

**AUDITORÍA INTERNA SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACION
SOLEDAD****INFORME DE AUDITORÍA**

Nombre Sistema y/o Proceso Auditado:	Sistema de Gestión de la Seguridad de la Información
Responsable del Sistema y/o Proceso:	Ing. Leyla Soraya Guzmán
Auditor Líder y Equipo:	Ing. Yaneth Constanza Rincón Ing. Sandra Rocio Castro Cruz
Funcionarios Entrevistados:	Dra. Trischa Thinna Toledo Kasimir
Fecha Realización Auditoría:	12 y 13 de Septiembre del 2022
Fecha Entrega Informe:	14 de Octubre de 2022

1. OBJETO DE LA AUDITORÍA

Identificar oportunidades para mejorar el sistema de gestión de seguridad de la información entorno a la política de seguridad de la información, generando valor agregado a la gestión de la Superintendencia de Notariado y Registro y recomendaciones al sistema.

2. ALCANCE DE LA AUDITORÍA

Validar el cumplimiento de la política General y específica del Sistema de Gestión de Seguridad de la información de la SNR, adoptada mediante Resolución No. 06416 de julio 13 de 2021.

3. CRITERIOS DE LA AUDITORÍA

Política General y específicas del Sistema de Gestión de Seguridad de la Información, la NTC-ISO-IEC-27001:2013, aspectos generales de MIPG y MSP

4. VERIFICACIÓN DE LAS IMPLEMENTACIÓN DE ACCIONES CORRECTIVAS Y/O PREVENTIVAS DE AUDITORIAS ANTERIORES:

Se realizó la verificación de acciones correctivas y/o preventivas

5. INFORME DE AUDITORÍA:

• Informe verificación de cumplimiento de la política General y políticas específicas del sistema de Seguridad de la información. (ISO 27001:2013).

Superintendencia de Notariado y Registro

Calle 26 No. 13 - 49 Int. 201

PBX 57 + (1) 3282121

Bogotá D.C., - Colombia

<http://www.supernotariado.gov.co>

correspondencia@supernotariado.gov.co

Metodología:

La auditoría se lleva a cabo conforme a lo establecido en el plan de Auditoria, tanto en su programación, como en la participación del equipo de Auditoria:

Se socializa en el Despacho de la Oficina de Registro Seccional de Soledad Atlántico, el objetivo, alcance y criterios de la Auditoria de la Seguridad de la Información

Para el levantamiento de la información y posterior análisis de la situación actual de seguridad de la información en la Superintendencia de Notariado y Registro, se realizaron: entrevistas y visitas en sitio a los responsables, revisión de la información, el manejo de los diferentes sistemas de información. Con el análisis respectivo de algunas políticas de la SGSI como el control de acceso, política de equipos, política de teletrabajo, áreas seguras entre otras.

Durante el Desarrollo:

Se realiza la presentación sobre los conceptos de seguridad de la información y la aprobación de la política general y políticas específicas del Sistema de Gestión de Seguridad de la información con soporte de acta de inicio y cierre a través de una socialización donde igualmente se explica la ubicación en el portal web de la política del SGSI, alcance, justificación y estructura de la norma ISO 27001:2013.

Identificación de los procesos misionales.

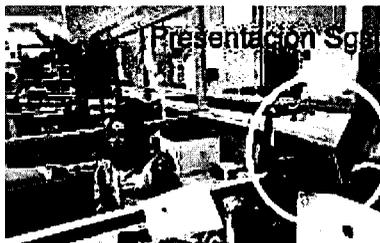
Revisión de la documentación y procesos relacionados con la política del SGSI y la norma ISO 2700:2013, con el fin de identificar y valorar el cumplimiento de las políticas del SGSI.

Se socializa por grupos en el siguiente orden:

Primer Grupo: Despacho

Segundo Grupo: Jurídica y Administrativa.

Tercer Grupo: Liquidación.



Fuente: Equipo Auditor en Orip

Dominio de la Política y actividades realizadas por el grupo auditor:

Superintendencia de Notariado y Registro

Calle 26 No. 13 - 49 Int. 201

PBX 57 + (1) 3282121

Bogotá D.C., - Colombia

<http://www.supernotariado.gov.co>

correspondencia@supernotariado.gov.co

Política Uso de Internet:

Se revisa aleatoriamente el historial de cada equipo de cómputo, se realiza pruebas a las diferentes páginas de redes sociales como facebook, youtube, que pueden afectar el tráfico de la Red, verificando su acceso restringido y el análisis del test de velocidad del operador de internet observando la posible mejora en la que actualmente trabaja la Oficina de Tecnología de la Información con el proveedor. Se verifica que no exista software instalado no autorizado.

