Instituto Nacional de Metrología de Colombia

Informe final de Evaluación a los Riesgos de Seguridad de la Información del INM

Oficina de Control Interno

Bogotá, D.C.

2025-07-04

CONTENIDO

Página.

1. INTRODUCCIÓN

En atención a las actividades establecidas en el Plan Anual de Auditoría aprobado para la vigencia 2025, específicamente en el rol de evaluación y gestión del riesgo, se presenta el informe de evaluación y seguimiento al mapa de riesgos de seguridad del Instituto Nacional de Metrología. En desarrollo del ejercicio se verificó el avance y la efectividad de las acciones de control propuestas por los distintos procesos institucionales para su mitigación.

El desarrollo de esta evaluación se hizo en el marco de los lineamientos establecidos en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, versión 6, de noviembre de 2022, expedida por el Departamento Administrativo de la Función Pública. Asimismo, se tuvo en cuenta un conjunto de referencias normativas, tanto de carácter interno como externo, que orientan la gestión del riesgo en el sector público y que sirvieron de base para la elaboración del presente documento.

En el numeral 6.1. del acápite de anexos de este informe, se relacionan los principales lineamientos normativos que sirvieron de sustento para la evaluación.

2. ALCANCE

El período objeto de análisis comprende las actividades ejecutadas en el primer semestre de 2025, incluyendo la revisión del mapa de riesgos de seguridad de la información aprobado en la sesión No. 3 del Comité Institucional de Gestión y Desempeño, realizada el 26 de marzo de 2025.

3. DESCRIPCIÓN METODOLÓGICA

Para el ejercicio de la evaluación, se aplicaron procedimientos de auditoría y se ejecutaron las siguientes actividades:

- Se revisó la última versión del mapa de riesgos de seguridad de la información del Instituto, aprobado para la vigencia 2025.
- Se analizó la información de la matriz de riesgos de seguridad de la información, con el fin de verificar los riesgos y controles identificados.
- Se examinó la trazabilidad del seguimiento realizado por los responsables de cada proceso, a los mapas de riesgos de seguridad de la información.
- Se valoró el estado actualizado de los riesgos y los controles asociados, considerando los criterios establecidos en la Guía para la Administración

del Riesgo y el diseño de controles en entidades públicas, versión 6 del 22 de noviembre de 2022, con el fin de determinar su pertinencia, eficacia y nivel de implementación.

Estos procedimientos permitieron obtener elementos de juicio suficientes para emitir conclusiones sobre la gestión del riesgo de seguridad de la información y formular las recomendaciones correspondientes.

4. RESULTADOS

4.1 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Como resultado del proceso de evaluación, se identificaron riesgos de seguridad de la información asociados a 11 procesos clave de la entidad. En total, se formularon 30 riesgos y 31 controles, clasificados de la siguiente manera: 2 controles detectivos, 24 controles preventivos y 5 controles correctivos, tal como se detalla en la Tabla No. 2 del numeral 6.3. del acápite de Anexos.

En la Imagen 1, del punto 6.2. numeral 6 del acápite de anexos, se muestra la matriz de riesgos de seguridad de la información vigente para el año 2025.

A continuación, se presentan los resultados correspondientes a la verificación realizada por la Oficina de Control Interno (OCI), como se muestra en la Tabla No. 1, donde se detalla lo evidenciado para cada uno de los procesos institucionales.

Tabla No. 1 Resultados de los riesgos de seguridad de la información

Proceso	Resultados de verificación realizada por la OCI
1.E-01 Direccionamiento Estratégico y Planeación	-En el primer trimestre de 2025, no se evidenció seguimiento del riesgo por parte de la primera línea de defensa. - No se evidencian soportes documentales o registros que respalden la implementación efectiva de los controles asociados. Específicamente, no se presenta información que relacione la "*Descripción del Control*" con acciones verificables, ni se evidencia el vínculo operativo con los controles correspondientes a la norma ISO/IEC 27001:2022. -Se evidenció que los riesgos residuales clasificados en las categorías de moderado, alto y extremo, identificados en el proceso, no cuentan con un Plan de Acción debidamente diligenciado en la matriz de riesgos de seguridad de la información. Los campos correspondientes a la descripción de

