Instituto Nacional de Metrología de Colombia

Informe de Evaluación y Seguimiento al Mapa de Riesgos de Seguridad de la Información

Oficina de Control Interno

Bogotá, D.C.

2026-05-11

CONTENIDO

Página.

1. INTRODUCCIÓN

En cumplimiento del Plan Anual de Auditoría de la Oficina de Control Interno aprobado para la vigencia 2026, el presente informe tiene como propósito evaluar la gestión de los riesgos de seguridad de la información en el Instituto Nacional de Metrología (INM), en lo relacionado con la identificación de los riesgos, su articulación con los activos de información, el análisis de variables de seguridad, el diseño y ejecución de controles, y el seguimiento a su implementación.

El ejercicio se desarrolla como una actividad de seguimiento y evaluación, a partir de la revisión de información documental, la verificación de registros en los sistemas institucionales, la indagación con los responsables del proceso y el análisis de la consistencia entre la matriz de riesgos de seguridad de la información y la matriz de activos de información.

La evaluación se fundamenta en lo establecido en la Ley 87 de 1993, la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Versión 7 del DAFP, el Modelo de Seguridad y Privacidad de la Información (MSPI) y buenas prácticas de la norma ISO/IEC 27001:2022, en lo aplicable a la gestión de riesgos de seguridad de la información.

Para tal efecto, se revisó la matriz de riesgos de seguridad de la información aprobada en el Comité Institucional de Gestión y Desempeño (CIGD) No. 5 del 25 de marzo de 2026, con información actualizada al 27 de abril de 2026, con el fin de verificar la consistencia entre los riesgos identificados, los activos de información asociados, el diseño y ejecución de los controles, así como la disponibilidad de evidencias que soportan su seguimiento.

2. ALCANCE

El presente seguimiento comprende la información contenida en la matriz de riesgos de seguridad de la información vigente y en los mecanismos de control y seguimiento definidos por la entidad, así como los controles y acciones de mejora asociados, en relación con los siguientes aspectos:

- La identificación de los riesgos y su relación con los activos de información.
- La identificación de las variables de seguridad de la información (confidencialidad, integridad y disponibilidad) asociadas a los riesgos.
- La articulación entre la gestión de riesgos de seguridad de la información y la gestión documental.

- El diseño, ejecución y seguimiento de los controles establecidos.
- El seguimiento al plan de mejoramiento asociado al Sistema de Seguimiento de Planes de Mejoramiento 2.0 (SISEPM).

Nota: El análisis se realiza con base en la información documentada y reportada por la entidad para el periodo evaluado.

3. DESCRIPCIÓN METODOLÓGICA

Para el desarrollo de la presente evaluación, se aplicaron los siguientes procedimientos de auditoría:

1. Consulta: Se realizó reunión virtual con la contratista encargada de la gestión de los riesgos de seguridad de la información de la entidad, con el fin de conocer la versión vigente de la matriz de riesgos correspondiente a la vigencia 2026 y su estado de actualización.

2. Inspección: Se revisaron documentos institucionales disponibles en el aplicativo ISOLUCION y en la carpeta compartida administrada por la OAP, incluyendo procedimientos del Sistema Integrado de Gestión, la matriz de riesgos de seguridad de la información y las evidencias asociadas a la ejecución de controles y planes de mejoramiento.

3. Rastreo: Se contrastó la información contenida en la matriz de riesgos de seguridad de la información con los soportes documentales y evidencias disponibles, con el fin de evaluar la consistencia, completitud y coherencia de los registros asociados a la gestión del riesgo.

4. Procedimientos analíticos: Se realizaron procedimientos analíticos orientados a evaluar la consistencia, coherencia y alineación de la gestión de los riesgos de seguridad de la información, a partir de la integración de diferentes fuentes de información y criterios normativos. En este sentido, se efectuó el cruce entre la matriz de riesgos de seguridad de la información y la matriz de activos de información, con el fin de verificar la correspondencia en la identificación, registro y utilización de los activos asociados a los riesgos.