Política de la seguridad de la información:

Se pregunta a diferentes funcionarios de la Orip si tienen el conocimiento de la política de SGSI y su ubicación identificando el desconocimiento de los funcionarios motivo por el que el equipo auditor realiza socialización de la política de seguridad de la información, mediante la presentación de apertura en power point, donde se explica el objetivo, alcance, criterios y algunas políticas específicas de la Seguridad de la información, mencionando casos reales y/o ejemplos de vulneración de la seguridad de la información, mencionando igualmente la resolución N° 06416 de 2021 *"Por el cual se adopta la Política general y Específicas del Sistema de Gestión de Seguridad de la Información de la Superintendencia de Notariado y Registro"*.

Política de Gestión Uso de Activos de la Información:

Se verifica en los pc que tipo de información almacenan, así como las herramientas que están usando para guardar la información.

Política para la Realización de Copias en estaciones de trabajo de usuario final:

Se observa el control en caso de usar discos externos, memorias, cd entre otros.

Política de Seguridad física y del entorno:

Se verifica la seguridad física de los servidores y cableados, las canaletas de los puntos de red para su correcto funcionamiento

Política de seguridad de centros de datos y conectividad:

Se revisa si los puntos de red están dentro de un rack.

Se verifica el uso de puertos usb que se encuentren inactivos para los usuarios no autorizados con el propósito de no extraer información de los equipos, el mal uso de los sistemas de la información.

Las condiciones físicas del centro de cómputo, se revisa la fecha de los extintores y el estado de los aires acondicionados

Política de Escritorio y pantalla limpia:

Se verifica si dejan claves anotadas, bloqueo de pantalla, escritorio limpio

Superintendencia de Notariado y Registro

Calle 26 No. 13 - 49 Int. 201

PBX 57 + (1) 3282121

Bogotá D.C., - Colombia

<http://www.supernotariado.gov.co>

correspondencia@supernotariado.gov.co

Política de Control de acceso:

Se verifica el reporte de los usuarios activos que coincida con el personal que está laborando actualmente. Gestión de Roles

Uso de Contraseñas, las cuales se recomienda cambiar periódicamente las claves, y que no sean tan vulnerables.

Se verifican que los pc estén vinculados al dominio, se solicita a la Registradora listado de usuarios activos, se verifica que no tengan las claves guardadas al ingresar a los sistemas misionales.

Aspecto Conforme: Los equipos de Cómputo se encuentran vinculados al dominio.

6. HALLAZGOS (fortalezas, conformidades, no conformidades y oportunidades de mejora)

Fortalezas

1. Se resalta la disposición participación de algunos funcionarios de la Oficina de Registro de instrumentos Públicos de Soledad, para atender la visita y todas las recomendaciones que se allí se derivan.
2. La Oficina tuvo muy buena disposición en conocer la Política de Seguridad de la Información y su aplicabilidad.

Observación 1: Se observa archivo físico (Gestión Documental) con información de la SNR debido a que no se ha realizado la transferencia primaria; adicionalmente se observa en sitio la existencia del archivo físico en un lugar de acceso restringido debido a la existencia de artefactos eléctricos los cuales son un riesgo laboral; de seguridad y salud en el trabajo y de seguridad de la información en la ORIP, por otra parte en el mismo lugar se observa alimento con veneno para roedores ya que se ha encontrado en el lugar la existencia de uno de estos animales.

Por esta razón no se da cumplimiento a la política denominada "**Política de seguridad física**" y la "**Política retención y archivo de datos**" que se referencian dentro de las políticas general y específicas del sistema de seguridad de la información de la SNR.

Superintendencia de Notariado y Registro

Calle 26 No. 13 - 49 Int. 201

PBX 57 + (1) 3282121

Bogotá D.C., - Colombia

<http://www.supernotariado.gov.co>

correspondencia@supernotariado.gov.co



Fuente: Equipo Auditor en Orip en archivo físico de la ORIP

Recomendación:

Gestionar la transferencia primaria que se encuentra en la ORIP con el Grupo de gestión documental de Nivel Central con el propósito de adelantar la gestión de almacenamiento en bodega correspondiente, dándole así la importancia y cuidados de la seguridad de la información física y/o digital. Solicitar a la ARL alguna inspección de seguridad física en la ORIP.

Observación 2: Debilidad en controles de Seguridad de las instalaciones físicas y del cableado: En el cuarto de cómputo se evidencian aspectos que representan riesgos en cuanto al acceso de personal no autorizado y para la seguridad física en el rack de red.



