Instituto Nacional de Metrología
de Colombia

Evaluación y Seguimiento a los Mapas de Riesgos y sus controles (Diseño y Efectividad)

Control Interno
Bogotá
(2019-04-24)

Instituto Nacional de Metrología de Colombia - INM
Av. Cra 50 No 26-55 Int. 2 CAN - Bogotá, D.C. Colombia
Conmutador: (571) 254 22 22
E-mail: contacto@inm.gov.co
www.inm.gov.co

1. Introducción

El presente informe tiene origen y fundamento básicamente a partir de las siguientes disposiciones legales:

- ✓ **Ley 87 de 1993**: *"Artículo 12: a). Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan. f). Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos."*

- ✓ **Decreto 1083 de 2015:** *"Artículo 2.2.21.5.4. Administración riesgos como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas (...). "*

  "Artículo 2.2.21.5.3. De las oficinas de control interno. Las Unidades u Oficinas de Control Interno o quien haga sus veces desarrollarán su labor a través de los siguientes roles: liderazgo estratégico; enfoque hacia la prevención, evaluación de la gestión del riesgo, evaluación y seguimiento, relación con entes externos de control. El Departamento Administrativo de la Función Pública determinará los lineamientos para el desarrollo de los citados roles".

- ✓ NTC ISO 31000. Gestión del Riesgo. Principios y Directrices.

- ✓ Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas - agosto de 2018.

- ✓ Lineamientos de la Guía Riesgos 2018.

- ✓ Documento Administración del riesgo – Código E1-02-D-01 del SIG.

Por su parte, la Función Pública a través de la *Guía Para la Administración del Riesgo* propuso la metodología para la Administración del Riesgo, la cual requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la entidad, el conocimiento de la misma desde un punto de vista estratégico, de la aplicación de tres (3) pasos básicos para su desarrollo y de la definición e implantación de estrategias de comunicación transversales a toda la entidad para que su efectividad pueda ser evidenciada. Los tres pasos a considerar son:

- ✓ antes de la metodología;
- ✓ paso 1: política administración de riesgos;
- ✓ paso 2: identificación del riesgo;
- ✓ paso 3: valoración del riesgo;
- ✓ comunicación y consulta.

