Instituto Nacional de Metrología de Colombia

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

Evaluación Acompañamiento y Asesoría de Control Interno
Bogotá
2020-05-28

Instituto Nacional de Metrología de Colombia - INM
Avenida Carrera 50 No.26- 55 Int. 2 CAN Bogotá D.C.-Colombia
Conmutador: (57- 1) 2542222 - **Website**: www.inm.gov.co
E-mail: contacto@inm.gov.co - Twitter: @inmcolombia
Código Postal 111321

CONTENIDO

Página.

1. INTRODUCCIÓN

Desde el 2015, a partir de la expedición del Decreto 1083, se determinó que las entidades públicas establecerían y aplicarán políticas de administración del riesgo, como parte integral del fortalecimiento de los sistemas de control interno y desde entonces ha de ser la identificación y análisis del riesgo un proceso permanente e interactivo, a través del cual se evalúen aspectos, tanto internos como externos, que pueden llegar a representar amenaza para la consecución de los objetivos organizacionales, con miras a establecer acciones efectivas, representadas en actividades de control.

Ahora bien; conforme lo ha indicado la Guía rol de las unidades u oficinas de control interno, auditoría o quien haga sus veces a través del rol de evaluación de la gestión del riesgo, las unidades u oficinas de control Interno, auditoría interna, o quien haga sus veces, deben proporcionar un aseguramiento objetivo a la Alta Dirección (línea estratégica) sobre el diseño y efectividad de las actividades de administración del riesgo en la entidad para ayudar a asegurar que los riesgos claves o estratégicos estén adecuadamente definidos, sean gestionados apropiadamente y que el sistema de control interno está siendo operado efectivamente.