Proceso	Resultados de verificación realizada por la OCI
	las acciones, responsables, fechas de implementación e indicadores clave de seguimiento se encuentran sin diligenciar.
2.(E-02) Administración del Sistema Integrado de Gestión	Se evidenció la materialización del riesgo identificado como: *"La ausencia de monitoreo de disponibilidad del sistema de información Isolucion puede ocasionar que haya fallas de conexión a la aplicación, lo que causa la pérdida de disponibilidad de la información en Isolucion"*. Durante el seguimiento, el líder del proceso mencionó que "*Se materializa el riesgo: No hubo disponibilidad de la aplicación Isolucion por tres días del 26 al 28 de marzo, debido a que generaba lentitud y se expiraba la sesión y ya no permita cargar los módulos. La situación fue atendida por la Oficina de Informática y Desarrollo Tecnológico (OIDT), que intervino asignando recursos adicionales a la base de datos, logrando restablecer el servicio".* -En la matriz de riesgos de seguridad de la información no se encontró documentada la sección correspondiente a la "*Evaluación del riesgo – Valoración de los controles*" para los siguientes riesgos: *"La ausencia de monitoreo de disponibilidad del sistema de información Isolucion puede ocasionar que haya fallas de conexión a la aplicación, lo que causa la pérdida de disponibilidad de la información en Isolucion."* *"Por uso de contraseñas débiles en Isolucion puede ocurrir un acceso no autorizado a la información, lo que causaría una pérdida de confidencialidad de la información en Isolucion."* -Se evidenció que los riesgos residuales clasificados en las categorías de moderado, alto y extremo, identificados en el proceso, no cuentan con un Plan de Acción debidamente diligenciado en la matriz de riesgos de seguridad de la información. Los campos correspondientes a la descripción de las acciones, responsables, fechas de implementación e indicadores clave de seguimiento se encuentran sin diligenciar.
3.(E-03) Comunicaciones	-Se evidenció que los riesgos residuales clasificados en las categorías de moderado, alto y extremo, identificados en el proceso, no cuentan con un Plan de Acción debidamente diligenciado en la matriz de riesgos de seguridad de la información. Los campos correspondientes a la descripción de

Proceso	Resultados de verificación realizada por la OCI
	las acciones, responsables, fechas de implementación e indicadores clave de seguimiento se encuentran sin diligenciar. -Para la vigencia 2025, se evidenció que se ha realizado seguimiento y registro de dicha información relacionada con la ejecución de controles de riesgo de manera periódica (trimestral), en lo correspondiente a la *"Descripción del Control*" y con el "*Control relacionado ISO/IEC 27001:2022".*
4. (E-05) Gestión de las Tecnologías de la Información	-Se identificó que las descripciones consignadas en el seguimiento de varios riesgos del proceso no presentan una relación clara, específica ni verificable con las causas o efectos de los riesgos documentados, lo que dificulta la trazabilidad y evaluación efectiva de las acciones adoptadas. A continuación, se citan algunos ejemplos representativos: **Riesgo 1:** *"La ausencia de capacitación de personal en el manejo de phishing, ausencia de monitoreo de seguridad, ausencia de backups, ausencia de segmentación en las redes y ausencia de actualización de software de sistema operativo, facilita la posibilidad de un secuestro de información..."* **Seguimiento reportado:** "*Está pendiente plan de trabajo en 2025 de actualización de sistemas operativos obsoletos de los servidores*." El seguimiento se limita a una mención general, sin indicar acciones concretas, responsables, fechas ni relación directa con todos los factores de riesgo mencionados. **Riesgo 2:** *"Ausencia de herramientas de seguridad, ausencia de monitoreo de seguridad y ausencia de políticas de seguridad de la información del personal pueden ocasionar la intrusión de un ataque informático, lo que puede causar la pérdida de disponibilidad de la información en los servidores "* **Seguimiento reportado:** "*Cerrar este plan de acción, pues el monitoreo se realiza con el SOC*." La justificación del cierre es ambigua y no se adjuntan evidencias que demuestren que todos los aspectos del riesgo han sido mitigados.