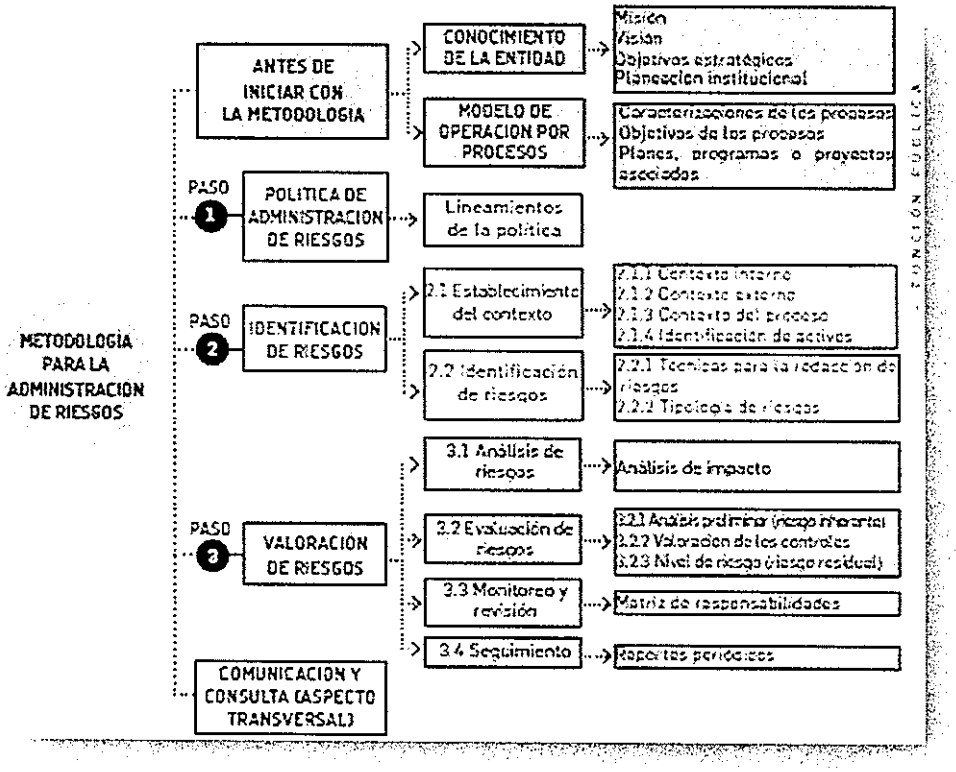
2. Alcance

Mapa de Riesgos institucional vigente. Periodo: enero, febrero y marzo de 2019.

3. Descripción metodológica

En aras de documentar y posteriormente elaborar este informe, se solicitó a la Oficina Asesora de Planeación la indicación de la ruta o link donde estuviera publicado el mapa de riesgos vigente, documentos estos que fueron ratificados y reposan en la carpeta de calidad, en: Z:\110 OAP\110 135 INFORMES\110 135.3 Inf. mapa admon riesgo\Proceso\2019.

A efectos de la revisión al mapa de riesgos se tuvieron en cuenta las orientaciones y en general, las directrices dispuestas en la *"Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas Riesgos de Gestión, Corrupción y Seguridad Digital"*. Ésta *es "una herramienta con enfoque preventivo, vanguardista y proactivo que permitirá el manejo del riesgo, así como el control en todos los niveles de la entidad pública, brindando seguridad razonable frente al logro de sus objetivos"*. La metodología que quedará entonces establecida, es la siguiente:



4. Resultados

A continuación, las observaciones relacionadas con cada paso de la metodología:

Política de Administración de Riesgos

Como declaración de la Dirección y las intenciones generales de la entidad con respecto a la gestión del riesgo, el INM definió la Política de riesgos, aprobada en Comité Institucional de Coordinación de Control Interno No. 2, la cual quedó plasmada en los siguientes términos:

"El Instituto Nacional de Metrología de Colombia (INM) establece las directrices que permiten la identificación, el análisis, la valoración y el tratamiento de los riesgos que afecten la misión, los objetivos institucionales, del Sistema Integrado de Gestión (SIG) y de los procesos.

El Comité Institucional de Gestión y Desempeño (CIGD) se compromete a gestionar la disponibilidad de los recursos, ejercer control y realizar seguimiento sobre los riesgos que puedan afectar negativamente la entidad, mediante una efectiva administración de los mismos, éstas directrices constituyen una herramienta de gestión para fortalecer la cultura del riesgo a todos los niveles, con la participación activa de los funcionarios y contratistas responsables de la identificación, documentación, el establecimiento de las acciones de control para su mitigación y toma de decisiones. Para esto se documentó la metodología donde se detalla los niveles de aceptación del riesgo y el tratamiento del riesgo, en el documento "Administración de riesgos" incluido dentro del SIG".

En cuanto al tratamiento de riesgos la Oficina Asesora de Planeación expuso:

Ubicación de Zona de Riesgo	Criterios de manejo ERCA
Baja	Se **ASUMIRÁ** el riesgo y se administra por medio de las actividades propias del proyecto o proceso asociado y se realiza monitoreo semestral de su desempeño por parte de la OAP
Moderada	Se establecen acciones de control que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo, se hace monitoreo trimestral de su desempeño por parte de la OAP
Alta	Se establecen acciones de control que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo o su impacto, puede evaluarse acciones para **EVITAR** el riesgo si dentro del análisis de impacto pude manejarse, se hace seguimiento trimestral de su desempeño por parte de la OAP.
Extrema	Se debe incluir en el Mapa de riesgos Institucional y se establecen acciones de Control que permitan **MITIGAR** la materialización del riesgo o **REDUCIR** la probabilidad de ocurrencia del riesgo o ambas, puede evaluarse acciones para **COMPARTIR** el riesgo, se hace seguimiento trimestral de su desempeño por parte de la OAP.
Riesgos de Corrupción. (*)	Ningún riesgo de corrupción podrá ser aceptado. Deben establecer acciones de control para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos.

