OFICINA DE CONTROL INTERNO

INFORME EJECUTIVO DE AUDITORÍA

AUDITORÍA AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA PROCURADURÍA GENERAL DE LA NACIÓN

JEFE OFICINA CONTROL INTERNO:	**MAGDA PATRICIA MORALES SÁENZ**
AUDITORA:	**SANDRA DEL PILAR CHUQUÍN BADILLO**
LUGAR Y FECHA AUDITORÍA:	**BOGOTÁ D.C., 11 AL 16 DE DICIEMBRE DE 2019**
FECHA DEL INFORME:	**27 DE MAYO DE 2020**

TABLA DE CONTENIDO

Pág.

RESUMEN EJECUTIVO

La Oficina de Control Interno, en cumplimiento de las funciones establecidas por el artículo 13 del Decreto Ley 262 de 2000, ejerce control de gestión sobre las actividades que adelantan las dependencias de la Procuraduría General de la Nación (PGN), realizando la evaluación independiente. En tal sentido, se programó auditoría al Sistema de Información de Gestión de Seguridad de la Información - SGSI.

La Procuraduría General de la Nación adoptó el Sistema de Gestión de Seguridad de la Información mediante Resolución No. 036 de 2009 y la Política de Seguridad con la Resolución No. 910 de 2019. Ha llevado a cabo el diagnóstico, planificación e implementación del Sistema y de controles que propenden por la seguridad de la información.

La valoración para la presente auditoría se realizó utilizando como referencia la Norma NTC-ISO/IEC 27001:2013, verificando el cumplimiento de los requisitos y la implementación de controles del Anexo A de la Norma precitada, relacionados con: Políticas de seguridad de la Información (A5), Organización de la Seguridad de la Información (A6), Control de acceso (A9) y Seguridad Física y del Entorno (A11).

Como resultado de la auditoría se identificaron quince (15) Conformidades, dos (2) No Conformidades, ocho (8) Observaciones, y tres (3) Oportunidades de mejora.

1. OBJETIVO

Verificar el Sistema de Gestión de Seguridad de la Información – SGSI de la Procuraduría General de la Nación, con el fin de determinar si los objetivos de control, controles, procesos y procedimientos:

- Cumplen los requisitos de la norma NTC-ISO/IEC 27001 y de la legislación o reglamentaciones pertinentes.
- Cumplen los requisitos identificados de seguridad de la información.
- Están implementados y se mantienen eficazmente
- Se están ejecutando en forma consistente y conforme con la Política de Seguridad de la Información de la Procuraduría General de la Nación.

2. ALCANCE

La auditoría al Sistema de Gestión de Seguridad de la Información cubrió los requisitos de la norma NTC-ISO/IEC 27001:2013 y los objetivos de control y controles del Anexo A, relacionados con: Políticas de Seguridad de la Información (A5), Organización de la Seguridad de la Información (A6), Control de acceso (A9), y Seguridad Física y del Entorno (A11).

La verificación se realizó en la ciudad de Bogotá D.C. en las sedes de la Torre A, B y C y Edificio Manuel Mejía, entre el 11 y el 16 de diciembre de 2019.

3. CRITERIOS DE AUDITORÍA

Esta auditoría se realiza con fundamento en:

- Inciso 2º del artículo 209 y 267 de la Constitución Política.
- Artículo 12 de la Ley 87 de 1993[1].
- Decreto-Ley 262 de 2000[2].
- Resolución No. 036 de 2009[3].
- Resolución No. 861 de 2019[4].

[1] Por el cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones.
[2] Por el cual se modifican la estructura y la organización de la Procuraduría General de la Nación y del Instituto de Estudios del Ministerio Público; el régimen de competencias interno de la Procuraduría General; se dictan normas para su funcionamiento; se modifica el régimen de carrera de la Procuraduría General de la Nación, el de inhabilidades e incompatibilidades de sus servidores y se regulan las diversas situaciones administrativas a las que se encuentren sujetos.
[3] Por medio de la cual se adopta el Sistema de Gestión de la Seguridad de la Información -SGSI - de la Procuraduría General de la Nación.
[4] Por medio de la cual se adopta la actualización del Modelo Estándar de Control Interno - MECI y se dictan otras disposiciones.