De igual manera, se realizó la comparación de la información analizada frente a los criterios establecidos en los procedimientos internos de la entidad, en particular el procedimiento E-02-P-009 Gestión del riesgo vigente, así como frente a la normatividad aplicable, incluyendo la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Versión 7 del DAFP.

Adicionalmente, se efectuaron validaciones en el sistema de información institucional ISOLUCIÓN, con el propósito de verificar la consistencia de los registros, la trazabilidad de la información reportada y la disponibilidad de evidencias asociadas a la ejecución de controles y al seguimiento de los riesgos, en concordancia con los lineamientos definidos por la entidad.

4. RESULTADOS

El presente informe presenta los resultados del seguimiento a la gestión de los riesgos de seguridad de la información en el Instituto Nacional de Metrología (INM), derivados del análisis de la matriz de riesgos institucional.

Los aspectos relacionados con el análisis transversal de la metodología de gestión del riesgo institucional, incluyendo su diseño, estructuración y nivel de madurez, fueron desarrollados en el "*Informe de evaluación y seguimiento a la gestión integral de riesgos de gestión en el INM*" del 15 de abril de 2026 publicado en la página web, por lo cual no son objeto de evaluación en el presente informe.

El documento se enfoca en los riesgos de seguridad de la información, en lo relacionado con la identificación de activos de información, variables de seguridad asociadas, diseño y ejecución de controles, y seguimiento a las acciones de mejora, en el marco de la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 y la normativa institucional vigente.

Los resultados se presentan organizados de acuerdo con los temas definidos para su evaluación.

4.1 Identificación de riesgos de seguridad de la información

4.1.1 Identificación de activos de información

La entidad cuenta con una matriz de activos de información con corte al 11 de noviembre de 2025, la cual se encuentra publicada en la página web institucional, según lo indicado en el Anexo No. 2 E-05-F-005-Matriz-de-activos-de-informacion-2025.

En la verificación realizada a la matriz de riesgos de seguridad de la información se identificaron nueve (9) activos de información incluidos en dicho instrumento que no se encuentran registrados en la matriz vigente de activos de información (ver Tabla No. 1).

Esta situación evidencia inconsistencias entre los instrumentos utilizados para la gestión de riesgos de seguridad de la información, en relación con el inventario

de activos de información, el cual constituye el insumo base para la identificación, análisis y evaluación de riesgos.

En consecuencia, se presenta una falta de correspondencia en la trazabilidad de la información, lo cual afecta la coherencia entre la identificación de activos, la determinación de amenazas y vulnerabilidades, y la valoración de los riesgos asociados, así como en la definición de controles y tratamientos aplicables dentro del proceso de gestión de riesgos de seguridad de la información, en tanto dichos elementos deben derivarse de un inventario de activos completo, actualizado y debidamente articulado entre los instrumentos de gestión correspondientes.

Como parte del proceso de gestión del cambio adelantado por la entidad para la implementación de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, se han definido actividades para la actualización metodológica en la gestión de activos de información y su articulación con la gestión de riesgos de seguridad de la información. (ver Anexo No. 1 – Gestión integral del riesgo 7.0).

De otro lado y como parte del proceso de gestión del cambio adelantado por la entidad para la implementación de la "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas", se han definido actividades orientadas a la actualización metodológica en la gestión de activos de información y su articulación con la gestión de riesgos de seguridad de la información (ver Anexo No. 1 – Gestión integral del riesgo 7.0).

4.1.2 Identificación de variables de seguridad de la información afectadas

En la revisión de la matriz de riesgos de seguridad de la información se evidenció que en todos los riesgos evaluados se encuentran identificadas las variables de seguridad de la información (confidencialidad, integridad y disponibilidad), en concordancia con lo establecido en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Versión 7 del DAFP. (ver Anexo 2.1 Matriz de Riesgos).