* En todos los casos los líderes de los procesos realizaran seguimiento permanente a la gestión de los riesgos mediante la cultura de auto control.

De igual manera se establecieron las siguientes responsabilidades de la segunda línea de defensa – en cabeza de la Oficina Asesora de Planeación:

Se observó la actualización de la politica de riesgos a través de la página web (http://www.inm.gov.co/index.php/el-inm/sistema-integrado-de-gestion) el 9 de abril de 2019 siendo aprobada el 27 de febrero de 2019.

Identificación de Riesgos

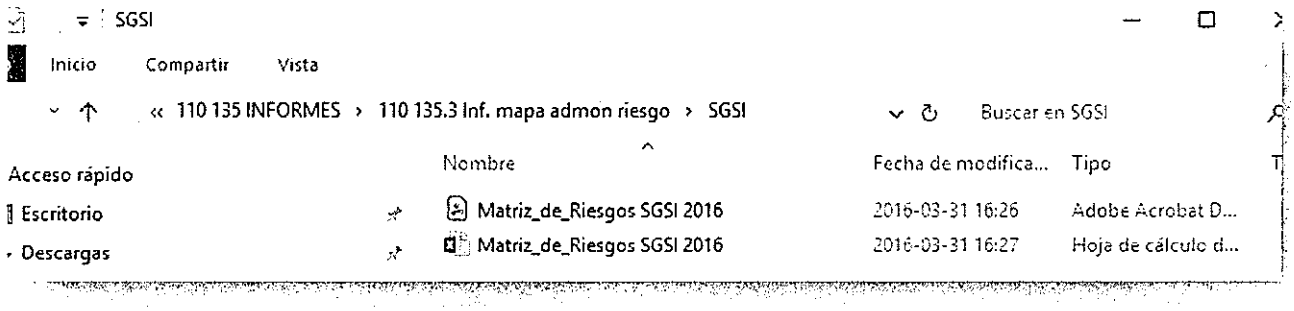
Con ocasión de la actualización en la norma ISO 31000:2018, el proceso para la identificación se mantiene, pero con mayor implicación y compromiso por parte de la Alta Dirección.

A propósito de la actualización en la norma ISO 31000:2018, se da realce de la naturaleza iterativa del riesgo, es decir, los procesos en respuesta a los diversos cambios que nos presenta tanto el entorno interno como el externo.

A través del archivo denominado E1-02-F-26 Matriz de Riesgos Institucionales INM 2019, se pudo determinar que, a la fecha, 2019-04-09, hay un total de 20 matrices (por cada uno de los procesos) que conforman la matriz de riesgos integrados.

Cada una de las matrices en comento registra un campo donde indica la aprobación que se da en acta CIGD 07del 2018-03-27, siendo este proceso poco consistente, precisamente con la iteratividad que tiene la Administración de Riesgos según la última actualización.

En la misma carpeta de calidad Z:\110 OAP\110 135 INFORMES\110 135.3 Inf. mapa admon riesgo\SGSI, se evidenció y se tuvo para consulta por parte de Control Interno el archivo denominado: Matriz_de_Riesgos SGSI 2016; documento este del que pudiera presumirse, hizo parte del proceso de Prestación de Servicios de Calibración y Ensayos en su momento, hoy por hoy desactualizada.



A través del archivo denominado E1-02-F-26 Matriz de Riesgos Institucionales INM 2019, se pudo determinar a la fecha 2019-04-09, hay un total de 20 matrices (por cada uno de los procesos) que conforman la matriz de riesgos integrados; cada una de ellas indicando: *"Aprobado: Acta CIGD 07 del 2018-03-27"*.

