puede llegar a generar riesgos que afecten la confidencialidad, integridad y disponibilidad de la información de la entidad.	Se evidencia la recurrencia en las debilidades en los controles preventivos, detectivos y correctivos que la Oficina de Tecnología de Información tiene establecido.
20210114	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	De acuerdo con las visitas realizadas a las Oficinas de Registro de Instrumentos Públicos, se pudo evidenciar el incumplimiento a los ANS ante la falla reportada desde el día 21 de febrero del 2002, frente a la afectación equipos que soportan el fluido eléctrico del ORIP de Popayán. Lo anterior, pone en riesgo la continuidad en la prestación del servicio misional y el cumplimiento de los objetivos de los procesos, entre otros. El hallazgo persiste. La acción de mejora es **INEFECTIVA**

	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.	
20211024	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."	Conforme a las revisiones efectuadas en las Oficinas de Registro de Instrumentos Públicos, se evidenció que se viene realizando reuniones de divulgación y socialización de Política de Seguridad de la Información, el procedimiento: Gestión de Incidentes de Seguridad de la Información. No obstante, se evidencia el incumplimiento de las mismas a través de la ejecución de comportamientos inseguros efectuados por los usuarios. La actividad se cumple, sin embargo. La acción de mejora es **INEFECTIVA**

Con relación a la suscripción de planes de mejoramiento producto de las auditorias internas de gestión realizadas por la oficina de control interno de Gestión, se evidencio que en la oficina de registro de Manizales no fue suscrito el plan de mejoramiento inobservando lo señalado en el Procedimiento de Plan de Mejoramiento.

Ahora bien, con respecto a las actividades del plan de mejoramiento calificadas como inefectivas, se hace necesario realizar el análisis causa raíz e implementar nuevas acciones de mejora tendientes a subsanar los hallazgos identificados. Dadlo lo anterior la Oficina Asesora de Planeación, por la responsabilidad que les asiste como segunda línea de defensa respectivamente, conforme al Modelo Integrado de Planeación y Gestión – MIPG; con el fin de formular y suscribir el Plan de Mejoramiento con los hallazgos consignados en el presente informe, dentro de los quince (15) días hábiles siguientes al recibo de este.

6. MATRIZ DE RESULTADOS PROCESO AUDITOR

En el presente informe de seguimiento, se establecieron dos (2) NO CONFORMIDADES REALES; razón por la que se hace necesario; formular, implementar y ejecutar acciones correctivas, preventivas y/o de mejora, mediante el análisis de causa raíz y el seguimiento de las acciones implementadas, con el propósito de subsanar la causa raíz que dio origen al mismo, relacionado a continuación:

ITEM	DESCRIPCION DEL HALLAZGO	TIPO DE HALLAZGO NCR / NCP	RECOMENDACIÓN	PROCESO RESPONSABLE
1	**Incumplimiento a lo establecido a Política General y políticas específicas del Sistema de Seguridad de la Información de la SNR - y numerales 5.1, 5.2, 5.3, 5.4 y 5.5 de la Guía 18:**	NCR	Dar cumplimiento la Política General y políticas específicas del Sistema de Seguridad de la Información de la	**Macroproceso Responsable:**

	Lineamientos frente a la afectación de la integridad, disponibilidad y/o confidencialidad de la información financiera gestionada con los Sistemas de Información misionales SIR y REL.		SNR y a los numerales 5.1, 5.2, 5.3, 5.4 y 5.5 de la Guía 18: Lineamientos: Terminales de áreas financieras entidades públicas. Modelo de Seguridad y Privacidad de la Información de MINTIC.	Gestión de las tecnologías de la información Administración del servicio público Registral Gestión Financiera
2	**Incumplimiento de la Resolución 193 de 2016, CONTADURÍA GENERAL DE LA NACIÓN, Numeral 3.2.3.1 SOPORTES DOCUMENTALES. – Numeral 3.2.8 -EFICIENCIA DE LOS SISTEMAS DE INFORMACIÓN 193 de 2016, a través de la identificación de situaciones que afectan la seguridad de la información de los Sistemas de Información misionales SIR y REL que contienen el componente financiero relacionados en las actividades del Procedimiento -Recaudos por la Prestación del Servicio Público Registral – Código: MP – GNFA- PO – 02 - PR – 02 - Versión: 01**	NCR	Dar cumplimiento a la Resolución 193 de 2016, CONTADURÍA GENERAL DE LA NACIÓN, Numeral 3.2.3.1 SOPORTES DOCUMENTALES. – Numeral 3.2.8 -EFICIENCIA DE LOS SISTEMAS DE INFORMACIÓN 193 de 2016.	**Macroproceso Responsable:** Gestión de las tecnologías de la información Administración del servicio público Registral Gestión Financiera