En el marco del proceso de gestión del cambio adelantado por la entidad para la implementación de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, se identificaron actividades orientadas al fortalecimiento del análisis que soporta la relación entre los eventos de riesgo y las variables de seguridad de la información, así como su articulación con los activos de información asociados en la matriz de riesgos de seguridad de la información. (ver Anexo No. 1 – Gestión integral del riesgo 7.0).

4.1.3 Articulación entre la gestión de riesgos de seguridad de la información y la gestión documental

En la revisión se evidenció que la matriz de activos de información se encuentra soportada en instrumentos de gestión documental, tales como las Tablas de Retención Documental (TRD) y las Tablas de Control de Acceso (TCA), definidos en el Plan Institucional de Archivos – PINAR 2026. (Anexo No. 3 – PINAR 2026 V1, numeral 9. Cronograma).

En la verificación se identificaron diferencias en el nivel de integración entre los instrumentos de gestión documental (TRD y TCA), la matriz de activos de información y la matriz de riesgos de seguridad de la información, particularmente en la identificación, clasificación y utilización de los activos en el proceso de gestión del riesgo. (ver Tabla No. 1).

Adicionalmente, en el marco del Plan Institucional de Archivos – PINAR 2026, se contemplan actividades para la actualización de las Tablas de Retención Documental (TRD) y de las Tablas de Control de Acceso (TCA) entre mayo y diciembre de 2026, las cuales se encuentran vinculadas a la gestión de los activos de información y a su actualización en la matriz institucional.

4.2 Matriz de riesgos de seguridad de la información vigencia 2026

Se realizó el seguimiento a la matriz de riesgos de seguridad de la información, con corte al 27 de abril de 2026, con el fin de evaluar el estado de gestión de los riesgos, la ejecución de los controles definidos, la materialización de eventos de riesgo y el avance de los planes de mejoramiento asociados.

La revisión abarcó la totalidad de los riesgos de seguridad de la información identificados por la entidad, correspondientes a 11 procesos institucionales, que en conjunto agrupan 26 riesgos y 25 controles asociados. Se precisa que el proceso de Administración del Sistema Integrado de Gestión cuenta con 3 riesgos y 2 controles. La clasificación de los controles se realizó conforme a su naturaleza funcional, identificándose 17 controles preventivos, 2 detectivos y 6 correctivos (ver Tabla No. 2).

En relación con la ejecución de los controles, se verificó la disponibilidad de soportes documentales asociados a su implementación mediante la revisión de las carpetas compartidas por la Oficina Asesora de Planeación (OAP), conforme a lo establecido en el procedimiento E-02-P-009 “Gestión del Riesgo”, versión 2.

4.2.1 Diseño y ejecución de controles

En relación con el diseño y ejecución de controles de seguridad de la información, se identificaron debilidades en un (1) proceso institucional, asociadas a la definición, documentación y efectividad de los controles establecidos en la matriz de riesgos.

(i) Para el proceso **A-04 Gestión de Talento Humano – Riesgo SI-20**, se identificó debilidades en la efectividad del control definido, de acuerdo con el seguimiento reportado por la primera línea de defensa. Lo anterior, debido a limitaciones técnicas en la gestión de accesos a la matriz sociodemográfica, dado que la restricción individual de permisos no es viable sin afectar el acceso a la totalidad de la carpeta, lo que deriva en la disponibilidad general de la información para el personal del proceso, evidenciando debilidades en el diseño y su capacidad para mitigar el riesgo identificado. (Ver Anexo 2.1 Matriz de Riesgos).

Estas situaciones afectan la capacidad de mitigación de los riesgos de seguridad de la información y limitan la verificación de la efectividad de los controles establecidos.

Lo anterior no se encuentra alineado con lo establecido en el procedimiento E-02-P-009 "Gestión del Riesgo", versión 2 - numeral 6.1.2 "*Primera Línea de Defensa*", el cual establece la responsabilidad de definir, adoptar, implementar y realizar seguimiento a los controles para la mitigación de los riesgos.