Proceso	Resultados de verificación realizada por la OCI
	Riesgo 3: *"El uso de contraseñas débiles, la ausencia de políticas de seguridad en el manejo de credenciales, no cumplimiento de procedimientos de gestión de usuarios y ausencia de encripción en la autenticación permite accesos no autorizados a la información, lo cual causaría la pérdida de la confidencialidad de la información de los sistemas internos".* **Seguimiento reportado:** "*Pendiente hacer plan para 2025 de continuación de inclusión de aplicaciones internas con la autenticación del directorio activo.*" No se especifica el alcance, ni los plazos o responsables de la acción, y se omiten medidas intermedias de mitigación. -Se evidenció que los siguientes riesgos no cuentan con seguimiento documentado, correspondiente al primer trimestre de 2025: *"Ausencia de supervisión de derechos de acceso, la falta de capacitación del personal en políticas de seguridad de la información y la ausencia de obligación contractual del cumplimiento de políticas de seguridad de la información..."* *"Ausencia de políticas de backups y falta de recursos para backups puede ocasionar que no se respalde adecuadamente la información crítica..."* La falta de seguimiento impide verificar el avance o estancamiento en la gestión de estos riesgos y limita la toma de decisiones basadas en evidencia. Para al menos cuatro (4) de los riesgos evaluados, se evidenció que los riesgos residuales clasificados en las categorías de moderado, alto y extremo, identificados en el proceso, no cuentan con un Plan de Acción debidamente diligenciado en la matriz de riesgos de seguridad de la información. Los campos correspondientes a la descripción de las acciones, responsables, fechas de implementación e indicadores clave de seguimiento se encuentran sin diligenciar.
5. (M-03) Producción de Materiales de Referencia y	-En la matriz de riesgos de seguridad de la información, no se evidenció el diligenciamiento de la información del indicador clave del riesgo, asociado en el Plan de Acción (acciones para abordar riesgos).

Proceso	Resultados de verificación realizada por la OCI
Desarrollo de Métodos Analíticos	
6.(M-07) Investigación, Desarrollo e Innovación	-En la matriz de riesgos de seguridad de la información, no se evidenció el diligenciamiento de la información del indicador clave del riesgo, asociado en el Plan de Acción (acciones para abordar riesgos).
7. (M-08) Gestión de patrones nacionales y sistemas medición	-En la matriz de riesgos de seguridad de la información, no se evidenció el diligenciamiento de la información del indicador clave del riesgo, asociado en el Plan de Acción (acciones para abordar riesgos).
8. (A-04) Gestión de Talento Humano	-No se evidenció seguimiento del riesgo para el primer trimestre de 2025. -En la matriz de riesgos de seguridad de la información, no se evidenció el diligenciamiento de la información del indicador clave del riesgo, asociado en el Plan de Acción (acciones para abordar riesgos).
9.(A-05) Gestión Administrativa	No se evidenció el seguimiento del riesgo correspondiente al primer trimestre de 2025, en términos de fecha de revisión ni responsable asignado para los siguientes riesgos críticos, asociados a la disponibilidad de los servicios del Instituto: *"Ausencia de respaldo de la planta eléctrica, fallas del proveedor de servicio de energía ocasionan la no disponibilidad de los servicios del datacenter, por lo cual hay pérdida de disponibilidad de todos los servicios del INM que están en las instalaciones."* *"La ausencia de controles de acceso físico a los centros de cableado o datacenter puede ocasionar la desconexión o apagado de elementos de comunicaciones por parte de alguien no autorizado, lo que causa la indisponibilidad de la información del INM."* La falta de seguimiento impide verificar el estado actual de estos riesgos, su nivel de exposición y las acciones implementadas para su mitigación. Dada la criticidad de estos escenarios, relacionados directamente con la continuidad operativa y la seguridad física de la infraestructura tecnológica, se considera indispensable establecer mecanismos de control, registro y monitoreo efectivos.