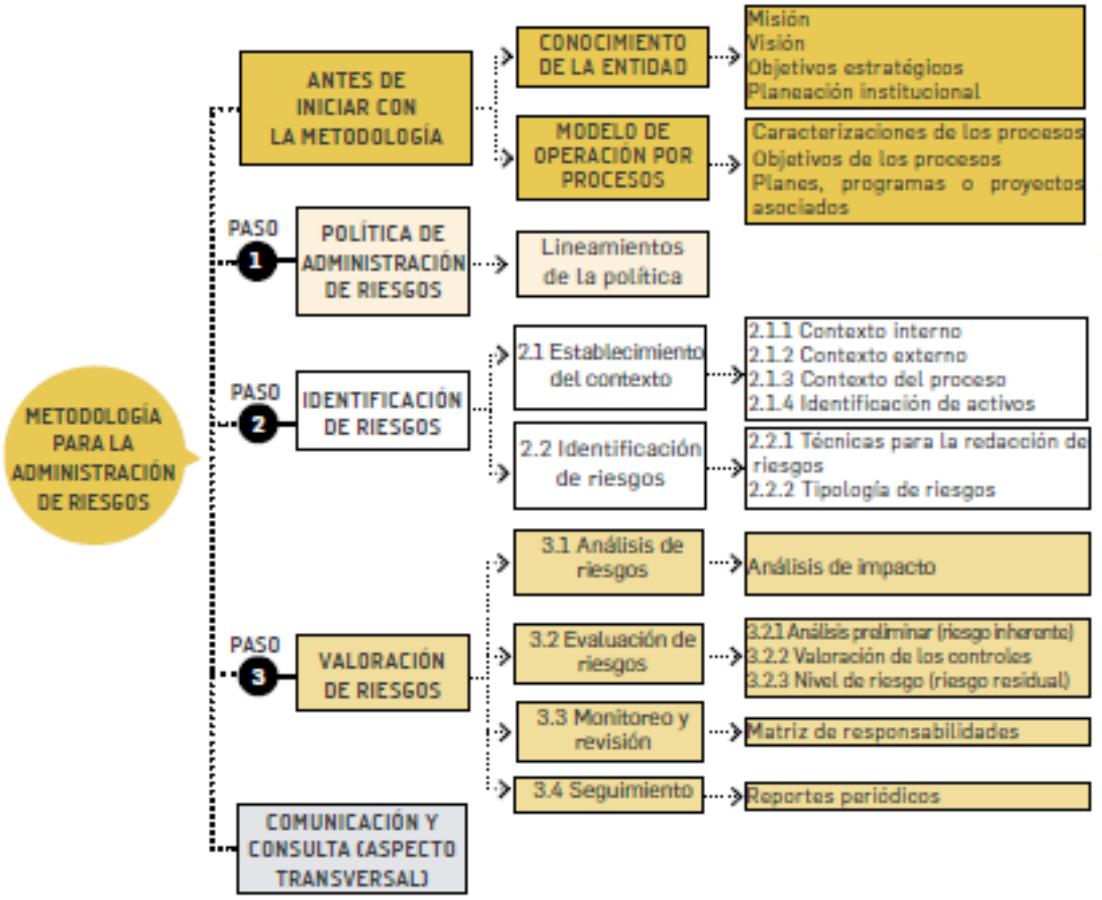
2. ALCANCE

Documentalmente ha de ser tenido en cuenta para el alcance de esta revisión la matriz dispuesta para consulta en la carpeta "Calidad INM": Z:\110 OAP\110 135 INFORMES\110 170 Inf. mapa admon riesgo\Proceso\Riesgos 2020

3. DESCRIPCIÓN METODOLÓGICA

Los métodos y pruebas de auditoria utilizados a efectos de esta evaluación y en general para la obtención de evidencia válida y suficiente para la emisión del informe de seguimiento, incluyó básicamente:

- Plan Anual de Auditorias de Control Interno (aprobado el 2020-02-28).
- Procedimientos del proceso Evaluación Acompañamiento y Asesoría de Control Interno (C1-01). Los procedimientos de auditoria como las técnicas aplicables en el proceso son de acuerdo a la experiencia y el criterio del auditor quien decide la estrategia que considera más adecuada para el desarrollo de la Auditoria de Seguimiento.
- La dinámica de la evaluación estuvo acorde a la metodología para la administración del riesgo, dispuesta por el Departamento Administrativo de la Función Pública a través de su la Guía para la administración del riesgo y el diseño de controles en entidades públicas – riesgos de gestión, corrupción y seguridad digital – Versión 4; sintetizada así:

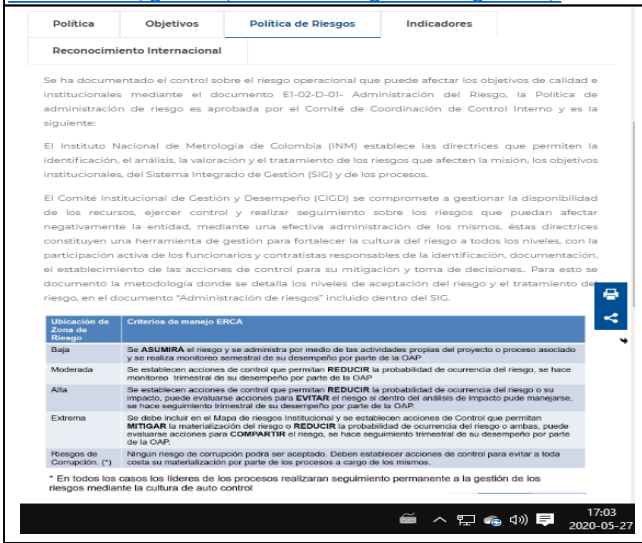
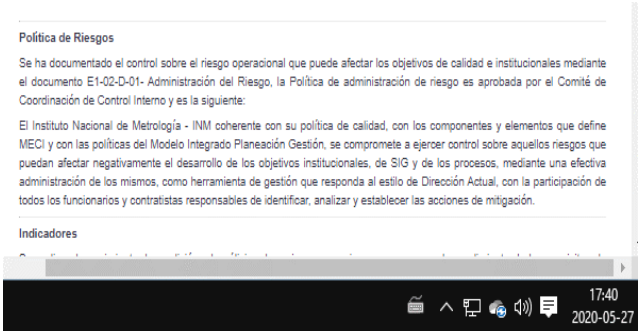


4. RESULTADOS

Política de Administración de Riesgos

Constituye la declaración de la Dirección y las intenciones generales del INM con respecto a la gestión del riesgo. La versión publicada a través del Manual Integrado de Gestión vigente (E-02-M-01 – versión 01), fue aprobada en sesión del Comité de Coordinación de Control Interno, en febrero 27 de 2019, es decir hace algo más de un año.

La política de riesgos del INM vigente se encuentra publicada en la página web, http://www.inm.gov.co/instituto-nacional-de-metrologia-de-colombia/gestion/sistema-integrado-de-gestion/; no obstante en consulta realizada en la INMtranet y considerada esta como sistema de información institucional; se encuentra publicada una política de riesgos con una versión diferente:

Página web	INMtranet
http://www.inm.gov.co/instituto-nacional-de-metrologia-de-colombia/gestion/sistema-integrado-de-gestion/	inm.gov.co/instituto-nacional-de-metrologia-de-colombia/gestion/sistema-integrado-de-gestion/
	

Se sugiere efectuar revisión de la política de riesgos vigente, teniendo presente que es a través de ella que se emiten lineamientos precisos para el tratamiento, manejo y seguimiento a los riesgos que afectan el logro de los objetivos institucionales.