4.2.1 Seguimiento a la ejecución de controles

En el desarrollo del seguimiento a la ejecución de los controles de seguridad de la información, se verificó la disponibilidad de soportes documentales asociados a su implementación, con el fin de validar su trazabilidad y cumplimiento dentro del proceso de gestión del riesgo.

Como resultado de la verificación realizada en las carpetas compartidas dispuestas por la OAP, se evidenció que para ocho (8) riesgos de seguridad de la información (ver Tabla No. 3) no se identificaron soportes documentales que permitan validar la ejecución de los controles definidos en la matriz de riesgos. (ver Anexo No. 4 "Ejecución de Controles – Riesgos de Seguridad de la Información").

Esta situación limita la verificación de la ejecución de los controles, así como su trazabilidad y seguimiento, impidiendo la validación de su cumplimiento conforme a lo establecido en el procedimiento E-02-P-009 "Gestión del Riesgo", versión 2 - numeral 6.4.2.7.1.1 "*Registro del seguimiento – Proceso de cargue de evidencias*", el cual establece la obligación de registrar las evidencias en el

repositorio institucional administrado por la OAP (SharePoint), como soporte del seguimiento y ejecución de los controles.

4.3 Plan de Mejoramiento No. 125 SISEPM

En el marco de la evaluación del Plan de Mejoramiento No. 125 asociado a la matriz de riesgos de seguridad de la información, se realizó la revisión de las acciones definidas, abarcando la verificación de su implementación, así como la evaluación de su eficacia y efectividad, a partir de las evidencias aportadas por la dependencia responsable. (Ver Anexo No. 5 Seguimiento Plan de Mejoramiento No. 125 SISEPM).

Hallazgo No. 1: Ausencia de diligenciamiento del Plan de Acción (acciones para abordar riesgos) en los riesgos residuales clasificados en las categorías moderado, alto y extremo y en los indicadores clave de riesgo.

Resultado: Se evidenció un cumplimiento parcial en la ejecución de las actividades evaluadas en el plan de mejoramiento. Las actividades 1 y 2 cuentan con soportes que permiten verificar su ejecución; sin embargo, las evidencias aportadas no permiten establecer de manera suficiente su contribución al fortalecimiento de la gestión de los riesgos de seguridad de la información.

Por su parte, la actividad 3 no presenta evidencia de la definición ni del reporte de indicadores clave de riesgo (KRI) para los riesgos SI-1, SI-2, SI-3, SI-14, SI-15, SI-17, SI-18, SI-19, SI-20, SI-21 y SI-26, lo cual limita la medición, seguimiento y monitoreo de dichos riesgos en el Sistema Integrado de Gestión.

En consecuencia, la efectividad de los controles asociados al plan de mejoramiento se considera limitada, en la medida en que las acciones implementadas no permiten asegurar de forma suficiente la medición continua del comportamiento de los riesgos ni el fortalecimiento del monitoreo a través de indicadores clave de riesgo (KRI).

Hallazgo No. 2: Ausencia de seguimiento a los riesgos de seguridad de la información

Resultado: Se evidenció un cumplimiento parcial de las acciones objeto de evaluación. Respecto de la actividad 1, se observó soporte documental correspondiente al registro en el formato de matriz de riesgos para el seguimiento por parte de la primera y segunda línea de defensa; no obstante, la evidencia aportada no permite determinar de manera objetiva su efectividad ni su contribución al fortalecimiento del control asociado al riesgo evaluado.

En relación con la actividad 2, se identificaron debilidades en la calidad y suficiencia de las actividades de seguimiento y verificación efectuadas por la segunda línea de defensa, situación que limita la validación de la efectividad de la acción implementada.

En consecuencia, no se evidenciaron elementos de juicio suficientes que permitan concluir, de manera verificable y objetiva, que las acciones implementadas hayan contribuido al fortalecimiento del esquema de seguimiento y control de los riesgos de seguridad de la información.