Fuente: Equipo Auditor en Orip – Cuarto de computo

Falta mantenimiento de cableado de redes debido a la existencia de polvo, cables sin etiquetado, y sin peinar. Motivo por el que no se da cumplimiento a las políticas general

Superintendencia de Notariado y Registro

Calle 26 No. 13 - 49 Int. 201
PBX 57 + (1) 3282121
Bogotá D.C., - Colombia
<http://www.supernotariado.gov.co>
correspondencia@supernotariado.gov.co

y específicas del SGSI de la SNR: "*políticas de seguridad física; políticas de seguridad del centro de datos y centros de cableado; políticas de seguridad de los equipos informáticos*", así como al incumplimiento de los objetivos de control de la Norma ISO 27001: 2013 del numeral "*A.11 Seguridad física y del entorno*".

Recomendación:

Se recomienda realizar una verificación o reportar a la mesa de ayuda la situación actual con los cables de datos, se evidencia desorden en el Rack de comunicaciones, poniendo en riesgo la operación en caso de ser desconectado algún cable no identificado. Se sugiere la organización del cuarto de datos y cableado. Socializar e implementar las políticas de seguridad física; políticas de seguridad del centro de datos y centros de cableado; políticas de seguridad de los equipos informáticos.

Se recomienda llevar un control de acceso, a las diferentes áreas delimitadas, como por ejemplo el área de sistemas, no cuenta con un control de acceso, y su ingreso no es controlado por personal interno y visitantes.

Se recomienda que, al ingresar portátiles, sean registrados en una bitácora al ingresar y salir de las instalaciones de la oficina.

Implementar el formato llamado "*Formato de ingreso y salida del datacenter snr*" del procedimiento "*Ingreso de elementos tecnológicos en los centros de cómputo OTI*". Llevando un control de acceso a las instalaciones de la Oficina de Registro mediante el registro en una bitácora para el ingreso o salida de equipos de cómputo, donde quede registro de la persona que ingresa o retira el activo incluyendo la serie del equipo.

Superintendencia de Notariado y Registro

Calle 26 No. 13 - 49 Int. 201

PBX 57 + (1) 3282121

Bogotá D.C., - Colombia

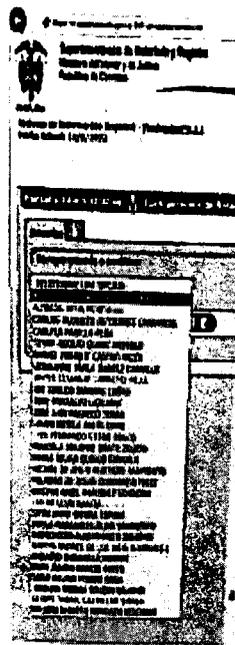
<http://www.supernotariado.gov.co>

correspondencia@supernotariado.gov.co

vacaciones, licencias entre otros, ni se evidencian reportes de solicitud a la mesa de ayuda para gestionar dichas actividades, las cuales se deben realizar por medio del formato de administración de usuarios, ya que no se está enterando oportunamente de las diferentes novedades para ajustar los diferentes sistemas de información quedando usuarios activos después de varios meses de su retiro.

No se evidencia un control respecto a los usuarios asignación de roles, y no se eliminan los privilegios asignados de los cargos anteriores.

Por otra parte no se evidencia documento oficial donde se autorice la asignación de segregación de funciones para la utilización de los sistemas misionales (SIR-Iris).



Fuente: Equipo auditor en Orip

Incumpliendo lo establecido en la "política de control de acceso" ubicada dentro de las políticas general y específicas de seguridad de la información de la SNR.

Recomendación:

Se debe llevar un proceso para el registro y cancelación de usuarios y el diligenciamiento del formato de activación y desactivación de usuarios, donde se notifiquen a la mesa de ayuda Sir e iris

El registro de la asignación de roles debe quedar documentado y autorizado por cada dueño de proceso.

Superintendencia de Notariado y Registro

Calle 26 No. 13 - 49 Int. 201

PBX 57 + (1) 3282121

Bogotá D.C., - Colombia

<http://www.supernotariado.gov.co>

correspondencia@supernotariado.gov.co

No se cuenta con una persona que este pendiente de la administración de los usuarios de los sistemas misionales.

Observación 4: Debilidad en escritorio limpio



Fuente: Equipo auditor en Orip

Se evidencia en los pc que no están despejados en el escritorio digital e igualmente en Escritorio físico estos últimos presentan congestión en la documentación confidencial y la seguridad de estos activos de información que se encuentran vulnerables a los diferentes funcionarios internos, externos como el personal no autorizado que se observó los días de atención al público (Martes y Jueves). Por esta razón no hay cumplimiento a la "**política de escritorio y pantalla limpia**"

No existe conciencia por cuidar la integridad de la información, ya que dejan los equipos prendidos con el usuario abierto al terminar la jornada laboral.

