OFICINA DE CONTROL INTERNO

INFORME DE AUDITORÍA

TIPO DE INFORME

Preliminar ☐ Definitivo ☒

AUDITORIA AL SISTEMA DE GESTIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

AÑO	AUDITORÍA No.	PROCESO, PROCEDIMIENTO O ACTIVIDAD	ÁREA RESPONSABLE
2025	A3	**Sistema de Gestión del Modelo de Seguridad y Privacidad de la Información**	Oficina de Tecnología y Sistemas de Información

PERIODO AUDITADO O EVALUADO	FECHA INFORME PRELIMINAR	FECHA INFORME DEFINITIVO
1 de enero al 31 de diciembre de 2024	14 de agosto de 2025	26 de agosto de 2025

Informe elaborado por:

Oscar Alonso Chamath Palacios
Raúl Darío Rodríguez Jiménez

Oficina de Control Interno

TABLA DE CONTENIDO

INTRODUCCIÓN

El presente documento consolida los resultados de la auditoría interna practicada al Sistema de Gestión del Modelo de Seguridad y Privacidad de la Información (MSPI). La evaluación se orientó a verificar el cumplimiento de los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y la norma ISO/IEC 27001:2013, con el fin de garantizar la protección de la confidencialidad, integridad y disponibilidad de la información institucional.

1. OBJETIVO

Verificar el cumplimiento de las disposiciones del Modelo de Seguridad y Privacidad de la información del Ministerio de Ciencia, Tecnología e Innovación, así como verificar la debida actualización de los activos asociados a este sistema de gestión.

2. ALCANCE

Comprende la verificación de la implementación de plan de seguridad de la información en el Ministerio de Ciencia, Tecnología e Innovación correspondiente al periodo del 1 de enero al 31 de diciembre de 2024.

3. NORMATIVIDAD

- Modelo de Seguridad y Privacidad de la Información – MINTIC.
- Manual de políticas de seguridad de la Información D103M01.
- ISO/IEC 27001:2013

4. METODOLOGÍA

La metodología utilizada para el desarrollo de la presente auditoría se basó en la verificación de la información suministrada por la Oficina de Tecnologías y Sistemas de Información - OTSI. Esta verificación incluyó la evaluación de cumplimiento de los requisitos técnicos conforme los lineamientos establecidos por el Modelo de Seguridad y Privacidad de la información del Ministerio de Ciencia, Tecnología e Innovación, frente a los lineamientos del Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC. Por otra parte, Se realizaron mesas de trabajo con los enlaces asignados de la OTSI para llevar a cabo la auditoría, con el fin de aclarar inquietudes generadas en el desarrollo de ésta.

Para la ejecución de lo descrito anteriormente, la Oficina de Control Interno llevó a cabo las siguientes etapas:

a. Planeación

- Revisión lineamientos internos y externos y elaboración listas de chequeo.
- Preparación de información para la apertura de auditoría.

b. Ejecución

- Diligenciamiento de listas de chequeo

- Preparación de Informe preliminar
- Mesa de trabajo con los auditados para aclarar dudas frente al informe preliminar de auditoría
- Preparación de informe final

c. Comunicación de resultados

5. MUESTRA

La muestra empleada para desarrollar la presente auditoria se fundamentó en la revisión de todas las actividades documentadas en el Manual de Seguridad y Privacidad de la Información y se cotejó el cumplimiento de los lineamientos del Modelo de Seguridad y Privacidad de la Información establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC, el cual se encuentra articulado con lo dispuesto en la norma ISO 27001:2013. En el sentido de lo anterior, entiéndase que se tomó como muestra el 100% de los elementos verificables.

6. EJECUCIÓN DE AUDITORÍA

La auditoría se desarrolló a través de la revisión y análisis de la documentación proporcionada y la evaluación del proceso relacionado con la seguridad de la información. Esto incluyó la verificación de su alineación con la norma ISO 27001:2013 y los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las comunicaciones-MinTIC. Adicionalmente, se realizó el análisis del riesgo asociado a Proceso de Gestión de Tecnologías y Sistemas de Información publicado en el Sistema de Información GINA, así como la verificación de las evidencias que respaldan la ejecución de los criterios del Modelo de Seguridad y Privacidad de la Información dispuesto para dicho fin.