5. CONCLUSIONES

1. Se evidenciaron debilidades en la consistencia e integración entre la matriz de activos de información y la matriz de riesgos de seguridad de la información, lo cual limita su utilización como insumo confiable para la identificación y gestión de los riesgos**.** Estas debilidades evidencian la necesidad de fortalecer la articulación de los insumos utilizados para la gestión de los riesgos de seguridad de la información, a fin de asegurar una adecuada identificación, valoración y tratamiento de los riesgos, con información confiable y completa.

2. Se evidenció que la entidad ha incorporado en la matriz de riesgos de seguridad de la información los principios de confidencialidad, integridad y disponibilidad, en concordancia con los lineamientos aplicables en materia de gestión de riesgos de seguridad de la información. Sin embargo, se identificaron oportunidades de mejora en la articulación técnica entre dichas variables, los eventos de riesgo y los activos de información asociados, particularmente en aspectos de consistencia en la clasificación y trazabilidad de la información registrada.

Esta situación puede limitar la precisión del análisis, la adecuada valoración de los riesgos y la efectividad en la toma de decisiones para el tratamiento y control de estos. En consecuencia, se recomienda fortalecer los criterios de asociación y documentación dentro de la matriz, de manera que se garantice una gestión integral, consistente y verificable de los riesgos de seguridad de la información.

3. La articulación entre la gestión documental, la gestión de activos de información y la gestión de riesgos de seguridad de la información no se encuentra plenamente consolidada, lo que genera diferencias en la aplicación de criterios para la identificación y clasificación de los activos.

4. Se evidencian debilidades en el diseño y la ejecución de los controles asociados a los riesgos SI-20, relacionadas con la definición del control, su documentación y en línea con buenas prácticas de la ISO/IEC 27001, lo cual afecta su capacidad de mitigación y evaluación de efectividad.

5. Se evidencian debilidades en el seguimiento a la ejecución de los controles de ocho (8) riesgos de seguridad de la información, debido a la ausencia de soportes documentales en la carpeta compartida de la OAP que permitan verificar su implementación, limitando la trazabilidad, verificación y seguimiento del cumplimiento de los controles asociados a la ISO 27001:2022

6. El Plan de Mejoramiento No. 125 presenta un cumplimiento parcial de las acciones definidas. Se evidencian debilidades en la definición de indicadores clave de riesgo (KRI), en el seguimiento por parte de la segunda línea de defensa (contratista encargada de la gestión de los riesgos de seguridad de la información) y en la suficiencia de las evidencias que soportan la eficacia y efectividad de las acciones implementadas. En consecuencia, no es posible establecer la efectividad del plan en el fortalecimiento de la gestión de los riesgos de seguridad de la información.

5.1 NO CONFORMIDADES

Es el incumplimiento de un requisito establecido (legal, normativo, contractual, procedimental o de gestión). Representa una desviación significativa que afecta la conformidad del proceso, producto o servicio con respecto a lo que se espera. Requieren la suscripción de Plan de Mejoramiento avalados por el líder del proceso en el aplicativo SISEPM.

5.1.1 Debilidades en la definición, documentación y ejecución de los controles (diseño y ejecución de controles)

Condición: En el proceso A-04 Gestión de Talento Humano – Riesgo SI-20, el control definido presenta limitaciones en su diseño y efectividad, conforme al seguimiento realizado por la primera línea de defensa, debido a restricciones insuficientes en la administración de accesos a la matriz sociodemográfica, permitiendo que información del proceso se encuentre disponible para un número amplio de usuarios del área, sin evidencia de criterios diferenciados de acceso según roles o necesidad funcional.

Criterio: Procedimiento E-02-P-009 "Gestión del Riesgo", numeral 6.1.2 "Primera Línea de Defensa", el cual establece la responsabilidad de definir, adoptar, aplicar y realizar seguimiento a los controles para la adecuada gestión de los riesgos, asegurando su documentación, implementación y evaluación de efectividad.