No Conformidad Real: Incumplimiento de un norma o requisito.
No Conformidad Potencial: Situación identificada, que puede dar lugar al incumplimiento de una norma o a la materialización de un riesgo.

7. CONCLUSIONES

De acuerdo con los 35 criterios evaluados, se cumplió con el 17% (seis); a continuación, se presentan los resultados consolidados del cumplimiento evidenciado en las pruebas y recorridos físicos a las Oficinas de Registro de Instrumentos Públicos de Manizales, Popayán y Bucaramanga, entre los meses de octubre y noviembre del 2022.

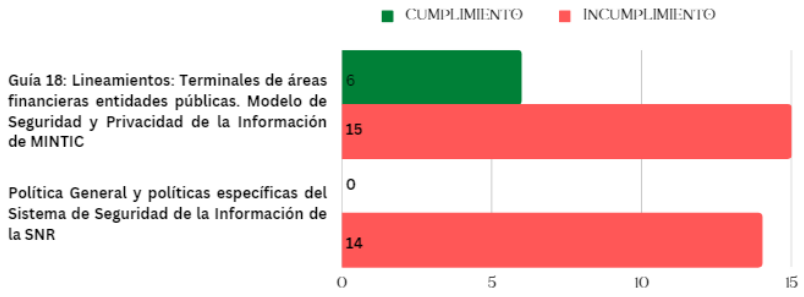

Ilustración 3: Resultado de los incumplimientos de los criterios evaluados.

Así mismo, se relacionan las recomendaciones mas relevantes:

- Desarrollar mesas de trabajo con Gestión Documental para que las Oficinas de Registro de Instrumentos Públicos que no cuentan con IRIS documental puedan tener el beneficio la custodia de la información y la reducción del riesgo de corrupción que puede existir en cuanto al manejo de la información de manera manual.
- A fin de mejorar y fortalecer la identificación de riesgos y el diseño de los controles, para prevenir, mitigar y evitar su materialización, en los procesos adscritos a las mismas, se recomienda considerar la posibilidad de realizar un análisis de contexto por cada Oficina de Registro, teniendo en cuenta la variación en la operatividad y las causas.

- Emitir una directriz desde la alta gerencia, con el fin de fortalecer la custodia de claves y dispositivos de acceso a los sistemas de información.
- Capacitar sobre la seguridad de la información y las medidas que deben adoptar los roles de contador y coordinador del grupo tecnológico y financiero, para mitigar los riesgos de fraude financiero.
- Potencializar las acciones que llevan a construir un control Interno eficaz en la aplicación de controles y procedimientos que dan cumplimiento a las políticas específicas de seguridad de la información.
- Establecer actividades de monitoreo y control a las situaciones de advertencia que pueden materializar riesgos que afecten la seguridad de la información
- Establecer procedimientos de aprovisionamiento y des aprovisionamiento de usuarios cuando ocurran situaciones que implican cambios o terminación de perfiles de acceso de los usuarios.
- Fomentar en la entidad formación de una cultura de control que contribuya at mejoramiento continuo para identificar oportunidades de mejora en los sistemas misionales de la entidad.
- Alinear las instrucciones dadas por el área misional junto con la preservación de la seguridad de la información que se encuentra en los sistemas de información misionales de la entidad.
- Para la Oficina de Registro Instrumentos Públicos Principal de Manizales se recomienda asignar un apoyo permanente que realice las actividades de soporte y gestión a la infraestructura tecnológica, para da respuesta a las necesidades de tecnología.

Cordialmente,

RITA CECILIA COTES COTES
Jefe Oficina de Control Interno de Gestión

Proyectó: Equipo Auditor OCI: Nayibe Barreto/ Johanna Gómez