Proceso	Resultados de verificación realizada por la OCI
	-En la matriz de riesgos de seguridad de la información, no se evidenció el diligenciamiento de la información del indicador clave del riesgo, asociado en el Plan de Acción (acciones para abordar riesgos).
10. (A-06) Control Disciplinario	-En la matriz de riesgos de seguridad de la información, no se evidenció el diligenciamiento de la información del indicador clave del riesgo, asociado en el Plan de Acción (acciones para abordar riesgos).
11. (A-07) Contratación y Adquisición de Bienes y Servicios	- Durante el primer trimestre de 2025, no se evidenció el seguimiento al riesgo identificado como: *"La gestión no adecuada de disposición de la información sensible en los repositorios definidos por la entidad y la ausencia de gestión de restricciones a las carpetas compartidas puede ocasionar un acceso no autorizado a dicha información y puede causar una pérdida de confidencialidad de la información de contratos."* -Adicionalmente, en la matriz de riesgos de seguridad de la información, no se evidenció el diligenciamiento de la información del indicador clave del riesgo, asociado en el Plan de Acción (acciones para abordar riesgos).

5. CONCLUSIONES

Con base en la revisión documental, análisis de registros en el Sistema Integrado de Gestión y en la matriz de riesgos de seguridad de la información, se observan esfuerzos recientes en el fortalecimiento del seguimiento a los riesgos de seguridad de la información. Sin embargo, se identificaron brechas importantes en la implementación, diligenciamiento y trazabilidad de la gestión de estos.

Se identificaron riesgos que han sido formulados, pero no evaluados, sin planes de acción diligenciados para los riesgos residuales clasificados en las categorías moderado, alto y extremo, ni indicadores clave de riesgos, así como casos de materialización de riesgos sin evidencia de una respuesta preventiva oportuna. Asimismo, algunos responsables de procesos no han realizado el seguimiento trimestral o han reportado información insuficiente.

A continuación, se relacionan algunos aspectos relevantes que resultaron de la evaluación de los riesgos de seguridad de la información en el INM:

- La gestión del riesgo de seguridad de la información en el INM presenta avances en la identificación y formulación de riesgos y controles, pero se

encuentra en un estado incipiente o incompleto en lo que respecta al ciclo completo de gestión: evaluación, tratamiento, seguimiento y mejora continua.

- Se evidenciaron inconsistencias en la claridad de la información reportada en el seguimiento de los riesgos de seguridad de la información, así como falta de diligenciamiento de la información del indicador clave del riesgo asociado al Plan de Acción (acciones para abordar riesgos), específicamente para los riesgos residuales clasificados en las categorías moderado, alto y extremo, lo que limita la trazabilidad, efectividad del control interno y capacidad de reacción frente a incidentes.

- La materialización de un riesgo identificado relacionado con indisponibilidad de la información en la aplicación ISOLUCION refuerza la necesidad de fortalecer el monitoreo y la respuesta oportuna a condiciones críticas.

Es de anotar que, al solicitar evidencia de los 31 controles reportados, se indicó que estos se encuentran en las herramientas tecnológicas de la entidad asociadas a cada proceso. Sin embargo, en la verificación realizada no se encontraron evidencias claras, completas ni consistentes en los seguimientos trimestrales. Esta falta de trazabilidad limita la posibilidad de validar la efectividad de los controles implementados y dificulta la correcta ejecución de la evaluación del riesgo y la valoración de los controles, tal como debe documentarse en la matriz de riesgos de seguridad de la información.

La ausencia de seguimiento adecuado y oportuno genera una mayor probabilidad de materialización de riesgos, con impactos que pueden afectar la disponibilidad, integridad y confidencialidad de la información, así como la reputación institucional y la sostenibilidad operativa del Instituto.

En este sentido, el análisis periódico y riguroso de los riesgos de seguridad de la información, representa un referente estratégico para la mejora continua del Sistema Integrado de Gestión (SIG) de la entidad.

En consecuencia, se dejarán algunas no conformidades, observaciones y oportunidades de mejora, que sirvan de insumo para el fortalecimiento de la gestión de los riesgos de seguridad de la información del INM.

