Función Pública

Concepto 452201 de 2025 Departamento Administrativo de la Función Pública

20255000452201

Al contestar por favor cite estos datos:

Radicado No.: 20255000452201

Fecha: 11/09/2025 08:05:10 a.m.

Bogotá D.C.

Referencia: Aclaración sobre auditoría al Sistema de Gestión de Seguridad de la Información (SGSI), por parte de la Oficina de Control Interno. Radicado No. 20259000546112 del 17 de agosto de 2025.

CONSULTA:

(...) En particular, entiendo que en mi caso al ser responsable de seguridad de la información (Oficial de Seguridad) soy segunda línea y debo realizar revisiones y seguimientos al SGSI, sin embargo, si yo solicitara una auditoría interna al SGSI, la oficina de control interno me responde que soy yo mismo el que debo realizarla, en ese caso considero que hay un conflicto de intereses al ser el responsable que está construyendo el Sistema de Gestión (además yo hago seguimiento con el instrumento de autodiagnóstico que emite MinTIC para el Modelo de Seguridad de la Información).

En ese orden de ideas, si se requiere realizar una auditoría interna al SGSI, ¿quién debería realizarla? ¿yo debería contratar a un ente externo para que la ejecute, dada la respuesta de control interno a que ellos solo auditan cuando la segunda línea demuestra deficiencias en su evaluación continua?

Agradezco mucho su orientación, dado que anteriormente lo que se hacía era incluir en los planes de auditoría interna (que ejecutaba control interno) al Sistema de Gestión de Seguridad de la Información, pero ahora la verdad no es claro. (...)

ANÁLISIS:

En primer lugar, es pertinente indicar que la Ley 87 de 1993, "Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones", define lo siguiente en materia de control interno:

ARTÍCULO 9.- DEFINICIÓN DE LA UNIDAD U OFICINA DE COORDINACIÓN DEL CONTROL INTERNO. Es uno de los componentes del Sistema de

Control Interno, de nivel gerencial o directivo, encargado de medir y evaluar la eficiencia, eficacia y economía de los demás controles, asesorando a la dirección en la continuidad del proceso administrativo, la reevaluación de los planes establecidos y en la introducción de los correctivos necesarios para el cumplimiento de las metas u objetivos previstos. (Subrayado fuera de texto)

ARTÍCULO 10.- JEFE DE LA UNIDAD U OFICINA DE COORDINACIÓN DEL CONTROL INTERNO. Para la verificación y evaluación permanente del Sistema de Control Interno, las entidades estatales designarán como Asesor, Coordinador, Auditor Interno o cargo similar, a un funcionario público que será adscrito al nivel jerárquico superior y designado en los términos de la presente Ley. (Subrayado fuera de texto)

ARTÍCULO 12.- FUNCIONES DE LOS AUDITORES INTERNOS. Serán funciones del Asesor, Coordinador, Auditor Interno, o similar las siguientes:

a. Planear, dirigir y organizar la verificación y evaluación del Sistema de Control Interno;

b. Verificar que el Sistema de Control Interno esté formalmente establecido dentro de la organización y que su ejercicio sea intrínseco al desarrollo de las funciones de todos los cargos y, en particular, de aquellos que tengan responsabilidad de mando;

c. Verificar que los controles definidos para los procesos y actividades de la organización, se cumplan por los responsables de su ejecución y en especial, que las áreas o empleados encargados de la aplicación del régimen disciplinario ejerzan adecuadamente esta función;

d. Verificar que los controles asociados con todas y cada una de las actividades de la organización, estén adecuadamente definidos, sean apropiados y se mejoren permanentemente, de acuerdo con la evolución de la entidad;

e. Velar por el cumplimiento de las leyes, normas, políticas, procedimientos, planes, programas, proyectos y metas de la organización y recomendar los ajustes necesarios;

f. Servir de apoyo a los directivos en el proceso de toma de decisiones, a fin que se obtengan los resultados esperados;

