AUDITORÍA INETRNA SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION
INFORME DE AUDITORÍA

Nombre Proceso Auditado:	Política de Seguridad de la Información.
Responsable del Proceso	Carlos Augusto Hoyos Peláez Registrador Seccional.
Auditor Líder y Equipo:	Leyla Zoraya Guzmán Rodríguez Jeiffe Jubelly Muñoz Robayo
Funcionarios y/o Contratistas Entrevistados:	Carlos Augusto Hoyos Peláez Valentina Garcés Usma – Contratista Laura Cristina Parra bedoya – Funcionaria.
Fecha Realización Auditoría:	12 y 13 de septiembre de 2022
Fecha Entrega Informe:	13 de septiembre 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

La NTC-ISO-IEC-27001:2013, aspectos generales de MIPG y MSPI. Política de seguridad de la Información.

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

La Oficina de Registro Instrumentos Públicos de Jericó no ha recibido visitas de seguimiento relacionadas con la seguridad de la información, razón por la cual no cuenta con planes de mejoramiento producto de auditorías o visitas internas y/o externas, lo anterior, dado que no ha sido visitada por algún Ente o de Dependencia de control; tampoco tiene planes de mejoramiento de seguridad de la información. Lo

anterior, en atención a que la SNR se encuentra incursionando en el proceso de implementación del Sistema de Gestión de Seguridad de la Información.

5. INFORME DE AUDITORÍA:

Siendo las 2 de la tarde del día 12 de septiembre del 2022, se da inicio a la auditoria del Sistema de Gestión de Seguridad de la Información entorno a la política de seguridad de la información, en la cual participaron el señor registrador y el equipo auditor. En dicha reunión se explicó la metodología a utilizar en el desarrollo de la auditoría, la cual consiste en realización de entrevistas con los ejecutores de los procesos, revisión física- técnica y como mecanismo evidencial se optó por el registro fotográfico.

Se realizó la socialización de la política de seguridad a todos los funcionarios de la Oficina de Registro, donde se hizo énfasis en la oportunidades para mejorar el sistema de gestión de seguridad de la información entorno a la política de seguridad de la información, para generar valor agregado a la gestión de la Superintendencia de Notariado y Registro.

En dicha socialización se informa sobre la importancia de la implementación del Sistema de Gestión de Seguridad de la información enfocando en la Política de Seguridad de la Información resaltando la Justificación, Objetivos, Alcance y políticas específicas como: Uso de correo electrónico, Trabajo en casa, uso de activos de información, uso de internet, Control de acceso y manejo de claves, Seguridad física y de entorno, Escritorio limpio, Realización de copias de seguridad, entre otras.

Adicionalmente, se explica la ubicación en el organigrama de la Oficia de Tecnología de la información por ser la encargada de la implementación del sistema de seguridad, indicando que ésta se encuentra en el nivel directivo, así mismo, se explica la ubicación de los Sistemas Integrados de Gestión en mapa de procesos de la Entidad.

Se explican con ejemplos los conceptos de los pilares de la información; Confidencialidad, Integridad y Disponibilidad.

Así mismo, se explica sobre activos de información y su clasificación según la ley 1712 de 2014: Información Clasificada, Información Reservada e Información Pública.

Se expone acerca de la integración del Modelo Integrado de Planeación y Gestión – MIPG, la NCT ISO 27001 y el Modelo de Seguridad de la Información. Así como el marco normativo que regla la implementación de dicho sistema.

Se dio a conocer el procedimiento de gestión de incidentes de seguridad. Se explicaron conceptos de relacionados con activos de información, la clasificación de la información según la ley de transparencia 1712 del 2014.

Durante la visita se realiza socialización de la importancia del cumplimiento de las Políticas de Seguridad de la Información y sus objetivos, recomendando su consulta periódica en la página web de la SNR y participación activa en la campaña de "Hoy es Miércoles de Política" la cual es enviada al todos los correos institucionales desde Somos SNR, con el fin de cumplir el *numeral 5.2 "Política", y 6.2 "Objetivos de Seguridad de la información y planes para lograrlos " de la Norma ISO 27001: 2013 por parte de las dependencias responsables.*

Así mismo, se explicaron conceptos básicos de riesgos de seguridad de la información, tratamiento de riesgos e implementación de controles. Norma *ISO27001:2013 Anexo A- 6.1 "ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES".*

Se explicó la política de uso del correo institucional, haciendo énfasis que el mismo es de exclusivo para fines institucionales, no enviar ni recibir información personal por éste medio. *"Política general y especifica de Seguridad de la Información de la SNR. Adoptada mediante resolución No. 06412 del 13 de julio de 2022".*