En medio de la revisión de la política de riesgos se recomienda tener presente entre otros aspectos:

- Propósito
- Alcance
- Marco normativo
- Niveles de aceptación del riesgo
- Niveles para calificar el impacto
- Tratamiento de riesgos
- Periodicidad para seguimiento
- Términos y definiciones
- Metodología a utilizar
- Software para el desarrollo
- Aspectos relevantes sobre los factores de riesgo
- Lineamientos
- Periodicidad para el monitoreo
- Otros aspectos

Identificación de Riesgos

En esta etapa es importante fijar especial atención en los riesgos más significativos para la entidad relacionados con los objetivos de los procesos y los institucionales.

En la matriz de riesgos vigente, se encuentran identificados riesgos por proceso; no obstante, a través de la misma matriz se pudo determinar existen oportunidades de mejora en cuanto a la identificación de riesgos, por ende, los elementos que lo desarrollan.

A modo de ejemplo se traen casos, desde procesos estratégicos, misional y apoyo:

Proceso: Administración del Sistema Integrado de Gestión **Riesgo:** Incumplimiento de la normatividad ambiental aplicable, metas y objetivos ambientales. **Descripción:** Desconocimiento o falta de compromiso por parte de los funcionarios y contratistas para la aplicación de los lineamientos establecidos para la gestión ambiental.	El texto: *"Desconocimiento o falta de compromiso por parte de…"* que constituye parte de la descriptiva del riesgo pudiera ser la causa del incumplimiento de la normatividad y no precisamente es la descripción del riesgo.
Proceso: Asistencia Técnica **Riesgo:** M04-R01) Incumplimiento contractual. **Descripción:** El cliente evidencia en la prestación del servicio que el profesional no tiene las competencias técnicas adecuadas para atender su requerimiento.	Con el aparte de la descriptiva con la que inicia la redacción: *"El cliente evidencia en la prestación del servicio que el profesional no tiene las competencias…"* no se puede establecer precisamente, por ejemplo: ¿Qué puede suceder?, ¿Cómo puede suceder?, ¿Cuándo puede suceder? y ¿Qué consecuencias tendría su materialización?, preguntas que deben tener en cuenta para efectos de la descripción y la identificación del riesgo.
Proceso: Contratación y Adquisición de Bienes **Riesgo:** Retrasos en el inicio de ejecución de los contratos. **Descripción:** los tiempos en la etapa precontractual de los procesos de contratación pueden aumentarse de manera desproporcionada. De la misma manera se puede demorar el inicio de la ejecución de los contratos.	La descriptiva del riesgo está dada a modo de justificación de la planificación a nivel de proceso y la consecuencia de la misma. En este caso no es posible determinar a partir del riesgo y su descriptiva ¿Cómo puede suceder? y ¿Cuándo puede suceder? preguntas que deben tener en cuenta por ejemplo para efectos de la descripción y la identificación del riesgo.

La Guía para la administración del riesgo y el diseño de controles en entidades públicas, considera importante asegurarse que el riesgo identificado está relacionado directamente con las características del objetivo y en el evento en que la respuesta sea negativa (no), este puede ser la causa o la consecuencia y no precisamente el riesgo.

Valoración de Riesgos

En esta etapa es considerada de suma importancia el diseño de los controles, es decir que efectivamente mitiguen las causas que hacen que el riesgo se materialice.

Desde la redacción según la misma Guía para la administración del riesgo y el diseño de controles en entidades públicas, se deben considerar las siguientes variables para el adecuado diseño de controles:

1. Debe tener definido el responsable de llevar a cabo la actividad de control.
2. Debe tener una periodicidad definida para su ejecución
3. Debe indicar cuál es el propósito del control.
4. Debe establecer el cómo se realiza la actividad de control.
5. Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.
6. Debe dejar evidencia de la ejecución del control

En la matriz de riesgos se pudo establecer debilidades y en general oportunidades de mejora en cuanto al diseño de controles. A modo de ejemplo se tienen casos como:

