Instituto Nacional de Metrología de Colombia

Seguimiento Mapa de Riesgos

Control Interno

Bogotá

2019-01-10

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

El progreso es de todos

1. Introducción

A través del rol de Evaluación de la Gestión del Riesgo; Control Interno en calidad o actuando como la tercera línea de defensa debe proporcionar un aseguramiento objetivo a la Alta Dirección 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 y sean gestionados apropiadamente y que el sistema de control interno está siendo operado de manera efectiva.

En este rol de Evaluación de la Gestión del Riesgo, Control Interno juega un papel fundamental, a través de la asesoría y acompañamiento técnico y de evaluación y seguimiento en los diferentes pasos de la gestión del riesgo, que van desde la fijación de la Política de Administración de Riesgo hasta la evaluación de la efectividad de los controles.

Conforme lo señala el Anexo 4 Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas en su numeral 4.3.4 le corresponde a las Unidades de Control Interno (tercera línea de defensa), realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo de seguridad digital en la entidad pública, catalogándola como una unidad auditable más dentro de su Universo de Auditoría, conforme al Plan Anual de Auditoría aprobado por el Comité Institucional de Coordinación de Control Interno de la entidad.

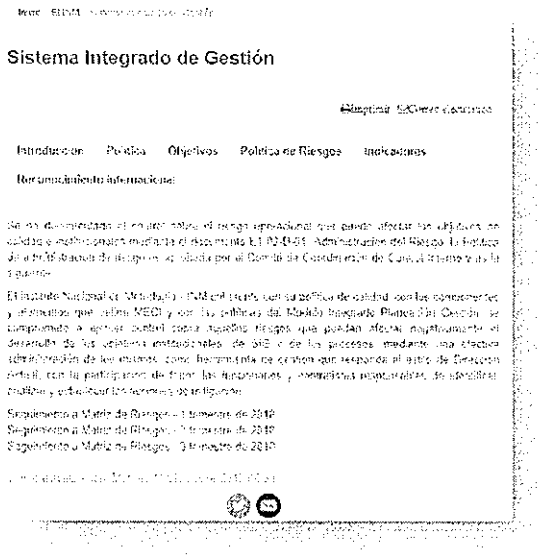
2. Alcance

Matriz de Riesgos Institucionales INM 2018. Periodo: octubre, noviembre y diciembre de 2018.

3. Descripción metodológica

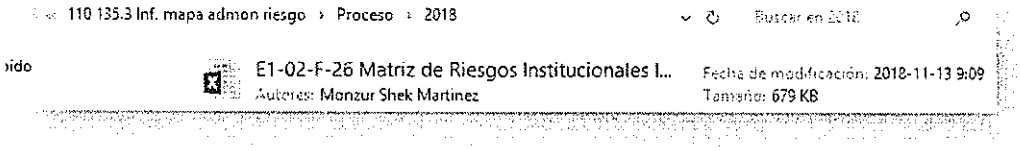
El seguimiento al mapa de riesgos se dio en los siguientes términos:

1. Consulta en la página web de la información disponible en materia de riesgos: http://www.inm.gov.co/index.php/el-inm/sistema-integrado-de-gestion



2. Consulta del archivo dispuesto en la carpeta de la Oficina Asesora de Planeación

   Z:\110 OAP\110 135 INFORMES\110 135.3 Inf. mapa admon riesgo\Proceso\2018



3. Revisión de los contenidos de la documentación e información obtenida en los dos ítems anteriores.

4. Resultados

Para este periodo de análisis se realizó el informe teniendo en cuenta los 3 pasos de la Metodología para la Administración de Riesgos:

1. Paso 1: Política de Administración de Riesgos

La Política de Administración de Riesgos está definida y se encuentra publicada en la página web de la entidad, así:

El Instituto Nacional de Metrología - INM coherente con su política de calidad, con los componentes y elementos que define MECI y con las políticas del Modelo Integrado Planeación Gestión, se compromete a ejercer control sobre aquellos riesgos que puedan afectar negativamente el desarrollo de los objetivos institucionales, de SIG y de los procesos, mediante una efectiva administración de los mismos, como herramienta de gestión que responda al estilo de Dirección Actual, con la participación de todos los funcionarios y contratistas responsables de identificar, analizar y establecer las acciones de mitigación.