Causa: Debilidades en la definición y documentación de los controles en la matriz de riesgos de seguridad de la información, así como limitaciones en la

revisión de la efectividad de los controles existentes frente a las condiciones operativas de acceso y gestión de la información.

Efecto/ potencial del riesgo: Debilidades en la mitigación efectiva de los riesgos de seguridad de la información, afectación de la trazabilidad y confiabilidad de los controles definidos, así como limitaciones en la evaluación de su efectividad, lo que podría incrementar la probabilidad de materialización de incidentes relacionados con la confidencialidad, integridad o disponibilidad de la información.

Recomendación: Revisar y reformular el control asociado al riesgo SI-20 en el proceso A-04, de manera que garantice su aplicabilidad, accesibilidad controlada y efectividad en la mitigación del riesgo identificado.

5.1.2 Ausencia de soporte documental para el seguimiento a la ejecución de controles de seguridad de la información

Condición: En la revisión realizada al seguimiento de la ejecución de los controles de seguridad de la información, se evidenció que para ocho (8) riesgos no se encontraron soportes documentales en la carpeta compartida definida por la OAP para el cargue de evidencias, que permitieran verificar la ejecución y seguimiento de los controles establecidos en la matriz de riesgos.

Criterio: Procedimiento E-02-P-009 "Gestión del Riesgo", numeral 6.4.2.7.1.1 "Registro del seguimiento – Proceso de cargue de evidencias".

Causa: Debilidades en la aplicación y seguimiento del procedimiento establecido para el cargue y gestión de evidencias de ejecución de controles, así como en los mecanismos de control documental y verificación de cumplimiento frente a los soportes requeridos en la matriz de riesgos.

Efecto/potencial riesgo: Limitaciones en la trazabilidad, verificación y seguimiento de la ejecución de los controles de seguridad de la información, afectando la capacidad de evaluar su cumplimiento y efectividad, así como incrementando el riesgo de que situaciones asociadas a la confidencialidad, integridad y disponibilidad de la información no sean detectadas o gestionadas oportunamente.

Recomendación: Fortalecer los mecanismos de control y seguimiento asociados al cargue, administración y conservación de evidencias de ejecución de controles de seguridad de la información, asegurando que los soportes documentales definidos en la matriz de riesgos se encuentren disponibles, completos, actualizados y verificables conforme al procedimiento establecido.

5.2 OBSERVACIONES

Es un hallazgo detectado durante el seguimiento que, si bien no constituye una no conformidad, podría convertirse en una si no se controla o mejora. También puede referirse a aspectos que no están alineados con las mejores prácticas o que generan dudas razonables al auditor. Queda a discreción de la unidad auditada, la toma de acciones correctivas para evitar la materialización de un riesgo que lleve a una No conformidad. Las observaciones no requieren la suscripción de Plan de Mejoramiento en SISEPM.
A continuación, se detallan:

5.2.1 Durante la verificación de la matriz de riesgos de seguridad de la información se identificaron nueve (9) activos de información registrados en dicho instrumento que no se encuentran incorporados en la matriz de activos de información vigente de la entidad. Esta situación evidencia inconsistencias en la articulación y trazabilidad de la información utilizada para la gestión de riesgos de seguridad de la información, lo que puede afectar la integridad, confiabilidad y completitud del proceso de identificación, valoración y tratamiento de riesgos, así como la adecuada definición de controles y medidas de mitigación orientadas a la protección de la información institucional.

5.3 OPORTUNIDADES DE MEJORA

Es una sugerencia basada en el juicio del auditor, orientada al fortalecimiento de los procesos o sistemas auditados. No implica incumplimiento ni riesgo inmediato, pero representa una posibilidad de optimizar el desempeño, aumenta la eficiencia o eleva la calidad. Estas no requieren suscripción de Plan de Mejoramiento.
A continuación, se detallan:

5.3.1 Fortalecer la integración entre la matriz de activos de información, los instrumentos de gestión documental y la matriz de riesgos de seguridad de la información, mediante la definición de criterios unificados para la identificación, clasificación y actualización de los activos, asegurando su consistencia en los diferentes instrumentos institucionales.