6.1 RIESGOS

Se evaluó el riesgo actual publicado en el Sistema de Información Gina para el Proceso de Gestión de Tecnologías y Sistemas de Información. Al respecto, se encontró que actualmente existe un (1) riesgo identificado asociado al objetivo y alcance establecido para esta auditoría, el cual se relaciona en la siguiente tabla:

Tabla 1. Riesgo del Proceso

Proceso	Riesgo actual asociado al procedimiento
Gestión de Tecnologías y Sistemas de Información	RSI01-D103 Posibilidad de afectación económica y reputacional, por acceso no autorizado o alteración de la información de las plataformas tecnológicas del Ministerio, generando pérdida de confidencialidad, integridad y disponibilidad de la información, debido a las vulnerabilidades de las plataformas tecnológicas del Ministerio.

Fuente: Sistema de información GINA / Módulo de Riesgos

Para la evaluación del riesgo mencionado en la tabla anterior, se tuvieron en cuenta los lineamientos establecidos por el Ministerio, a través de la Guía para la Gestión del Riesgo (D102PR03G01) específicamente el numeral 13 RIESGOS DE SEGURIDAD DE LA INFORMACIÓN, en este sentido, se detalla a continuación la evaluación realizada a los dos (2) controles asociados a la mitigación de riesgo evaluado RSI01-D103, teniendo en cuenta que para tratar los riesgos de Seguridad de la información el Ministerio de Ciencia, Tecnología e Innovación aplica los criterios establecidos para la definición de controles del Anexo A de la norma ISO 27001:2013, los cuales también se

encuentran en el anexo 4. *"Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas"*[1]*:*

Tabla 2. Análisis controles riesgo RSI01-D103

Información Sistema de Información Gina		**Observaciones Oficina de Control Interno**
Controles	**Tipo de Control**	
1. Pruebas de vulnerabilidades sobre los diferentes servicios tecnológicos y componentes de la plataforma tecnológica y aplicativos web, para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información, utilizando la solución de Tenable SC y Tenable IO o las soluciones vigentes y utilizadas por el Ministerio.	Preventivo	La Oficina de Control Interno verificó que, este control está alineado con varios puntos del Anexo A de ISO 27001:2013, principalmente en las secciones de Gestión de la Vulnerabilidad, Gestión Técnica de la Seguridad y Pruebas de Seguridad donde aborda directamente la gestión técnica de las vulnerabilidades (A.12.6.1) y la verificación de la seguridad del sistema (A.14.2.8). Así mismo, aunque la tipología de control se identifica como preventivo, en el sistema de información Gina, se observa que este control tiene un enfoque tanto preventivo como detectivo. En primera medida, cuando busca identificar y corregir vulnerabilidades previo a su ocurrencia; en segundo lugar, cuando las pruebas ejecutadas detectan la existencia de vulnerabilidades. En cuanto a los elementos de la estructura para la descripción del control, mencionados en la Guía para la Gestión del Riesgo: **¿Cómo se realiza el control?** y **observaciones y desviaciones**, no se identifican las actividades que se deberían realizar una vez se detecten las vulnerabilidades (cómo se priorizan, cómo se asignan responsabilidades, cómo se corrigen las vulnerabilidades identificadas y cómo se verifica su solución), lo cual cobra importancia, toda vez que son puntos críticos para determinar la efectividad de un control. Así mismo, para el elemento de **evidencia de la ejecución del control** se observó que no está identificado el documento que describe la ejecución del control o de los elementos asociados al control, por lo cuál se debería incluir el procedimiento o lineamiento que define el control para subsanar y realizar el seguimiento de las vulnerabilidades encontradas. Teniendo en cuenta lo anterior, se identifica la necesidad de revisar y ajustar los elementos de la estructura para la descripción del control.
2. Sensibilizaciones y capacitaciones en seguridad de la Información a los usuarios de los servicios tecnológicos del Ministerio.	Preventivo	La Oficina de Control Interno evidenció que, este control se encuentra alineado con lo definido en el Anexo A de la norma ISO 27001:2013, en los requisitos relacionados con la Concientización, Educación y Formación en la Seguridad de la Información, incorporando el factor humano, relevante para la seguridad de la información (A.7.2.2).