5.1 NO CONFORMIDADES

Estas no conformidades, requieren la suscripción de Plan de Mejoramiento avalados por la Dirección General y comunicado vía correo electrónico a la Oficina de Control Interno, para su respectivo seguimiento.

5.1.1 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.

Condición: Se evidenció que los riesgos residuales clasificados en las categorías de moderado, alto y extremo, identificados en el proceso, no cuentan con un Plan de Acción debidamente diligenciado en la matriz de riesgos de seguridad de la información. Los campos correspondientes a la descripción de las acciones, responsables, fechas de implementación e indicadores clave se encuentran incompletos o ausentes. (Ver Tabla No. 1 Resultados de los riesgos de seguridad de la información).

Criterio: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, versión 6 – DAFP; ISO/IEC 27001:2022, numeral 6.1 – Acciones para abordar riesgos y oportunidades; Documento E-02-P-009 Gestión del riesgo - versión 2 de 2025.

Causa: Falta de seguimiento y control por parte de la primera y segunda línea de defensa sobre el diligenciamiento y actualización de la matriz de riesgos, así como posible desconocimiento o desatención a los lineamientos establecidos para la gestión del riesgo.

Efecto/potencial del riesgo: Se limita el tratamiento efectivo de los riesgos residuales, lo que podría derivar en la materialización de amenazas que comprometan la confidencialidad, integridad y disponibilidad de la información. Esto podría conllevar impactos operativos y reputacionales para la entidad.

Recomendación: Hacer exigible el diligenciamiento completo del Plan de Acción en los riesgos residuales clasificados en las categorías moderado, alto y extremo; capacitar a los responsables de cada proceso en la correcta gestión y reporte de riesgos; implementar una revisión periódica por parte de la segunda línea de defensa para verificar cumplimiento.

5.1.2 Ausencia de seguimiento a los riesgos de seguridad de la información

Condición: Ausencia de seguimiento documentado y verificable para los riesgos (E-01; E-05; A-04; A-05 y A-07), de conformidad con los lineamientos establecidos para la gestión del riesgo institucional.

Criterio: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 6 – DAFP; Manual Operativo del MIPG, versión 5 – marzo de 2023; Documento E-02-P-009 Gestión del riesgo - versión 2 de 2025.

Causa: - Claridad en los mecanismos formales de verificación y control periódico del seguimiento; posible desconocimiento o falta de apropiación de roles y responsabilidades por parte de los responsables del proceso; debilidad en el acompañamiento y supervisión de la segunda línea de defensa.

Efecto/potencial del riesgo: Incremento en la probabilidad de materialización de los riesgos de seguridad de la información; impacto negativo en la continuidad operativa y reputación institucional.

Recomendación: Realizar seguimiento periódico a la matriz de riesgos de seguridad de la información, asegurando que cada actividad de seguimiento quede debidamente documentada y con trazabilidad verificable. Adicionalmente, es recomendable implementar una matriz de control y trazabilidad que consolide el estado y avance de los riesgos y planes de acción registrados. Esta matriz requiere ser supervisada por la segunda línea de defensa, con el fin de garantizar el cumplimiento de los lineamientos institucionales y normativos aplicables.

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.

5.2.1 Ambigüedad en la redacción de riesgos de seguridad de la información

Condición: En los seguimientos reportados, se identificó ambigüedad en la redacción, falta de especificidad en las acciones descritas y ausencia de evidencias que permitan validar el cierre o avance de los riesgos de seguridad de la información.

Criterio: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, versión 6 – DAFP; Manual Operativo del MIPG, versión 5 – marzo de 2023; Documento E-02-P-009 Gestión del riesgo - versión 2 de 2025.

Causa: Redacción imprecisa de los seguimientos; posible falta de orientación técnica sobre cómo reportar adecuadamente el avance o cierre del riesgo; débil control por parte de la segunda línea de defensa.

Efecto/potencial del riesgo: Imposibilidad de verificar el estado real del riesgo; toma de decisiones inadecuada por falta de información confiable; pérdida de trazabilidad en la gestión del riesgo.