Riesgo: (E02-R10) - *Incumplimiento de la normatividad ambiental aplicable, metas y objetivos ambientales.* **Control:** *Informe trimestral de ejecución del Plan de Acción Ambiental.*	El responsable de ejecutar la actividad de control es un contratista, situación esta que ha de ser revisada toda vez que el esquema de contratación de la entidad no asegura vinculación de contratistas por los 365 días del año. Adicionalmente a través del texto que hace parte de la descriptiva del control: *Informe trimestral..*; no es posible determinar cuál es el propósito del control ni como se realiza la actividad del control y por consiguiente que pasa con las desviaciones resultantes de ejecutar el control, aunando a ello que el soporte corresponde a un radicado, del cual se puede inferir puede tener cualquier otro uso y no precisamente un control.
Riesgo: (E03-R05) - *Tratamiento Inadecuado de la información.* **Actividades de Control:** *Informes de seguimiento al cumplimiento de la norma.*	A partir de la descriptiva de la actividad de control, no es posible determinar un informe constituye la actividad; el mismo informe bien pudiera ser el resultado de otra actividad del proceso de comunicaciones. La actividad vista desde la descriptiva adolece de inclusión de variables como: el cargo del responsable de llevar a cabo la actividad de control, la periodicidad con la que se realiza la actividad de control, el propósito del control, cómo se realiza la actividad de control, entre otros.

Comunicación y consulta (transversal)

La comunicación de la información y el reporte en la administración de riesgos debe garantizar que se tienen en cuenta las necesidades de los usuarios, de modo tal que los riesgos identificados, permitan encontrar puntos críticos para la mejora en la prestación de los servicios.

A través de la validación del registro de seguimiento que incorpora la matriz se pudo determinar por ejemplo el proceso Gestión de las Tecnologías de la Información; no reportó información para el Q1 de 2020, que según la misma matriz registrara fecha de seguimiento 22 de mayo de 2020; lo que quiere decir entonces que cronológicamente hablando corresponde a los primeros 4 meses del año (enero a abril):

ID	Riesgo	Descripción	Control	Periodo: Trimestre Q1 2020		
				Fecha Seguimien	Responsable seguimiento	Descripción del Avance, Evidencia y/o Observacione
E05-R07	Exposición ante nuevas amenazas informáticas	Hace referencia principalmente a la reacción para brindar protección a la información del INM ante nuevos ataques informáticos a raíz de la ausencia y debilidades en los lineamientos frente a la confidencialidad y no divulgación. Estas situaciones pueden presentarse cuando se realizan prestamos de archivos físicos o digitales a Funcionarios / Colaboradores y terceros sin los debidos acuerdos de confidencialidad y debida autorización.	Control: Establecer restricciones de acceso a la Información Propósito: Proteger la infraestructura critica del INM Periodicidad: diaria Responsable: Profesional designado por el Coordinador de TI Documento: Procedimiento de ingreso seguro Términos y condiciones del empleo Desviación : Presentar fallas en la herramienta existente ,	2020-05-22	Yesid Pineda	No se registra Información
E05-R08	Intermitencias en la prestación de los servicios prestados por terceros	Situaciones en las cuales se detienen las operaciones misionales y administrativas de la entidad, por fallas presentadas durante la prestación del servicio por parte de los proveedores de servicios tecnológicos, durante situaciones que presente el proveedor en la prestación del servicio, ocasionando que los aplicativos utilizados dejan de funcionar por un periodo de tiempo.	Control: Realizar seguimiento de los acuerdos ANS con las herramientas de monitoreo correspondientes sobre los servicios críticos "internet, correo". Propósito: Monitorear en la calidad del servicio. Como: Realizando seguimiento según las obligaciones contractuales Periodicidad: Trimestral Responsable: Supervisor del contrato Documento: (Evidencia): Reporte solicitado según lo contratado Desviación: fallas en el funcionamiento de las herramientas	2020-05-22	Yesid Pineda	No se registra Información
E05-R09	Exposición de dispositivos informáticos a condiciones e instalaciones inadecuadas	Pueden presentarse daños en conexiones de Switches, servidores, cintas magnéticas, locaciones etc., dejando los dispositivos en condiciones e instalaciones no apropiadas, cuando las áreas incumplen las políticas o buenas practicas establecidas.	Control: Elaborar y aplicar Check Lista para verificar el cumplimiento de las políticas y buenas practicas definidas y documentadas sobre los equipos críticos. Propósito: Asegurar el cumplimiento de las Políticas y buenas practicas. Como: Realizando visitas a las áreas constatando el cumplimiento de las Políticas. Periodicidad: semestral Responsable: Profesional asignado por el coordinador de	2020-05-22	Yesid Pineda	No se registra Información

A partir de casos como el que se acaba de mencionar e ilustrar, se pone en evidencia la oportunidad de mejora a nivel de proceso en cuanto al aseguramiento de la implementación de la metodología como actores protagónicos de la primera línea de defensa.