Recomendación:

Se recomienda no anotar las claves en papeles, o guardarlas en el escritorio. Mantener el escritorio limpio de documentos confidenciales que puedan ser manipulados y transportados y bloquear los pc al retirarse de los puestos de trabajo.

Observación 5: Debilidad en el almacenamiento de la información



Fuente: Equipo auditor en Orip

Se evidencia la utilización de memorias en funcionarios autorizados, que pueden afectar la seguridad de los pc.

Superintendencia de Notariado y Registro

Calle 26 No. 13 - 49 Int. 201
PBX 57 + (1) 3282121
Bogotá D.C., - Colombia
<http://www.supernotariado.gov.co>
correspondencia@supernotariado.gov.co

Se evidencia que la protección de los activos de información se encuentra vulnerable por manejo de dispositivos externos tales como memorias usb, discos duros, debido a que almacenan la información de la ORIP en dichos dispositivos, no haciendo uso de herramientas seguras como la herramienta disponible en la entidad denominada One drive, como mecanismo de almacenamiento para la protección del activo de la información.

Lo anterior afectando el cumplimiento del dominio A.12.3 "**Copias de Respaldo**" del Anexo A de la ISO 27001 y de la política general y específica de la SNR "**política para realización de copias en estaciones de trabajo de usuario final**".

Recomendación:

No anotar las claves en papeles, o guardarlas en el escritorio, Mantener el escritorio físico y digital (PCs) limpio de documentos confidenciales que puedan ser manipulados y transportados por personas no autorizadas.

Se recomienda no usar discos externos para realizar backucps, o copiar en el disco interno de los computadores.

Se recomienda el uso del one drive, como mecanismo de almacenamiento para la protección del activo de la información.

7. CONCLUSIÓN DE LA AUDITORÍA

Es necesario implementar la política de seguridad de la información que se encuentra aprobada y publicada en el portal Web, con la resolución N° 06416 del 13 de julio de 2021 y hacer énfasis a los usuarios finales, sobre las restricciones de seguridad para la descarga e instalación de posibles aplicativos no autorizados por la Oficina de Tecnología de la Información, que pueden llegar a poner en riesgo la seguridad de la información.

Es necesario nombrar un funcionario interno que se encargue de la supervisión y la mejora continua de la política de seguridad de la información.

ADECUACIÓN:

Para el Sistema de Gestión de Seguridad de la Información - SGI de la **Oficina de Registro de Soledad** se identifican oportunidades de mejora por medio de observaciones, con el propósito de cumplir con los requisitos establecidos NTC-ISO 27001:2013 y aspectos generales de las políticas general y específicas de seguridad de la información que le aplican a la ORIP.

Superintendencia de Notariado y Registro

Calle 26 No. 13 - 49 Int. 201

PBX 57 + (1) 3282121

Bogotá D.C., - Colombia

<http://www.supernotariado.gov.co>

correspondencia@supernotariado.gov.co

PERTINENCIA:

El SGSI de la ORIP, en el **Proceso de la Auditoria**, se evidencia su alineación a la misión y visión de la SNR, mediante el cumplimiento de los requisitos legales, y la aplicabilidad de los valores y principios institucionales. Para esto se socializa y se refuerza la importancia y los conceptos del Sistema de Gestión de Seguridad de la Información, los cuales aportan al cumplimiento de los objetivos de la entidad.

EFICACIA:

El SGSI de la ORIP, en el **Proceso de la Auditoria**, muestra capacidad para alcanzar las metas trazadas, donde se pudo evidenciar que se puede mejorar en el conocimiento para el seguimiento, medición, análisis y evaluación realizada por el equipo de trabajo demostrando por medio de sus funciones que se puede cumplir con una debida planificación de resultados y salvaguardando este recurso valioso de la información física y digital de la entidad aplicando los tres pilares del sistema SGSI (Confidencialidad, integridad y disponibilidad).

Cordialmente,



Trischa Thinna Toledo Kasimir

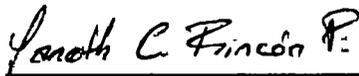
REGISTRADORA SECCIONAL (E) OFICINA DE REGISTRO DE SOLEDAD- ATLÁNTICO

Equipo Auditor:

Sandra Castro Cruz

Sandra Rocio Castro Cruz

Profesional Esp. Oficina Tecnologías de la Información



Yaneth Constanza Rincón Pulido

Profesional Esp. Oficina Tecnologías de la Información

Superintendencia de Notariado y Registro

Calle 26 No. 13 - 49 Int. 201

PBX 57 + (1) 3282121

Bogotá D.C., - Colombia

<http://www.supernotariado.gov.co>

correspondencia@supernotariado.gov.co