[1] Guía para la Gestión del Riesgo (D102PR03G01) específicamente el numeral 13 RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Información Sistema de Información Gina		Observaciones Oficina de Control Interno
Controles	**Tipo de Control**	
		Del mismo modo se evidencia que los elementos de la estructura para la descripción del control, mencionados en la Guía para la Gestión del Riesgo (responsable, periodicidad, propósito, ¿cómo se realiza el control?, observaciones y desviaciones y evidencia de la ejecución del control) se encuentran definidos en el sistema de información GINA, acorde con lo establecido en la Guía para la gestión del riesgo - D102PR03G01.

Fuente: Elaboración propia a partir de información extraída del Sistema de Información GINA

Teniendo en cuenta la revisión realizada a cada uno de los controles descritos en la tabla anterior, la Oficina de Control Interno determina que el proceso Gestión de Tecnologías y Sistemas de Información debería revisar y ajustar los elementos de la estructura para la descripción del control, que contribuyan a la efectiva ejecución del control denominado "Pruebas de vulnerabilidades sobre los diferentes servicios tecnológicos y componentes de la plataforma tecnológica y aplicativos web, para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información, utilizando la solución de Tenable SC y Tenable IO o las soluciones vigentes y utilizadas por el Ministerio". **(Esta situación da lugar a la recomendación número 1, la cual se detalla en el numeral 7.4.1 del presente informe).**

6.2 VERIFICACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En cumplimiento de los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones y teniendo en cuenta el objeto y alcance de esta auditoría, se realizó un ejercicio consistente en la verificación de los elementos derivados de cada actividad del Manual de Políticas de Seguridad de la Información (D103M01). Lo anterior con el fin de identificar el cumplimiento de acuerdo con las evidencias aportadas por la Oficina de Tecnologías y Sistemas de Información (OTSI).

A partir de lo anterior, se exponen a continuación los resultados de auditoría tomando como referencia los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las comunicaciones-MinTIC, el cual se compone de cuatro (4) fases (planificación, operación, evaluación de desempeño y mejoramiento continuo).

6.2.1 Fase 1: Planificación

En esta fase se verificó que la entidad realizó la planeación del tiempo, recursos y presupuesto de las actividades relacionadas con el MSPI, organizadas en cuatro (4) subfases (contexto, liderazgo, planeación y soporte).

6.2.1.1 Contexto.

Para el análisis de la subfase de contexto, se verificó el desarrollo de las tres (3) actividades que se describen a continuación:

- **Actividad 7.1.1 Comprensión de la organización y de su contexto**

La Oficina de Control Interno observó que el Ministerio ha determinado los elementos internos y externos relevantes, reconociendo la información como un activo para el desarrollo de su misión, teniendo en cuenta la realidad del entorno en cuanto a la importancia de velar por la seguridad y protección de la información. El manual de Políticas de Seguridad de la Información identificado con código D103M01, reglamenta la gestión de seguridad y privacidad de la información, con el fin de mantener la disponibilidad, integridad, confidencialidad, privacidad, continuidad y autenticidad de la información.

- **Actividad 7.1.2 Necesidades y expectativas de los interesados**

Se identificó que el manual de seguridad de la información define a las partes interesadas incluyendo servidores públicos, contratistas, visitantes y terceros; detallando sus responsabilidades en la protección de la información y sus derechos, especialmente en la política de protección de datos personales.

- **Actividad 7.1.3 Definición del alcance del MSPI**

La Oficina de Control Interno verificó que en el manual de seguridad y privacidad de la información se define el alcance, que comprende los lineamientos y su aplicabilidad para todos los aspectos administrativos y de control que deben ser cumplidos por los servidores públicos, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con el Ministerio a través de la recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, con personal interno o externo, en el desarrollo de la misión institucional y el cumplimiento de sus objetivos estratégicos.

6.2.1.2 Liderazgo

Para el análisis de la subfase de liderazgo, se verificaron las tres (3) actividades que se describen a continuación:

- **Actividad 7.2.1 Liderazgo y Compromiso**

Se evidenció la aprobación de los temas relacionados con la Seguridad y Privacidad de la Información por parte del Comité de Gestión y Desempeño Sectorial e Institucional el cual se encuentra documentada en el acta del CGDSI No. 11 del 23 de abril de 2024. La política de Seguridad de la Información tiene establecida la implementación, operación y mejora continua del Sistema de Gestión de Seguridad de la Información. De acuerdo con la resolución 083 del 29 de enero de 2020, el Comité de Gestión y Desempeño Sectorial e Institucional tiene la función de *"Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información"* (página 11, Artículo 30, numeral 13).