5.3.2 Fortalecer la relación técnica entre los eventos de riesgo, los activos de información y los principios de seguridad de la información (confidencialidad, integridad y disponibilidad), con el fin de mejorar la calidad del análisis y la coherencia en la valoración de los riesgos.

5.3.3 Se sugiere fortalecer la definición, documentación y alineación de los controles asociados a los riesgos de seguridad de la información, asegurando que estos incluyan de manera completa su descripción, relación con los controles

de referencia de la ISO 27001:2022 y su aplicabilidad operativa dentro de los procesos.

5.3.4 Se sugiere fortalecer el proceso de seguimiento a la ejecución de los controles de seguridad de la información, asegurando la disponibilidad, completitud y trazabilidad de los soportes documentales en el repositorio definido por la OAP.

5.3.5 Se recomienda robustecer la calidad, completitud y trazabilidad de las evidencias asociadas a las acciones del plan de mejoramiento, de manera que permitan verificar de forma suficiente su implementación, eficacia, efectividad y contribución a la mitigación de los hallazgos identificados.

Luz Marina Doria Cavadia

Firmado digitalmente por Luz Marina Doria Cavadia

Luz Marina Doria Cavadía
Jefe Oficina de Control Interno
2026-05-11

Elaborado por. Leidy Liliana Ríos Martínez

6. ANEXOS

6.1 Marco Normativo

1. Decreto 648 de 2017 "Por medio del cual se modifica y adiciona el Decreto 1083 de 2015, Reglamento Único del Sector de la Función Pública".

2. Decreto 1081 de 2015 "Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República."

3. Decreto 1083 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública". Artículo 2.2.23.2 "Actualización del modelo estándar de Control Interno".

4. Decreto 1499 de 2017 "Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015".

5. Ley 1474 de 2011 "Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública."

6. Ley 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones."

7. Decreto 1078 de 2015 Decreto Único Reglamentario del Sector TIC, Artículo 2.2.17.1.4. Definiciones Generales

8. Manual Operativo del Modelo Integrado de Planeación y Gestión-MIPG, versión 5, marzo 2023, Consejo para la Gestión y Desempeño Institucional.

9. Guía rol de las unidades u oficinas de control interno, auditoría interna o quien haga sus veces – Versión 3 – septiembre de 2023 – Rol de Evaluación de la Gestión del Riesgo – Páginas 53.

10. Guía para la Gestión y Clasificación de Activos de Información de MINTIC, Numeral 5 Definiciones.

11. E-02-P-009 Procedimiento Gestión del Riesgo, versión 2 del 12 de mayo de 2025, del Sistema Integrado de Gestión para consulta en el aplicativo ISOLUCION.