A partir de la matriz que incorpora la totalidad de riesgos de la entidad, consultada a efecto de esta evaluación se pudo determinar en el campo denominado fecha límite no hubo actualización de las mismas; tal cual como se aprecia en la imagen que sigue, capturada desde la fuente, que incluye solamente algunos ejemplos.

ID	Riesgo	Soporte	Responsable	Fecha límite	Indicador Clave de Riesgo
E02-R01	Uso de documentos del SIG obsoletos y/o desactualizados	Listado de Asistencia	**Enlaces Calidad** Isabel / Linda P. (SMF) Daisy / Mónica (SMQB) Diana Pedraza (SIST) Jeimy / Dwight (SG) **Prof. OAP** Daniel/Milena/Yesid	2019-08-31	Por definir
		Software en operación	Maria L. Saldarriaga **Jefe OAP** Daniel Delgado Milena Rodríguez Yesid Pineda **Prof. OAP**	2019-08-31	Por definir
		documento de requisitos legales y otros requisitos actualizado	Daniel Delgado Milena Rodríguez Yesid Pineda Prof. OAP	2019-10-31	Documento actualizado en la fecha establecida
E02-R02	Cierre de Hallazgos y de no Conformidades vencidos	Listado de Asistencia	Daniel Delgado Milena Rodríguez Yesid Pineda **Prof. OAP**	2019-12-15	# de reuniones para revisión y análisis de hallazgos transversales / # de Hallazgos identificados como transversales
		Listado de Asistencia	**Enlaces Calidad** Isabel / Linda P. (SMF) Daisy / Mónica (SMQB) Diana Pedraza (SIST) Jeimy/Dwight (SG)	2019-12-15	# de reuniones para revisión y análisis de hallazgos de difícil cierre / # de Hallazgos

5. CONCLUSIONES & RECOMENDACIONES

A través del rol de evaluación de la gestión del riesgo y del rol de evaluación y seguimiento que desarrolla el proceso de Evaluación Acompañamiento; se ha evidenciado la administración de riesgos a nivel institucional es un proceso que requiere de fortalecimiento, a todo nivel, en todas las etapas que lo constituyen: Establecimiento del contexto, Valoración del riesgo (identificación, análisis, evaluación y tratamiento), Comunicación y consulta y Monitoreo y revisión.

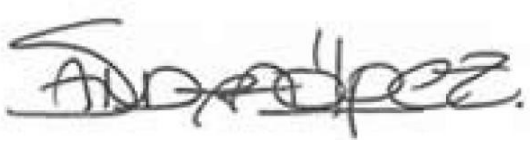
En tiempos de pandemia, se recomienda tener presente en la identificación de riesgos factores como:

- Fallas y debilidades en los protocolos de comunicación a nivel institucional y con usuarios (por prestación de bienes y/o servicios).
- Cambios en el comportamiento de usuarios por la pandemia.
- Actualización de riesgos con nuevas necesidades a nivel institucional.
- Aplazamiento de proyectos estratégicos con previa inversión y en vigencias futuras.
- Implementación de nuevos proyectos para afrontar los cambios sin análisis de riesgos.
- Transformación digital vs capacitación a funcionarios.
- Automatización de procesos ante el surgimiento de nuevas vulnerabilidades.
- Eliminación de los log de auditoría para nuevos usuarios o roles asignados.
- Controles de monitoreo eliminados o simplificados para agilizar procesos.

- Debilidades para accesos remotos a los sistemas de información
- Trabajo en casa para periodos largos.

A propósito de la entrada en producción del software Isolución que cuenta con el módulo de riesgos, se recomienda aprovechar las jornadas de capacitación y entrenamiento de los usuarios y hacer de este espacio uno más para apropiar el tema a todo nivel en cada uno de los pasos que componen la metodología de la administración de riesgos, asegurando que permee a la totalidad del INM.

Finalmente es importante indicar que cada línea de defensa en el Modelo Estándar de Control Interno tiene responsabilidades que deben fortalecerse en la gestión del riesgo institucional.



Sandra Lucía López Pedreros

Asesor con Funciones de Jefe de Control Interno.
2020-05-28