- **Actividad 7.2.2 Política de seguridad y privacidad de la información**

Se constató que la entidad tiene establecida la política de seguridad y privacidad de la información en la cual se evidencia el compromiso por proteger, preservar y administrar la confidencialidad, integridad, disponibilidad y no repudio de la información del ministerio. En cuanto a la normatividad, el manual incluye la norma de estándares internacionales como la ISO 27001:2013 el cual se encuentra articulado con los lineamientos del Modelo de Seguridad y Privacidad de la Información de MINTIC.

La aprobación de los temas relacionados con la Seguridad y Privacidad de la Información por parte del Comité de Gestión y Desempeño Sectorial e Institucional está documentada en el acta del CGDSI No. 11 del 23 de abril de 2024. Finalmente, la política de seguridad y privacidad de la información es comunicada al interior de la entidad a través correos electrónicos para la apropiación del SGSI.

- **Actividad 7.2.3 Roles y Responsabilidades**

Se evidenció que la entidad cuenta con el manual de roles y responsabilidades del sistema de gestión de seguridad de la información – SGSI con código D103M07, en el cual se definen los roles que tienen responsabilidad directa en el Sistema de Gestión de Seguridad de la Información, en cumplimiento con lo normado en las políticas de seguridad de la información.

De otra parte, no se evidenció que en el manual de seguridad y privacidad de la información o algún otro documento se haya designado un responsable del modelo de seguridad y privacidad de la información, con un equipo de apoyo, dependiente de un área estratégica distinta a la de Tecnología. **(Esta situación da lugar a la recomendación número 2, el cual se detalla en el numeral 7.4.2 del presente informe).**

6.2.1.2 Planeación.

Para el análisis de la subfase de planeación, se verificaron las tres (3) actividades que se describen a continuación:

- **Actividad 7.3.1 Identificación de activos de información e infraestructura crítica cibernética**

Se observó que la entidad cuenta con el "Manual de Inventario de Activos, Clasificación y Publicación de la Información" con código D103M02, que tiene por objetivo establecer lineamientos para la identificación, clasificación, valoración y actualización de los activos tecnológicos de información, aplicable para todos los procesos del Ministerio de Ciencia Tecnología e Innovación.

- **Actividad 7.3.2 Valoración de los riesgos de seguridad de la información**

La Oficina de Control Interno verificó que el Ministerio tiene establecido el lineamiento de valoración de riesgos, mediante la identificación, clasificación, valoración, gestión y tratamiento de los riegos de seguridad digital con el fin de proteger la confidencialidad, integridad, disponibilidad y privacidad de la información. De igual forma, tiene definido la Gestión de Riesgos como un proceso que debe llevarse a cabo en forma periódica, el cual implica la identificación, minimización o eliminación.

- **Actividad 7.3.3 Plan de tratamiento de los riesgos de seguridad de la información**

La Oficina de Control Interno evidenció que el Ministerio tiene identificados, clasificados, valorados, gestionados y da tratamiento a los tres (3) riesgos de seguridad de la información identificados en la matriz de riegos, con el propósito de implementar medidas y controles efectivos que permitan estar preparados ante situaciones en las que se vea comprometida tanto la seguridad física de sus instalaciones, personas, recursos y sistemas, como la seguridad de su información, como consta en los planes de tratamiento de riesgos.

6.2.1.3 Soporte

Para el análisis de la subfase de soporte, se contempla el desarrollo de las tres (3) actividades que se describen a continuación:

- **Actividad 7.4.1 Recursos**

Se verificó que en la política general, la entidad se compromete a implementar, operar y mejorar de forma continua el Sistema de Gestión de Seguridad de la Información, lo que implica la necesidad de asignar recursos para lograr este objetivo, en este sentido, se observó qué en el Plan Anual de Adquisiciones de 2024 se contempla la asignación de recursos para atender los aspectos inherentes al funcionamiento de la Oficina de Tecnologías y Sistemas de Información, así como lo relacionado a la seguridad de la información.

- **Actividad 7.4.2 Competencia, toma de conciencia y comunicación**

Se observó que la Oficina de Tecnologías y Sistemas de Información, tiene diseñado y ejecuta un plan para la apropiación del Sistema de Gestión de la Seguridad de la Información SGSI, el cual incluye concientización en seguridad de la información. Adicionalmente, promueve la divulgación y sensibilización sobre la protección de datos personales y se establece la responsabilidad de comunicar la importancia de la protección de la información.