- Resolución No. 910 de 2019[5].
- Mapa de Riesgos Institucional[6]
- Guía GTC-ISO 19011:2018[7].
- Políticas de seguridad, procedimientos, formatos, instructivos, registros y demás documentos que hayan sido definidos por la Entidad en el SGSI.

4. RESULTADOS DE LA AUDITORÍA

4.1 Conformidades

1. Se evidencia que existe conocimiento de la organización, el contexto y se comprenden las necesidades de las partes interesadas, las cuales se encuentran plasmadas en el numeral 2 del documento “Manual Sistema de Gestión de Seguridad de la Información”, el cual fue un entregable del contrato 179-089-2018; no obstante, éste se encuentra con control de cambios y no es definitivo; sin embargo, para efectos de la auditoría se considera conforme con los numerales 4.1 y 4.2 de la Norma NTC-ISO/IEC 27001:2013, por haberse realizado el análisis y determinación de los mencionados ítems.

2. Se evidencia, plasmado en el numeral 2 del anexo de la Resolución No. 910 de 2019, la definición del alcance del Sistema de Gestión de Seguridad de la Información, siendo conforme con el numeral 4.3 de la Norma NTC-ISO/IEC 27001:2013.

3. El Sistema de Gestión de Seguridad de la Información fue adoptado mediante la Resolución No. 036 de 2009. Con el contrato 179-089-2018 se llevó a cabo el diagnóstico, planificación e implementación del Sistema de Gestión de Seguridad de la Información de la Procuraduría General de la Nación, observándose conformidad con el numeral 4.4. de la Norma NTC-ISO/IEC 27001:2013.

4. Mediante la Resolución No. 910 de 2019 se adopta la Política de Seguridad de la información de la Procuraduría General de la Nación y en el anexo de la misma se hace referencia al liderazgo y compromiso de la alta dirección, observándose conformidad con los numerales 5.1 y 5.2 de la Norma NTC-ISO/IEC 27001:2013.

5. Se evidencia que la Entidad determina riesgos de seguridad de la información, lleva a cabo la valoración y realiza el tratamiento a los mismos, según lo plasmado en el documento “190408-Mapa-Riesgos-PGN.pdf” publicado en la opción de transparencia del portal institucional, siendo conforme con los numerales 6 y 6.1 de la Norma NTC-

[5] Por medio de la cual se adopta la Política de Seguridad de la Información de la Procuraduría General de la Nación.
[6] https://www.procuraduria.gov.co/portal/media/file/190408-Mapa-Riesgos-PGN.pdf
[7] Directrices para la auditoría de los Sistemas de Gestión.

ISO/IEC 27001:2013.

6. Los objetivos de la seguridad se encuentran plasmados en la Política de Seguridad adoptada mediante Resolución No. 910 de 2019, son coherentes y comunicados, observándose conformidad con el requisito 6.2 de la Norma NTC-ISO/IEC 27001:2013; sin embargo, existen debilidades que deben ser atendidas.

7. Se evidencia que, han sido asignados recursos para el diagnóstico, planificación e implementación del Sistema de Gestión de Seguridad de la Información; así como, para actividades de sensibilización, adquisición de herramientas informáticas de seguridad mediante contratos 179-089-2018, 179-130-2019 y 179-266-2019. También se cuenta, en la Oficina de Sistemas, con un grupo de funcionarios asignados a realizar tareas relacionadas con la seguridad informática, lo que contribuye con la seguridad de la información, cumpliendo con el numeral 7.1 “Recursos” de la Norma NTC-ISO/IEC 27001:2013.

8. Se evidencia la existencia de manual de funciones, adoptado mediante las Resoluciones Nos. 253 de 2012 y 111 de 2006, relacionada con la creación de grupos de trabajo en la oficina de Sistemas, existiendo conformidad con el numeral 7.2 de la Norma NTC-ISO/IEC 27001:2013.