Se explicó detalladamente y con ejemplos la política de acceso y contraseñas. Haciendo énfasis en no prestar las contraseñas de acceso de ningún sistema de información y/o aplicación Institucional. Así mismo, se explicaron las consecuencias de compartir las claves de acceso al Sistema de Folio Magnético. Norma ISO27001:2013 Anexo A - A.9 "CONTROL DE ACCESO" 7.5.3 Control de la información documentada" y . Política general y específica de Seguridad de la Información de la SNR. Adoptada mediante resolución No. 06412 del 13 de julio de 2022."Política de establecimiento, uso y protección de claves de acceso".

Los servidores públicos auditados tienen identificado las responsabilidades en la ORIP. Sin embargo, los funcionarios manifiestan no haber recibido inducción en temas asociados a seguridad de la información.

No hubo restricciones, impedimento o imposibilidad de realizar la auditoria *in-situ*. La auditoría se realizó de manera presencial y fue atendida por el señor registrador.

La Oficina de Registro de Jericó cuenta con cuatro (4) funcionarios, que cumplen con las funciones asignadas, entre los cuales se encuentran funcionarios de planta y contratistas.

Nombre	Apellido 1	Apellido 2	Cargo Actual	Código	Grado
CARLOS AUGUSTO	HOYOS	PELAEZ	Registrador Seccional	0192	10
LAURA CRISTINA	PARRA	BEDOYA	Auxiliar Administrativo	4044	16
GLORIA PATRICIA	RESTREPO	RUIZ	Auxiliar Administrativo	4044	16
VALENTINA	GARCES	USMA	Contratista		
LINA MARLLORI	BEDOYA	CARBAJAL	Servicios Generales		

Existió permanente retroalimentación entre el equipo auditor y el equipo auditado para socializar las oportunidades de mejora identificadas.

Se da cumplimiento a la planificación de la auditoria desarrollando lo programado en el plan de auditoría general y diario. De otra parte, se desarrolló la visita acorde con la lista de chequeo, utilizando las preguntas predefinidas en la metodología.

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

Fortalezas:

1. Se resalta la disposición de los funcionarios que laboran en la Oficina de Registro de Instrumentos Públicos de Jericó para atender la auditoría y todas las recomendaciones que de allí se derivan. Se observa receptividad en la socialización de la Política de seguridad de la información.

2. Los funcionarios y contratistas de la ORIP manifiestan conocer el procedimiento de baja de equipos e inservibles.

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

4. No se evidencio, durante el desarrollo de la auditoria, la problemática *de los tramitadores* en las afueras de las instalaciones de la ORIP, que represente una amenaza a la seguridad de la información.

5. Se encuentra en el tapiz de los computadores la información relacionada con la seguridad de la información y el procedimiento para gestionar los incidentes de seguridad.

No conformidades:

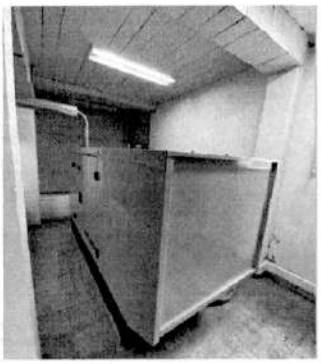
1. La Oficina de registro de Jericó cuenta con la infraestructura física necesaria para la operación de los procesos y lograr la conformidad de los productos y servicios, la infraestructura física es suficientemente amplia y adecuada para la prestación del servicio. No obstante, se evidenciaron goteras que generan humedades, las cuales podrán representar riesgos para la conservación de la documentación física. Norma *ISO27001:2013 Anexo A.*"A.11 *SEGURIDAD FÍSICA Y DEL ENTORNO*".

2. Los funcionarios manifestaron desconocer la política general y especifica de seguridad de la información. Norma ISO27001:2013 Anexo A. – "*4.1 CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO*". *Y "Política general y específica de Seguridad de la Información de la SNR. Adoptada mediante resolución No. 06412 del 13 de julio de 2022".*

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

3. Los extintores se encuentran vencidos, lo cual representa un riesgo que afecta la disponibilidad de la información, tanto física como digital, en caso de presentarse un incendio en las instalaciones de la Oficina de Registro.

4. La planta eléctrica se encuentra averiada y fuera de servicio. No existe UPS, lo cual afecta uno de los tres componentes de la triada de la información, como es la disponibilidad de la información al usuario en caso de presentarse cortes de energía.