g. Verificar los procesos relacionados con el manejo de los recursos, bienes y los sistemas de información de la entidad y recomendar los correctivos que sean necesarios;

h. Fomentar en toda la organización la formación de una cultura de control que contribuya al mejoramiento continuo en el cumplimiento de la misión institucional;

i. Evaluar y verificar la aplicación de los mecanismos de participación ciudadana, que, en desarrollo del mandato constitucional y legal, diseñe la entidad correspondiente;

j. Mantener permanentemente informados a los directivos acerca del estado del control interno dentro de la entidad, dando cuenta de las debilidades detectadas y de las fallas en su cumplimiento;

k. Verificar que se implanten las medidas respectivas recomendadas;

l. Las demás que le asigne el jefe del organismo o entidad, de acuerdo con el carácter de sus funciones.

De acuerdo con las normas citadas, la unidad u oficina de coordinación del control interno es uno de los componentes del Sistema de Control Interno, de nivel gerencial o directivo, encargado de medir y evaluar la eficiencia, eficacia y economía de los demás controles, asesorando a la dirección en la continuidad del proceso administrativo, la revaluación de los planes establecidos y en la introducción de los correctivos necesarios para el cumplimiento de las metas u objetivos previstos.

Para este efecto, las Oficinas de Control Interno en todas las entidades del Estado, para la ejecución de sus funciones utilizan las técnicas y normas de auditoría generalmente aceptadas. Al respecto es importante mencionar que la Guía de auditoría interna basada en riesgos para entidades públicas (versión 4), emitida por este Departamento Administrativo, determina cinco (5) fases que permiten llevar a cabo el proceso auditor en general de manera técnica y profesional, al hacer uso de diferentes herramientas y procedimientos de auditoría. Estas fases son:

Planeación general de auditoría basada en riesgos (Plan Anual de Auditorías)

Planeación de una auditoría interna basada en riesgos

Ejecución de la auditoría

Informe de auditoría (Comunicación de resultados)

Seguimiento del progreso

Cada una de estas etapas desarrolla orientaciones contempladas en el Marco para la Práctica Profesional de Auditoría Interna que deben ser tenidas en cuenta por parte del Jefe de Control Interno, con el fin de mejorar la efectividad del proceso auditor.

Se debe aclara en este caso, que en la etapa de planeación, el Jefe de Control Interno debe establecer las auditorías para la vigencia, pero también debe incluir los seguimientos e informes de ley que son de su responsabilidad, información a partir de la cual se emiten observaciones o recomendaciones para la mejora institucional, que pueden derivar en acciones de mejora para la entidad, las cuales se podrán articular con planes de mejoramiento existentes como resultado de procesos de auditoría, esto para evitar reprocesos o recargas innecesarias a los líderes de los procesos.

Ahora bien, dado que usted se refiere en su consulta a la auditoría interna requerida para evaluar el Sistema de Gestión de Seguridad de la Información, es relevante precisar que, para la ejecución de las actividades mencionadas, la Oficina de Control Interno debe estructurar el Plan Anual de Auditorías, el cual bajo los lineamientos de la guía en mención debe incluir no solamente las auditorías internas para la vigencia, sino también todas aquellas actividades que cubren cada uno de los roles establecidos en la normatividad, es decir que el plan cubre todas las actividades a realizar en el año para la Oficina de Control Interno, incluyendo seguimiento a temas claves de la gestión, a fin de garantizar el suministro de información y los espacios necesarios con los líderes de los temas internamente, evitando retrasos o posibles incumplimientos frente a informes de ley u otras necesidades.