El mapa de riesgos vigente está conformado por la sumatoria de los riesgos de proceso y en total son 76, de los cuales después de aplicación de controles (residuales) están distribuidos de la siguiente manera, incluso porcentualmente:

Riesgos	**Total**	**%**
Riesgo Extremo	**8**	**11%**
Riesgo Alto	24	32%
Riesgo Moderado		
Riesgo Bajo	**20**	**26%**
Total	**76**	**100%**

A la fecha 2019-04-10 no se pudo determinar cuál fue el resultado del seguimiento para el primer trimestre de 2019, dado que los registros no habían sido incorporados en la matriz destinada para tal fin. Aunado a lo anterior, es importante señalar que el Mapa de Riesgos institucionales del INM no contempla riesgos de seguridad digital.

Valoración de Riesgos

Esta etapa del proceso la desarrollan básicamente 2 elementos: Análisis de riesgos y evaluación de riesgos; para este último hay que hablar del riesgo antes y después de controles.

La norma ISO 31000:2018 define **controlar** como*: "es medir para mantener y modificar el riesgo. Los controles incluyen, entre otros, cualquier proceso, política, dispositivo, práctica u otras condiciones, además de las acciones que mantienen o modifican el riesgo. Los controles pueden no siempre ejercer el efecto de modificación previsto o supuesto".*

Del mapa de riesgos vigentes se pudieron analizar algunos casos, como el que se trae en esta oportunidad, a modo de ejemplo:

Riesgo	Control
R1: Pérdida de clientes y disminución en los servicios prestados.	**Control:** Registros de competencia técnica de profesionales habilitados (internos y externos) para prestar servicios. **Periodicidad:** Anual. **Responsable:** Profesional de cada laboratorio. **Documento:** Procd. M1-04-P-01 Prestación del serv. de asistencia técnica (Núm.. 6.1 Planeación).
R2: Desalineación del proceso con los cambios relacionados con su entorno	**Control:** Informe de gestión de asistencia técnica.
R3: Incumplimiento contractual.	Pre-asignación de profesionales a vincular a un proyecto con aprobación de las Subdirecciones correspondiente.
	Realización de reuniones previas a la ejecución de un servicio 1. Operativa. 2. Inicio con el cliente.
	Confirmación de la capacidad de recursos para la prestación de servicios.

Control Interno observó:

Criterio evaluación	Observación		
	R1	R2	R3
Responsable		No está determinado con precisión.	No está determinado con precisión.
Periodicidad	La periodicidad anual difícilmente deja identificar las debilidades que se pueden dar en la ejecución del control.	La oportunidad con la que se realiza el control no permite determinar la materialización del riesgo en un periodo inferior al trimestre.	No la define.
Propósito	La actividad de: *"registro de competencia técnica de profesionales"* no busca por si sola prevenir o detectar la causa que da origen al riesgo.	El informe de gestión por si solo no busca prevenir el riesgo.	El riesgo está descrito de forma idéntica como consecuencia.
Como se realiza la actividad de control	No es clara la fuente de información.	No se puede determinar.	No hay certeza si la reunión tratada como el control mitiga el riesgo.
Que pasa con las observaciones o desviaciones	No se puede determinar cuál es el tratamiento con las desviaciones resultantes de la actividad de control.	Con la redacción que da al supuesto control no se puede determinar si se resuelve o investiga la observación cuando por ejemplo hay una desviación.	A partir de los datos registrados en la matriz no se puede determinar cuál es el tratamiento con las desviaciones resultantes de la aplicación del control.
Evidencia de la ejecución del control	A través de la denominación del registro (actas) no puede determinarse la efectividad en la actividad de control.	El acta es un documento amplio y general.	

5. Conclusiones

- ✓ El mapa de riesgos del INM, se encuentra desactualizado.
- ✓ Debilidades de la primera Línea de Defensa frente a su rol principal en la gestión de riesgos: diseñar, implementar y monitorear los controles y gestionar de manera directa en el día a día los riesgos de la entidad.