- **Actividad 7.4.3 Información documentada**

La Oficina de Control Interno constató qué el manual contiene la información documentada de los lineamientos establecidos para el Modelo de Seguridad y Privacidad de la Información (MSPI) y el Sistema de Gestión de Seguridad de la Información (SGSI). Este contiene reglas para su creación y actualización, evidenciado por el código D103M01, de fecha 22/01/2024, en su versión 02. Además, la sección de control de cambios relaciona las modificaciones entre versiones y para dicho fin se incluyen numerales y descripciones, que permiten asegurar la trazabilidad y el control de versiones. Así mismo, la nota recurrente *"Una vez descargado o impreso este documento se considerará una COPIA NO CONTROLADA"* indica la existencia de una versión digital, controlada y disponible para su uso.

6.2.2 Fase 2: Operación

En esta fase se evaluó que la entidad haya implementado los mecanismos de seguridad de la información, se esté fomentando la cultura de seguridad y se hayan definido criterios de cumplimiento y mecanismos de control a los procesos y servicios relevantes, para lo cual se revisaron las siguientes actividades contempladas en el modelo:

- **Actividad 8.1 Control y planeación operacional**

Se observó que la Oficina de Tecnologías y Sistemas de Información, reporta, analiza, monitorea y evalúa el control operacional de la seguridad de la información, mediante el formato informe de incidente de seguridad de la información, código D103PR03F01, con el fin de prevenir cualquier riesgo de incidente que se pueda presentar. La Oficina de Control Interno evidenció la existencia de un marco para la planeación y el control operacional de la seguridad de la información, a través de mecanismos de supervisión continua y de la aprobación del manual por parte del Comité de Gestión y Desempeño Sectorial e Institucional.

- **Actividad 8.2 Plan de tratamiento de riesgos**

La Oficina de Control Interno verificó que el manual de seguridad y privacidad de la información tiene establecidos los controles físicos y digitales para mitigar riesgos. De igual forma, se evidenció que el Ministerio tiene implementados, conserva y documenta los planes de tratamiento de riesgos y realiza evaluaciones periódicas de riesgos de seguridad de la información.

- **Actividad 8.3 Definición de indicadores de gestión**

Se evidenció que la Oficina de Tecnologías de la información realizó un diagnóstico en el cual se evaluó el nivel de madurez en la implementación del Modelo de Privacidad y Seguridad de la Información. En este diagnóstico se observa el nivel de madurez alcanzado por cada uno de los controles e indicadores. De otra parte, se observó la identificación del indicador denominado "Nivel de disponibilidad de los Servicios Tecnológicos", el cual tiene una periodicidad de medición trimestral cuyo nivel de cumplimiento al cierre de 2024 corresponde al 99,70%.

6.2.2 Fase 3: Evaluación de desempeño

En esta fase se evaluó que la entidad esté realizando el seguimiento, medición y análisis del sistema a través de indicadores y que incluya la interacción entre el Modelo de Seguridad y Privacidad de la Información MSPI y el Modelo Integrado de Planeación y Gestión MIPG, para lo cual se realizó la verificación de las siguientes actividades:

- **Actividad 9.1 Seguimiento, medición, análisis y evaluación**

Se observó que la entidad tiene alineado el Sistema de Gestión de Seguridad de la Información (SGSI/MSPI) con el Modelo Integrado de Planeación y Gestión (MIPG), lo cual se evidencia en el instrumento de identificación de la línea base de seguridad establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC. Así mismo, se comprobó que la Oficina de Tecnologías y Sistemas de Información realizó este seguimiento con corte a 31 de diciembre de 2024, en cumplimiento de lo requerido en esta actividad.

- **Actividad 9.2 Auditoría Interna**

Se verificó que el Manual de Políticas de Seguridad y Privacidad de la Información menciona que la Oficina de Control Interno debe realizar auditorías internas con el fin de obtener información sobre el cumplimiento del Modelo de Seguridad y Privacidad de la Información. La ejecución de la presente auditoría confirma la aplicación de este lineamiento, a partir de la revisión del funcionamiento del Sistema de Gestión de Seguridad de la Información (SGSI) en lo referente a los objetivos de control, controles, políticas y procedimientos, lo cual mitiga el riesgo de incumplimiento del modelo y fortalece el aseguramiento de la seguridad de la información.