9. Durante el año 2019 se ejecutó el contrato 179-229-2019 cuyo objeto consistió en la sensibilización, socialización y capacitación del SGSI al interior de la Entidad. Dentro de las actividades que se desarrollaron se encuentran: encuesta de conocimiento del SGSI a través de plataforma virtual, se habilitó un sistema en la plataforma Moodle virtual para los funcionarios de la PGN, charla dirigida a gestores de calidad, actividad lúdica visitando las dependencias; actividades que procuran por el cumplimiento del numeral 7.3 de la Norma NTC-ISO/IEC 27001:2013.

10. Las Resoluciones No. 036 de 2009 y No. 910 de 2019 se encuentran publicadas en la opción de Relatoría del Portal Institucional de la PGN y mediante la ejecución del contrato 179-229-2019 se dio a conocer temas relacionados con la seguridad de la información, lo que es conforme con el numeral 7.4 de la Norma NTC-ISO/IEC 27001:2013.

11. A nivel interno de la Oficina de Sistemas, se tiene una carpeta compartida, para el grupo de seguridad informática, con documentación relacionada con el SGSI. En la Intranet, en la opción Oficina de Sistemas, se encuentran publicadas las Resoluciones Nos. 036 de 2009 y 910 de 2019, lo que muestra que se cuenta con información documentada, relacionada con lo establecido en el numeral 7.5; no obstante, existen observaciones.

12. Se evidencia que, para cumplir con los requisitos de la seguridad de la información, se cuenta con el plan de manejo de riesgos, con el Plan Estratégico de Tecnologías de la Información y el Plan Anual de Adquisiciones, lo que cumple con el numeral 8.1 “Operación” de la Norma NTC-ISO/IEC 27001:2013. Sin embargo, existen oportunidades de mejora.

13. Se evidencia que se está llevando a cabo la evaluación del Modelo de Seguridad y Privacidad de la Información, haciendo uso de una herramienta que contempla los lineamientos establecidos por el Ministerio de Tecnologías de la Información, el cual arroja un resultado de 20 puntos en una escala de 1 a 100, lo que muestra que el Modelo se encuentra en un nivel inicial. Se cumple con el numeral 9.1 de la NTC-ISO/IEC 27001:2013; no obstante, existen oportunidades de mejora.

14. Se evidencia la existencia de controles de acceso, cumpliendo con el numeral A.9.1.2 “Acceso a redes y a servicios de red”, y algunos de los relacionados con el numeral A.9.2 “Gestión de acceso de usuarios” del Anexo A de la Norma NTC-ISO/IEC 27001:2013; sin embargo, existen oportunidades de mejora.

15. En cuanto a los controles de seguridad física y del entorno se cuenta con el contrato de vigilancia 179-142-2018. Por parte de la División de Seguridad, se han emitido varias circulares y memorandos con lineamientos y recomendaciones al respecto. En el Sistema de Gestión de Calidad se encuentran publicado el documento “Guía de seguridad”, lo que propende por la seguridad de la Entidad; sin embargo, existen observaciones al respecto.

4.2 No conformidades

1. No se evidencia la designación del Oficial de Seguridad incumpliendo con los artículos Tercero y Cuarto de la Resolución No. 036 de 2009 y dando lugar a una no conformidad en el numeral 5.3 “Roles, Responsabilidades y autoridades en la organización” de la Norma NTC-ISO/IEC 27001:2013.

2. No se evidencia la operatividad del Comité de Seguridad de la Información incumpliendo con el requisito 9.3 “Revisión por la Dirección” de la Norma NTC-ISO/IEC 27001:2013 y el artículo Octavo de la Resolución No. 036 de 2009. Se debe revisar a la luz del Decreto 1499 de 2017 y normatividad interna, si éste debe ser absorbido por alguno de los Comités creados mediante la Resolución No. 642 de 2019 o cumplir con lo establecido en el artículo precitado.

4.3 Observaciones:

1. La PGN cuenta con la Política de Seguridad establecida mediante Resolución No. 910 de 2019, la cual es adecuada para la Entidad; sin embargo, no se observan definidas las políticas de seguridad relacionadas con la seguridad física y del entorno, de continuidad del negocio y, aunque se menciona la del recurso humano, es muy general.