- ✓ La administración de riesgos en el INM es un proceso que requiere en si mismo un proceso de comunicación.

6. Recomendaciones de Control Interno

1. Tener presente que según Decreto 648 de 2017, en su Artículo 2.2.21.1.6, una de las funciones del Comité Institucional de Coordinación de Control Interno es hacer seguimiento a la política de administración del riesgo, en especial a la prevención y detección de fraude y mala conducta.

2. A propósito de los lineamientos a los que hace referencia la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, se recomienda entonces tener presente, a la hora de hacer seguimiento a la Política, los siguientes aspectos:

Objetivo:	Se debe establecer su alineación con los objetivos estratégicos de la entidad y gestionar los riesgos a un nivel aceptable.
Alcance:	La administración de riesgos debe ser extensible y aplicable a todos los procesos de la entidad. En el caso de los riesgos de seguridad digital, estos se deben gestionar de acuerdo con los criterios diferenciales descritos en el Modelo de Seguridad y Privacidad de la Información (ver caja de herramientas).
Niveles de aceptación al riesgo:	Decisión informada de tomar un riesgo particular (NTC GTC137, Numeral 3.7.1.6). Para riesgo de corrupción es inaceptable.
Niveles para calificar el impacto:	Esta tabla de análisis variará de acuerdo con la complejidad de cada entidad, será necesario considerar el sector al que pertenece (riesgo de la operación, los recursos humanos y físicos con los que cuenta, su capacidad financiera, usuarios a los que atiende, entre otros aspectos).
Tratamiento de riesgos:	Proceso para modificar el riesgo (NTC GTC137, Numeral 3.8.1.).
Periodicidad:	Tiempo de seguimiento para evitar materialización y de acuerdo con el nivel de riesgo residual

3. Como el mapa de riesgos vigentes no incluye los riesgos de seguridad digital, es importante tener en cuenta, a la luz del proceso de identificación de dichos riesgos, la orientación que sobre el particular tiene la Guía para la administración del riesgo y el diseño de controles en entidades públicas:

   ✓ Existirían tres (3) tipos de riesgos: *pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos*. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.

✓ Los catálogos de amenazas y vulnerabilidades comunes se encuentran en la sección 4.1.7. del anexo *"Lineamientos para la gestión del riesgo de seguridad digital en entidades públicas",* el cual hace parte de la Guía para la administración del riesgo y el diseño de controles en entidades públicas.

✓ **NOTA 1**: Tener en cuenta que la agrupación de activos debe ser del mismo tipo; por ejemplo, analizar conjuntamente activos tipo hardware, software, información, entre otros, para determinar amenazas y vulnerabilidades comunes que puedan afectar a dicho grupo.

✓ **NOTA 2:** Las entidades públicas deben incluir, como mínimo, los procesos y procedimientos establecidos en esta guía. Aquellas entidades que ya estén adelantando procesos relacionados con la gestión de este tipo de riesgo y que incorporen al menos lo dispuesto en estas guías, podrán continuar bajo sus procedimientos. Si alguno de los aspectos contenidos en esta guía no está contemplado, deberá ser agregado a lo que manejan actualmente.

4. En las matrices de riesgos vigentes, verificadas en este informe del INM, se puede determinar si no están o no se encuentran presentes las variables a evaluar para el diseño adecuado de controles:

   ✓ responsable;
   ✓ periodicidad;
   ✓ propósito;
   ✓ como realizar la actividad;
   ✓ observaciones o desviaciones;
   ✓ evidencia de la ejecución del control.

5. Para la adecuada mitigación de los riesgos, no basta con que un control esté bien diseñado, el control debe ejecutarse por parte de los responsables tal como se diseñó; lo anterior porque un control que no se ejecute, o un control que se ejecute y esté mal diseñado, no van a contribuir a la mitigación del riesgo.

Sandra Lucía López Pedreros
Asesor con Funciones de Jefe de Control Interno

Elaboró: María Margarita Peña Vargas.
Revisó: Sandra Lucía López Pedreros.
2019-04-24