12. E-05-P-004 Procedimiento de Gestión de Activos de Información, versión 5 del 30 de diciembre de 2024.

13. A-03-P-010 Procedimiento de Tablas de Control de Acceso Documental, versión 1 del 28 de abril de 2023.

14. E-05-M-006 Manual Técnico del Sistema de Gestión de Seguridad de la Información.

6.2 Tablas

Tabla No. 1 Evidencias de activos de información sin identificación

Proceso	Riesgos de Seguridad de la Información	Activos de información sin identificación
(E-01) Direccionamiento Estratégico y Planeación	**SI-1**	Información publicada en redes sociales
(E-05) Gestión de Tecnologías de la Información	**SI-7**	Sistemas internos
	SI-12	Directorio activo
(M-01) Gestión de patrones nacionales y sistemas medición **(M-03) Producción de Materiales de Referencia y Desarrollo de Métodos Analíticos**	**SI-15**	Registros técnicos de las actividades del laboratorio para el proceso M-01 Servicios de calibración y Medición Metrológica
	SI-16	Registros técnicos de las actividades del laboratorio para el proceso M-01 Servicios de calibración y Medición Metrológica
(M-08) Gestión de patrones nacionales y sistemas medición **(M-03) Producción de Materiales de Referencia y Desarrollo de Métodos Analíticos**	**SI-14**	Registros técnicos de las actividades del laboratorio para el proceso M-08 Gestión de Patrones Nacionales y Sistemas de Medición
(A-04) Gestión de Talento Humano	**SI-20**	Información empleados
(A-05) Gestión Administrativa	**SI-10**	Instalaciones
	SI-26	Instalaciones

Fuente: Elaborado por Oficina de Control Interno

Tabla No. 2 Riesgos de Gestión de Seguridad de la Información por Procesos

No.	Nombre del Proceso	No. de Riesgos	Controles	Tipo de Control
1	(E-01) Direccionamiento Estratégico y Planeación	1	1	Preventivos: 1 Detectivos: 0 Correctivos: 0
2	(E-02) Administración del Sistema Integrado de Gestión	3	2	Preventivos: 2 Detectivos: 0 Correctivos: 0
3	(E-03) Comunicaciones	1	1	Preventivos: 1 Detectivos: 0 Correctivos: 0
4	(E-05) Gestión de las Tecnologías de la Información	10	10	Preventivos: 3 Detectivos: 2 Correctivos: 5
5	(M-01) Servicios de Calibración y medición metrológica (M-03) Producción de Materiales de Referencia y Desarrollo de Métodos Analítico	2	2	Preventivos: 2 Detectivos: 0 Correctivos: 0
6	(M-07) Investigación, Desarrollo e Innovación	1	1	Preventivos: 1 Detectivos: 0 Correctivos: 0
7	(M-08) Gestión de patrones nacionales y sistemas medición (M-03) Producción de Materiales de Referencia y Desarrollo de Métodos Analítico	2	2	Preventivos: 2 Detectivos: 0 Correctivos: 0
8	(A-04) Gestión de Talento Humano	1	1	Preventivos: 1 Detectivos: 0 Correctivos: 0
9	(A-05) Gestión Administrativa	3	3	Preventivos: 3 Detectivos: 0 Correctivos: 0
10	(A-06) Control Disciplinario	1	1	Preventivos: 0 Detectivos: 0 Correctivos: 1

No.	Nombre del Proceso	No. de Riesgos	Controles	Tipo de Control
11	(A-07) Contratación y Adquisición de Bienes y Servicios	1	1	Preventivos: 1 Detectivos: 0 Correctivos: 0
TOTAL		**26**	**25**	**25**

Fuente: Elaborado por la Oficina de Control Interno.

Tabla No. 3 Evidencias sin soporte documental en la ejecución controles alineados a la ISO 27001:2022

Proceso	Riesgos de Seguridad de la Información	Controles relacionados alineados con la ISO 27001:2022
(E-01) Direccionamiento Estratégico y Planeación	**SI-1**	A.5.17 Authentication information
(E-02) Administración del Sistema Integrado de Gestión	**SI-22**	No se muestra el control relacionado con la ISO 27001:2022
	SI-23	No cuenta con el control relacionado con la ISO 27001:2022
	SI-24	A5.18 Derechos de acceso
(M-08) Gestión de patrones nacionales y sistemas medición **(M-03) Producción de Materiales de Referencia y Desarrollo de Métodos Analíticos**	**SI-14**	A.5.36 Cumplimiento de políticas, normas y estándares de seguridad de la información
	SI-17	A.5.36 Cumplimiento de políticas, normas y estándares de seguridad de la información
(A-06) Control Disciplinario	**SI-3**	A.8.3 Restricción de acceso a la información
(A-07) Contratación y Adquisición de Bienes y Servicios	**SI-19**	A.5.36 Cumplimiento de políticas, normas y estándares de seguridad de la información

Fuente: Elaborado por Oficina de Control Interno