A propósito del alcance, en el caso de los riesgos de seguridad digital, estos deben gestionarse de acuerdo a los criterios diferenciales descritos en el Modelo de Seguridad y Privacidad de la Información.

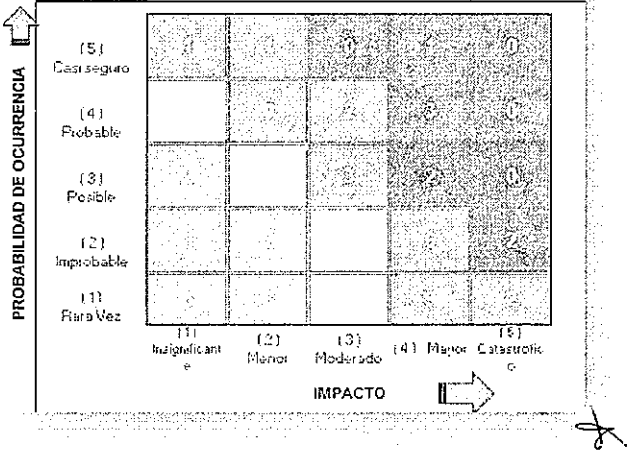
Aunado a lo anterior debe tenerse en cuenta también en la revisión de la Política de Administración de Riesgos la periodicidad para el seguimiento de acuerdo con el nivel de riesgo residual.

2. Paso 2: Identificación de Riesgos

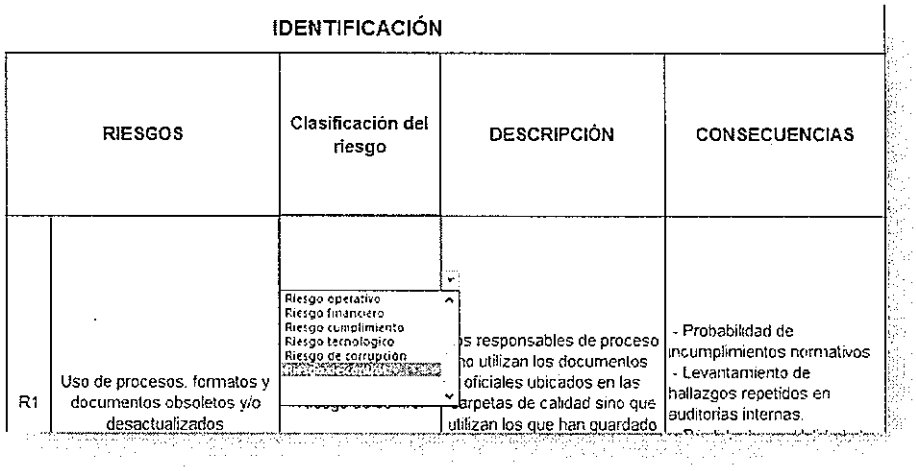
A 31 de diciembre de 2018, se habían identificado según el mapa de riegos un total de 76:

MAPA DE RIESGOS
DE PROCESOS 2018

NIVEL	ZONA RIESGO EXTREMO	ZONA RIESGO ALTO	ZONA RIESGO MODERADO	ZONA RIESGO BAJO	TOTAL
CANTIDAD	8	24	24	20	76
%	10,5%	31,6%	31,6%	26,3%	



A propósito de la Tipología de Riesgos a partir de la Matriz objeto de consulta no se pudo determinar la existencia dentro de la clasificación de los riesgos de seguridad digital, definido como la posibilidad de combinación de amenaza y vulnerabilidades en el entorno digital. Situación que puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.