Recomendación: Brindar capacitación a los responsables del seguimiento sobre buenas prácticas de redacción y seguimiento de riesgos, con énfasis en la claridad; precisión y soporte documental; implementar un formato estandarizado de seguimiento que incluya campos obligatorios para acciones realizadas, evidencias y grado de avance; reforzar el control y la revisión crítica por parte de la segunda línea de defensa, con retroalimentación a los responsables.

5.2.2. Indisponibilidad de la información en el aplicativo ISOLUCION

Condición: La materialización del riesgo de indisponibilidad de la información en el aplicativo ISOLUCION, pone de manifiesto debilidades en la respuesta temprana ante condiciones advertidas previamente.

Criterio: ISO/IEC 27001:2022, numerales 6.1 y 8.2 sobre gestión de riesgos y respuesta a incidentes; Guía para la Administración del Riesgo y el diseño de controles, versión 6 – DAFP; Documento E-02-P-009 Gestión del riesgo - versión 2 de 2025.

Causa: Debilidad en los mecanismos de alerta temprana.

Efecto/potencial del riesgo: Indisponibilidad de la información institucional; afectación a la continuidad de los procesos que dependen de la información reportada en el aplicativo ISOLUCION.

Recomendación: Fortalecer los mecanismos de monitoreo y alerta temprana sobre el estado de los sistemas críticos, como ISOLUCION; asegurar la implementación efectiva de controles preventivos identificados en el análisis de riesgo; establecer protocolos claros de respuesta inmediata a incidentes de indisponibilidad, con responsables, tiempos de reacción y canales de comunicación definidos; incluir esta situación como un caso de lección aprendida en la gestión de riesgos tecnológicos del INM.

5.3 OPORTUNIDADES DE MEJORA

Con el fin de fortalecer la gestión de los riesgos de seguridad de la información en el Instituto, y conforme a los hallazgos identificados durante la presente evaluación, se formulan las siguientes oportunidades de mejora. Estas no requieren suscripción de Plan de Mejoramiento. 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.

5.3.1 Revisar y actualizar los *Planes de Acción (acciones para abordar riesgos)* consignados en la matriz de riesgos de seguridad de la información para los riesgos residuales clasificados en las categorías moderado, alto y extremo, con el propósito de verificar con claridad cuál es la variable de seguridad comprometida (disponibilidad, confidencialidad o integridad de la información), en concordancia con lo establecido en la norma ISO/IEC 27001:2022, numeral 6.1 "*Acciones para abordar riesgos y oportunidades*".

5.3.2 Diligenciar y conservar las evidencias correspondientes a los controles definidos para cada riesgo, con énfasis en aquellas relacionadas con el seguimiento a la aplicación de dichos controles. Esto con el fin de garantizar la trazabilidad, efectividad y verificabilidad de las medidas implementadas, conforme a los lineamientos de la gestión de riesgos.

5.3.3 Establecer de forma explícita el responsable de realizar el seguimiento de los riesgos de seguridad de la información, desde la segunda línea de defensa, así como establecer mecanismos de control y supervisión desde esta línea de defensa, para verificar la consistencia y oportunidad del seguimiento realizado por los procesos.

5.3.4 Actualizar los controles consignados en la matriz de riesgos de seguridad de la información, asegurando su alineación con los requisitos establecidos en la norma ISO/IEC 27001:2022 sobre gestión de la seguridad de la información, ciberseguridad y protección de la privacidad, como parte del cumplimiento normativo y la mejora continua.

5.3.5 Asegurar que la información consignada en los seguimientos trimestrales de los riesgos sea clara, específica, verificable y alineada con la naturaleza del riesgo.

5.3.6 Capacitar a los responsables de cada proceso sobre el diligenciamiento adecuado de la matriz de riesgos de seguridad de la información y la importancia de la trazabilidad documental.