2. No se evidencia el componente de medición de los objetivos de la seguridad, por lo que se incumple, en parte, el numeral 6.2 “Objetivos de la seguridad de la información y planes para lograrlos” de la Norma NTC-ISO/IEC 27001:2013.

3. Se evidencia que existe información documentada, sin embargo, se debe mejorar en los controles sobre la misma, estableciendo formatos estandarizados y protocolos de control, que cumplan con lo establecido en los numerales 7.5.2 “Creación y actualización” y 7.5.3 “Control de la información documentada” de la Norma NTC-ISO/IEC 27001:2013.

4. La PGN adoptó el Sistema de Gestión de Seguridad de la Información mediante Resolución No. 036 de 2009 y se hace mención a un anexo reposa en la Oficina de Sistemas y que se debería encontrar publicado en la página web; no obstante, el documento no fue puesto disposición de la auditoría y no se observó la publicación, lo que incumple con el numeral 7.5.3 “Control de la información documentada” de la Norma NTC-ISO/IEC 27001:2013.

5. En la verificación realizada a tres centros de cableado, se evidenció que el del piso “X” tiene la puerta de entrada deteriorada en la parte inferior; el rack del centro de cableado del piso “X” presenta obstáculos que impiden que pueda ser cerrado; sin embargo, las puertas principales si lo están; en dos de los racks se observó la presencia de abundante polvo producto de obras locativas, situaciones que pueden poner en riesgo la disponibilidad en el acceso a la información.

6. Se evidencia que se cuenta con controles de seguridad física y del entorno; no obstante, algunos dispositivos de tecnología que forman parte del Sistema Integrado de Seguridad física presentan disminución de la calidad o cantidad insuficiente, que merman o imposibilitan el adecuado funcionamiento de los mismos, lo que conlleva a que no se cumpla a cabalidad con lo establecido en el numeral A.11 del anexo A de la Norma NTC-ISO/IEC 27001:2013, relacionado con controles de la seguridad física y del entorno.

7. Se observan debilidades en los controles de circulación de visitantes a la Entidad, debido a que una vez ingresan, les es permitido circular libremente por los diferentes pisos y dependencias de la Entidad, lo que puede poner en riesgo la seguridad de la información.

8. Las áreas de ingreso y algunas zonas perimetrales de las instalaciones en las Torres A, B, C de la Sede Central y del Edificio Manuel Mejía, están construidas en vidrio, lo que las hace vulnerables a amenazas externas tales como asonadas, lo que podría poner en riesgo la seguridad de las personas, de la información y la infraestructura de la Entidad.

4.4 Oportunidades de mejora

1. La seguridad de la información es un asunto transversal a toda la Entidad. Las actividades desarrolladas en el marco del Sistema de Gestión de Seguridad de la Información, se observan realizadas principalmente, desde el punto de vista de la Oficina de Sistemas, por lo que se debe articular con las diferentes áreas a las que les corresponda implementar controles, para dar cabal cumplimiento a la Política de Seguridad de la Información.

2. Revisar el anexo a la Resolución No. 910 de 2019 y analizar si hay lugar a ajustes, en cuanto al ciertos contenidos, que podrían ser más apropiados para un instructivo u otro tipo de documento.

3. Se está llevando a cabo la medición del Modelo de Seguridad y Privacidad de la Información; no obstante, se deben definir indicadores que permitan la medición del cumplimiento de los objetivos y de la eficacia del Sistema de Gestión de Seguridad de la Información, de acuerdo con lo establecido en el numeral 9.1 “Seguimiento, medición y análisis y evaluación” de la Norma NTC-ISO/IEC 27001:2013.

Sandra del P Chuquín Badillo

SANDRA DEL PILAR CHUQUÍN BADILLO
Auditor Oficina de Control Interno

Vo.Bo.

Magda Patricia Morales Sáenz

MAGDA PATRICIA MORALES SÁENZ

Jefe Oficina de Control Interno