IDENTIFICACIÓN				
	RIESGOS	Clasificación del riesgo	DESCRIPCIÓN	CONSECUENCIAS
R1	Uso de procesos, formatos y documentos obsoletos y/o desactualizados	Riesgo operativo Riesgo financiero Riesgo cumplimiento Riesgo tecnologico Riesgo de corrupción	s responsables de proceso no utilizan los documentos oficiales ubicados en las arpetas de calidad sino que utilizan los que han guardado	- Probabilidad de incumplimientos normativos - Levantamiento de hallazgos repetidos en auditorias internas.

A partir de las fallas presentadas en los servicios informáticos desde el 5 de diciembre de 2018, se evidenció para el contexto del proceso los activos de seguridad digital de los procesos sufrieron afectación y por expreso señalamiento el 17 de diciembre de 2018, del Grupo de Sistemas que desarrollarían un Plan de Contingencia para habilitar aplicativos de la entidad.

Los riesgos de Seguridad Digital se basan en la afectación de tres criterios en un activo o un grupo de activos dentro del proceso: integridad, confidencialidad o disponibilidad. Para el caso del Proceso de Control Interno la afectación fue directamente a la integridad del proceso y por ende a los procesos auditados en el 2018; se tuvo a partir de la fecha de presentación de la falla e incluso hasta después de la puesta en marcha del Sistema de Seguimiento de Planes de Mejoramiento SISEPM a partir del 28 de diciembre de 2018.

3. Paso 3: Valoración de Riesgos

Evaluación de riesgos

En el primer paso se identificaron riesgos; no obstante, en algunos casos se evidenció que para cada causa no existe un control, verbigracia:

Proceso	Riesgo	Número de Causas Identificadas	Controles Asociados
Planeación Institucional	R2	3	2
Administración del SIG	R1	4	3
Interacción con el ciudadano	R2	2	1
Prestación de servicios de calibración y ensayo	R2	4	2
Producción, certificación y comercialización de materiales de referencia	R1	1	2
Asistencia técnica	R3	1	3

Al momento de definir actividades de control por parte de los líderes de cada proceso, es importante considerar que los controles estén bien diseñados, es decir que efectivamente estos mitigan las causas que hacen que el riesgo se materialice.

En la construcción o mejor en el diseño de los controles se evidenció omisión de los pasos para diseñar un control, a modo de ejemplo se tiene en el proceso de Administración de Sistemas de Información:

Control: Gestión de carpetas compartidas **Periodicidad:** Permanente **Responsable:** **Documento:**
Control: Identificación de propietarios de la información Periodicidad: Permanente Responsable: Documento:

A partir del informe de ejecución del Contrato 140-2018, suscrito con Eduardo Andrés Ospina Jarro, quedó señalado en el numeral VI, el promedio evaluación de controles alcanzó una calificación de 63, respecto a una calificación objeto de 100.

4. Conclusiones

Frente a la administración del riesgo, Control Interno tiene un papel proactivo, a través de la medición de la efectividad de los controles y haciendo seguimientos a la actualización de los mapas de riesgos.

A partir del informe de ejecución del contrato 140 de 2018, suscrito con Eduardo Andrés Ospina Jarro, concluyó el mismo contratista se efectuó la evaluación de las actividades que se requieren para la implementación del Modelo, hay un 63% de acumulado total.

Con las fallas presentadas en los servicios informáticos desde el 5 de diciembre de 2018, se aumentó en el INM la desconfianza en el uso del entorno digital ocasionada básicamente por la pérdida de la integridad y disponibilidad de la información y el desgaste administrativo en todos los procesos (estratégicos, misionales, de apoyo y de control).