Luz Marina Doria Cavadia

Firmado digitalmente por Luz Marina Doria Cavadia

Luz Marina Doria Cavadía
Jefe Oficina de Control Interno
2025-07-04

Elaborado por. Leidy Liliana Ríos Martínez

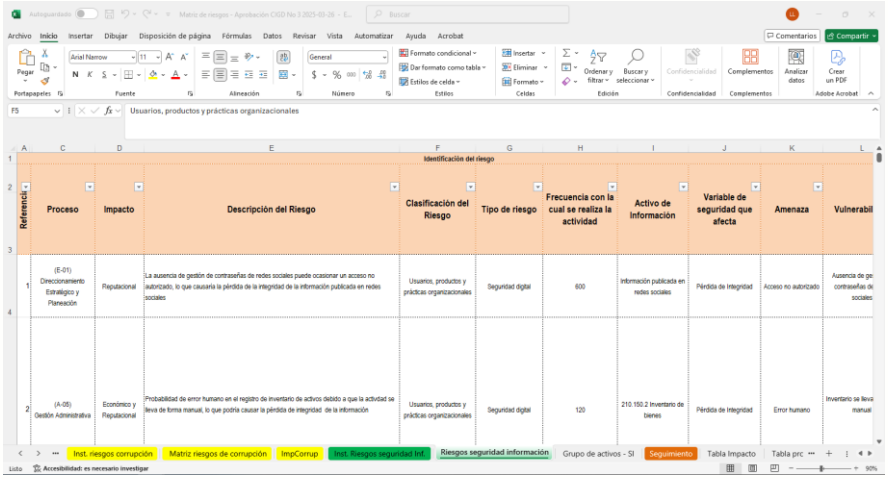
6. ANEXOS

6.1 Marco normativo

- 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".
- Decreto 1081 de 2015, "Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República".
- Decreto 1083 de 2015, "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", especialmente el Artículo 2.2.23.2 sobre la actualización del Modelo Estándar de Control Interno.
- Decreto 1499 de 2017, que modifica el Decreto 1083 de 2015 en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- Manual Operativo del Modelo Integrado de Planeación y Gestión (MIPG), versión 5, marzo de 2023, del Consejo para la Gestión y Desempeño Institucional.
- Guía Rol de las Unidades u Oficinas de Control Interno, Auditoría Interna o quien haga sus veces, versión 3, septiembre de 2023, con énfasis en el rol de evaluación de la gestión del riesgo.
- Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, versión 6 del 22 de noviembre de 2022.
- Documento "Gestión del Riesgo" código E-02-P-009, versión 2 del 12 de mayo de 2025, del Sistema Integrado de Gestión, disponible para consulta en el aplicativo ISOLUCION.

6.2 Imágenes

Imagen 1. Matriz de Riesgos Seguridad de la Información – Aprobación CIGD No. 3 2025-03-26



6.3 Tablas

Tabla No. 2 Riesgos 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	Detectivos: 0 Preventivos: 1 Correctivos:1
2	(E-02) Administración del Sistema Integrado de Gestión	3	3	Detectivos: 0 Preventivos: 3 Correctivos: 0
3	(E-03) Comunicaciones	1	1	Detectivos: 0 Preventivos: 1 Correctivos: 0
4	(E-05) Gestión de las Tecnologías de la Información	10	11	Detectivos: 2 Preventivos: 4 Correctivos: 5
5	(M-03) Producción de Materiales de Referencia y Desarrollo de Métodos Analítico	4	4	Detectivos: 0 Preventivos: 4 Correctivos: 0
6	(M-07) Investigación, Desarrollo e Innovación	1	1	Detectivos: 0 Preventivos: 1 Correctivos: 0
7	(M-08) Gestión de patrones nacionales y sistemas medición	4	4	Detectivos: 0 Preventivos: 4 Correctivos: 0
8	(A-04) Gestión de Talento Humano	1	1	Detectivos: 0 Preventivos: 1 Correctivos: 0
9	(A-05) Gestión Administrativa	3	3	Detectivos: 0 Preventivos: 3 Correctivos: 0
10	(A-06) Control Disciplinario	1	1	Detectivos: 0 Preventivos: 1 Correctivos: 0
11	(A-07) Contratación y Adquisición de Bienes y Servicios	1	1	Detectivos: 0 Preventivos: 1 Correctivos: 0
TOTAL		**30**	**31**	