En este sentido, la guía en mención expresa lo siguiente:

"(...) *El Plan Anual de Auditorías es el documento formulado por el equipo de trabajo de la Oficina de Control Interno, o quien haga sus veces en la entidad, cuya finalidad es planificar y establecer los trabajos a cumplir anualmente para evaluar y mejorar la eficacia de los procesos de gestión de riesgos y control.*

Las actividades que se deben considerar para la elaboración del plan anual de auditoría son: Auditorías internas a los procesos (de acuerdo a priorización y plan de rotación de las auditorías), Auditorías especiales o eventuales sobre procesos o áreas responsables específicas y ante eventualidades presentadas que obliguen a ello, Auditorías especiales solicitadas por el cliente de auditoría (representante legal), Actividades de asesoría y acompañamiento en temas puntuales, de acuerdo a las necesidades de la entidad, Elaboración de informes determinados por ley, Capacitación para los funcionarios de la oficina, Atención a entes de control, Seguimiento a planes de mejoramiento y Determinar tiempos para

situaciones imprevistas que afecten el tiempo del plan de auditoría, entre otros. (...)".

En consecuencia, sería necesario, en primer lugar, validar si dentro de la planeación para la vigencia la Oficina de Control Interno tenía contemplada el proceso auditor que es requerido para el Sistema de Gestión de Seguridad de la Información, toda vez que el universo de auditoría analiza todos los aspectos que desarrolla la entidad en el marco de su gestión y cubre diferentes componentes, tanto de planeación estratégica, articulada con la gestión presupuestal, gestión contractual, procesos, programas o proyectos, sistemas de información, áreas o grupos desconcentrados, entre otros aspectos y sus riesgos asociados, lo que le permite a la Oficina de Control Interno establecer a detalle las unidades auditables que conforman el universo y a partir del análisis de priorización poder definir los temas a auditar en cada vigencia.

En todo caso, me permito aclararle que, en relación con las auditorías al sistema objeto de su consulta, que el Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC, en desarrollo del Modelo de Seguridad y Privacidad de la Información - MSPI, *"imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital"*[1].

En este marco general, mediante el documento Lineamientos de Roles y Responsabilidades, el cual me permito adjuntar para su referencia, en los numerales 6.1 y 6.5 establece lo siguiente:

"(...)

6.1. Responsable de Seguridad de la Información para la entidad

El responsable de seguridad y privacidad de la información u oficial de seguridad de la información tendrá a su cargo liderar y gestionar la implementación y mantenimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) en la entidad y tendrá entre otras las siguientes responsabilidades principales:

- Definir y gestionar la normativa de seguridad y privacidad de la información y seguridad digital.

- Participar y reportar la gestión de seguridad y privacidad de la información en los comités institucionales relevantes.

- Promover la concientización, capacitación y mejora continua en materia de seguridad y privacidad de la información para todo el personal de la entidad.

- Definir, socializar e implementar los procedimientos relacionados con la gestión de seguridad y privacidad de la información al interior de la entidad.

- Asesorar y acompañar a las diferentes áreas de la entidad en la gestión de activos de información, riesgos, implementación de controles y definición de actividades de planes de tratamiento para mejorar la postura de seguridad en la entidad.

(...)

6.5. Control Interno

- En el marco de su Plan Anual de Auditoría, la Oficina de Control Interno o quien haga sus veces debe incluir auditorías técnicas y de gestión de seguridad de la información.

- Se deben definir responsables de planificar, ejecutar y reportar las auditorías de seguridad de la información, asegurando que cuenten con la competencia y formación necesarias para evaluar la efectividad de los controles del MSPI.

- Se debe establecer la efectividad de los controles para asegurar el cumplimiento de la normativa vigente en materia de seguridad de la información y protección de datos personales, a través de sus procesos de seguimiento y evaluación.

- Las responsabilidades principales del encargado de realizar las auditorias técnicas y de gestión de seguridad de la información son:

- Realizar auditorías internas de seguridad de la información

- Evaluar la efectividad de los controles de seguridad de la información Identificar no conformidades, desviaciones y oportunidades de mejora del MSPI Informar sobre los resultados de las auditorías

- Coordinar actividades con otras áreas (ej. Oficina Asesora de Planeación)

- Realizar seguimiento al cumplimiento normativo (Subrayado fuera de texto)

Su función primordial es la de proporcionar una evaluación independiente y objetiva sobre la eficacia del sistema de gestión de seguridad de la información, identificando áreas de riesgo y proponiendo mejoras para garantizar el cumplimiento de los objetivos y la normativa aplicable".