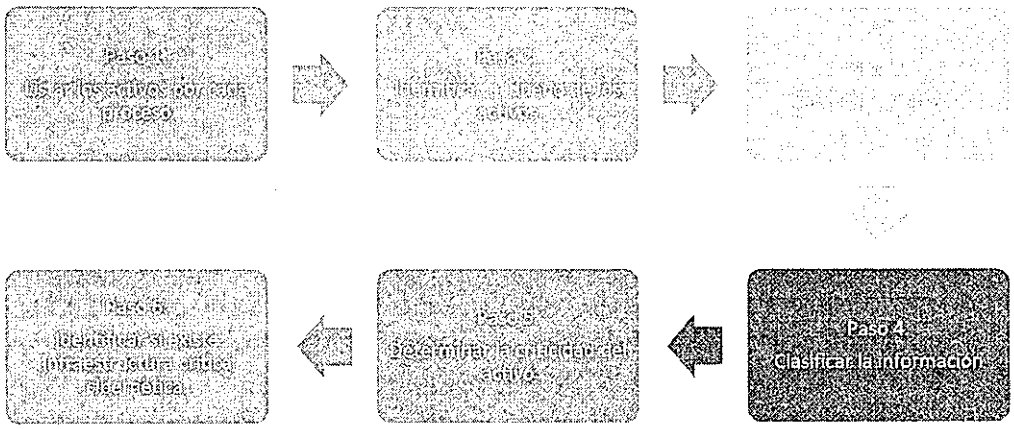
5. Recomendaciones de Control Interno

De cara a la revisión efectuada, Control Interno sugiere:

a. Para la revisión de la Política de Administración del Riesgo; tener presente debe incluir mínimo aspectos como: objetivo, alcance, niveles de aceptación del riesgo o tolerancia al riesgo, términos y definiciones y la estructura para la gestión del riesgo.

   En lo que atañe al Modelo de Seguridad y Privacidad de la Información la entidad decide si realiza la gestión de riesgos en todos los activos identificados o si lo hace en los activos más críticos, dejándolo registrado de manera explícita en la Política de Administración de Riesgos.

b. En la identificación de los riesgos, bajo el contexto del proceso, para los activos de seguridad digital del proceso: información, aplicaciones, hardware entre otros, se deben tener en cuenta las medidas de protección para garantizar el funcionamiento interno de cada proceso, así como también de cara al ciudadano y tener en cuenta los siguientes pasos:



Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

c. Designar un Responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información, el cual debe pertenecer a un área que haga parte de la Alta Dirección o Línea Estratégica y las responsabilidades que deberá cumplir respecto a la gestión del riesgo de seguridad digital, entre otras:

   - Definir el procedimiento para la Identificación y Valoración de Activos.
   - Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento).
   - Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos.
   - Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
   - Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.

   El responsable de seguridad digital debe reportar periódicamente a la Alta Dirección y al Comité Institucional de Coordinación de Control Interno:

   - Matriz de riesgos de seguridad digital,
   - Listado de activos críticos,
   - Reporte de criticidad,
   - Plan de tratamiento de riesgos,
   - Reporte de evolución de riesgos y modificación de apetito de riesgo,
   - Cantidad de riesgos por fuera de la tolerancia del riesgo identificados de acuerdo con la periodicidad de evaluación realizada,
   - Impacto económico que podría presentarse frente a la materialización de los riesgos.

d. Como buena práctica en seguridad digital se recomienda llevar registro de los incidentes de seguridad digital que se hayan materializado con el fin de analizar las causas, las deficiencias de los controles implementados y las pérdidas que se pueden generar y garantizar que se tomen las acciones adecuadas para evitar su ocurrencia e implementar o adoptar nuevos controles.

e. Una vez más se sugiere tener en cuenta al momento de diseñar y documentar controles:

Responsable	Quien lleva a cabo la actividad de control
Frecuencia	La periodicidad para la ejecución del control
Objetivo	El propósito del control
Procedimiento	Cómo se realiza la actividad de control
Observaciones	Qué pasa con las desviaciones resultantes de ejecutar el control
Evidencia	Dejar registro de la ejecución del control

f. Realizar monitoreo permanente a los controles de los riesgos por parte de los líderes de procesos.

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

Fecha: 2019-01- 10