- **Actividad 9.3 Revisión por la dirección**

La Oficina de Control Interno constató la aprobación de los temas relacionados con la Seguridad y Privacidad de la Información por parte del Comité de Gestión y Desempeño Sectorial e Institucional el cual se encuentra documentada en el acta del CGDSI No. 11 del 23 de abril de 2024. Esto evidencia que la Política y el Manual de Seguridad y Privacidad fueron formalmente revisados y aprobados por el Comité de Gestión y Desempeño Institucional.

6.2.3 Fase 4: Mejoramiento continuo

En esta fase se evaluó que la entidad esté llevando a cabo las acciones oportunas para mitigar las debilidades identificadas, para lo cual se revisaron las siguientes actividades:

- **Actividad 10.1 Mejora continua**

La Oficina de Control Interno verificó que el Ministerio cuenta con un procedimiento para la mejora y la innovación en los procesos del Sistema Integrado de Gestión, en el cual se especifican las acciones necesarias para abordar los hallazgos, oportunidades de mejora y/o recomendaciones derivadas de auditorías o evaluaciones.

- **Actividad 10.2 Acciones Correctivas y no conformidades**

Se evidenció que la Oficina de Tecnologías y Sistemas de Información tiene en desarrollo un plan de mejoramiento, resultante del seguimiento y evaluación a la Política y Sistema de Gestión de Continuidad de la vigencia 2024.

7 RESULTADOS DE AUDITORÍA

7.2 HALLAZGOS

De conformidad con lo expuesto en el presente informe, no se generaron hallazgos.

7.3 OPORTUNIDADES DE MEJORA

De conformidad con lo expuesto en el presente informe, no se generaron oportunidades de mejora.

7.4 RECOMENDACIÓN

De conformidad con lo expuesto en el presente informe, identificaron las siguientes recomendaciones:

7.4.1 Recomendación 1: Fortalecer la documentación de los controles de los riesgos para una ejecución más efectiva.

Teniendo en cuenta la revisión realizada a los controles de los riesgos asociados al proceso, la Oficina de Control Interno determina que el proceso de Gestión de Tecnologías y Sistemas de Información debe revisar y ajustar los componentes asociados a los controles para mejorar su entendimiento y efectiva ejecución. Se ha observado que, si bien se enuncian los controles, es importante que cada control cuente con los detalles suficientes para guiar su aplicación, permitiendo así un monitoreo más efectivo, y garantizando la consistencia de los resultados.

7.4.2 Recomendación 2: Designación responsable del modelo de seguridad y privacidad de la información

Para dar cumplimiento al lineamiento del manual de seguridad y privacidad de la información en materia de roles y responsabilidades, se recomienda designar un responsable de este modelo con

un equipo de apoyo que dependa de un área estratégica de la entidad, distinta a la Oficina de Tecnologías y Sistemas de la Información, con el fin de asegurar que la supervisión, adopción, implementación y mejora continua del modelo cuenten con una visión transversal.

Antes de finalizar el presente informe es necesario que se tenga en cuenta que:

1. El proceso evaluador al que se refiere el presente documento es selectivo. Por lo tanto, los resultados de las pruebas practicadas y las evidencias obtenidas en este documento se realizaron de acuerdo con los criterios definidos en la planificación de la auditoría. Esto significa que se refieren únicamente a la muestra seleccionada, así como a los registros y/o documentos examinados durante el periodo evaluado. Por lo tanto, dichas muestras no pueden considerarse una evaluación general del estado a los demás elementos de la gestión del proceso de Gestión de Tecnologías y Sistemas de Información.

2. De acuerdo con el Procedimiento para la Mejora y la Innovación en los Procesos del Sistema Integrado de Gestión (D102PR02) y la Guía para la Mejora y la Innovación en los Procesos Sistema Integrado de Gestión (D102PR02G01), para el caso de las recomendaciones, es discrecional de la dependencia auditada su adopción y elaboración de un plan de mejoramiento, para lo cual agradecemos informar vía correo electrónico si las recomendaciones generadas en el presente informe serán o no acogidas.

[ORIGINAL FIRMADO]

Oscar Alonso Chamath Palacios
Auditor de la Oficina de Control Interno

[ORIGINAL FIRMADO]

Raúl Darío Rodríguez Jiménez
Auditor de la Oficina de Control Interno

[ORIGINAL FIRMADO]

Víctor Osmar Vergara Torres
Jefe de la Oficina de Control Interno