Se tiene entonces que, el oficial de seguridad de la información tiene a su cargo liderar y gestionar la implementación y mantenimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) en la entidad, marco en el cual debe participar y reportar la gestión de seguridad y privacidad de la información, así como asesorar y acompañar a las demás áreas de la entidad en temas relevantes para garantizar la seguridad de la información en la entidad.

Por su parte, la Oficina de Control Interno o quien haga sus veces debe incluir auditorías técnicas a la gestión de seguridad de la información, por lo que se precisa que dicha instancias sí tiene la responsabilidad frente a su planificación y ejecución, para lo cual será necesario establecer el auditor de dicha oficina que cuenta con los conocimientos necesarios y experticia para su aplicación, ya que no se trata de ejecutar auditorías de lista de chequeo, sino que se adelanten procesos de fondo que permita establecer la idoneidad del sistema y evaluar la efectividad frente a la seguridad de la información.

CONCLUSIÓN

De acuerdo con lo anteriormente expuesto, teniendo en cuenta que como oficial de seguridad de la información, tiene bajo su responsabilidad liderar y gestionar la implementación y mantenimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) en la entidad, no resulta viable que pueda realizar la auditoría interna requerida para el sistema, ya que no se contaría con la objetividad necesaria para evaluar la efectividad del sistema.

Por lo tanto, corresponderá a la Oficina de Control Interno planificarlas y ejecutarlas, de acuerdo con el análisis de unidades auditables y del análisis basado en riesgos que a esta instancia le corresponde, por lo que, lo que procede es analizar esta necesidad y que se pueda incluir en el Plan Anual de Auditorías y someterla a aprobación del Comité Institucional de Coordinación de Control Interno, instancia regulada a través del

Decreto 648 de 2017 y tiene dentro de sus funciones aprobar el plan anual y las modificaciones que sean necesarias en desarrollo de la gestión institucional.

Sugerimos entonces, que, en el marco del Comité de Gestión y Desempeño Institucional instancia responsable frente al análisis y seguimiento a las políticas de gestión y desempeño, dentro de las cuales se encuentra la de Gobierno Digital para que se pueda tratar este tema y canalizar la necesidad puntual para la ejecución de las auditorías objeto de su consulta y que sea a través del jefe de planeación, como secretario técnico de este comité, se pueda solucionar la situación que se presenta.

Es importante en todo caso que tengan en cuenta que, tal requerimiento debe atender la capacidad actual de la Oficina de Control Interno, ya que para poder adelantar este tipo de auditorías que requieren conocimientos específicos y la experticia necesaria, por lo que, si dentro del equipo no se cuenta en este momento con el perfil requerido será necesario que internamente la entidad disponga de los recursos para la capacitación o formación del auditor o grupo de auditores que se determinen, de manera tal que se pueda dar cumplimento al proceso auditor bajo las condiciones técnicas necesarias.

Finalmente, lo invitamos a ingresar al Espacio Virtual de Asesoría –EVA-, al cual puede acceder a través de: http://www.funcionpublica.gov.co/eva donde podrá encontrar normatividad, guías, conceptos chat, entre otros.

El anterior concepto se imparte en los términos del artículo 28 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

LUZ DAIFENIS ARANGO RIVERA

Directora de Gestión y Desempeño Institucional

Proyectó Carlos Andrés Rodríguez

Revisó: Myrian Cubillos Benavides

11302.8.2

NOTAS DE PIE DE PÁGINA

1 Fuente: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

Fecha y hora de creación: 2025-11-23 02:11:02