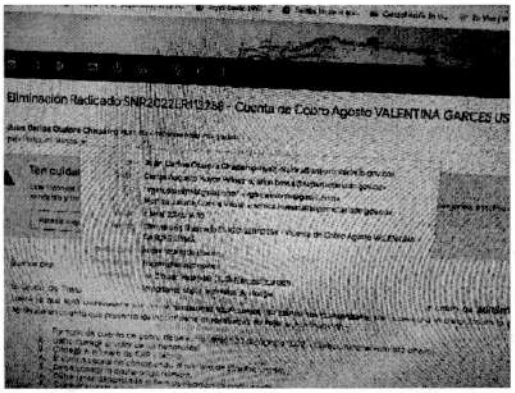


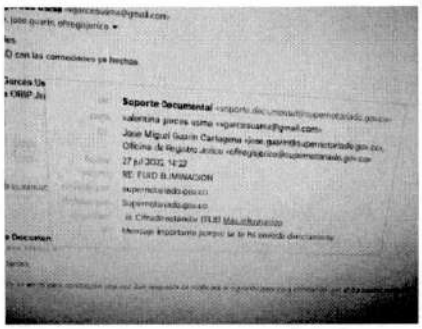
5. Existen en el sistema de información registral SIR, funcionarios activos a pesar de estar retirados definitivamente de la Entidad. Situación que genera incumplimiento de la *Norma ISO27001:2013 Anexo A - "A.9 CONTROL DE ACCESO - A.9.2 Gestión de acceso de usuarios". Y política general y especifica de seguridad de la Información de la SNR, adoptada mediante resolución No. 06412 del 13 de julio de 2022 - Política de establecimiento, uso y protección de claves de acceso".*

6. Se evidencia que los funcionarios y/o contratistas se prestan los usuarios. *Norma ISO27001:2013 Anexo A - "A.9 CONTROL DE ACCESO - A.9.2 Gestión de acceso de usuarios". Y política general y especifica de seguridad de la Información de la SNR, adoptada mediante resolución No. 06412 del 13 de julio de 2022 - Política de establecimiento, uso y protección de claves de acceso".*

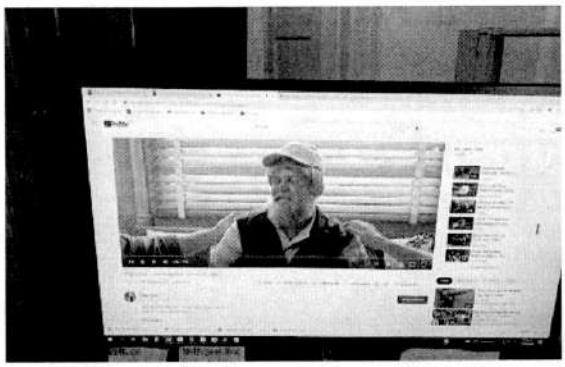
Superintendencia de Notariado y Registro
Calle 26 No. 13 - 49 Int. 201
PBX 57 + (1) 3282121
Bogotá D.C., - Colombia
http://www.supernotariado.gov.co
correspondencia@supernotariado.gov.co

7. Los contratistas y personal de gestión documental de la SNR utilizan el correo personal para envío y/o recepción de información institucional.





8. Existen funcionarios que acceden a páginas no autorizadas por 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

7. CONCLUSIÓN DE LA AUDITORÍA

RECOMENDACIONES:

1. Acceder a la política de seguridad de la Información publicada en el portal Web de la Entidad y dar aplicabilidad a la misma.
2. Tener presente que las políticas de seguridad de la información de la Entidad son de obligatorio cumplimiento tanto para funcionarios, contratistas pasantes, proveedores y todo personal que se encuentre vinculado de alguna manera a la Entidad.
3. Gestionar la recarga de los extintores.
4. Desactivar en el Sistema SIR, los funcionarios que se retiran de forma temporal o definitiva de la Oficina de Registro.
5. Reiterar a los funcionarios que las claves de acceso para acceder a los sistemas de información y/o correo electrónico son de uso personal e intransferible.
6. Gestionar ante el nivel central la creación del correo institucional a la contratista.
7. Continuar gestionando ante el nivel central la reparación de la planta eléctrica, suministro de una UPS y reparación de las goteras en la Oficina.
8. Recordar a los funcionarios que no se deben usar los correos personales para uso de información institucional y el correo institucional es para uso exclusivo de información de la Entidad.

Carlos Augusto Hoyos Peláez Registrador Seccional	**Leyla Zoraya Guzmán Rodríguez** Auditor Líder
Jeiffe Jubelly Muñoz Robayo 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