



**INFORME DE EVALUACIÓN A LA GESTIÓN DE RIESGOS
27/09/2019**

ASESOR DE CONTROL INTERNO

Código: SG-110-FM-037-Versión: 7– Vigencia: 29/01/2019

Carrera 13 No. 34 - 91 / www.inci.gov.co
aciudadano@inci.gov.co / PBX:(57 1) 384 66 66
Bogotá D.C., Colombia



La educación
es de todos

Mineducación

CONTENIDO

1. INTRODUCCIÓN	3
2. OBJETIVOS	3
3. MARCO LEGAL	3
4. METODOLOGÍA	4
5. DOCUMENTOS EXAMINADOS	4
6. RESULTADOS DEL SEGUIMIENTO Y ANÁLISIS	5
6.1. LA ADMINISTRACIÓN DE RIESGOS EN LA ENTIDAD.....	5
6.2. INDICADOR DE DESEMPEÑO DEL REPORTE FURAG II 2018.....	5
6.3. ANÁLISIS DE LOS RIESGOS DE GESTIÓN Y SEGURIDAD DIGITAL 2019.	6
6.4. LINEAS DE DEFENSA.....	12
7. CONCLUSIONES	14
8. RECOMENDACIONES	15

1. INTRODUCCIÓN

De acuerdo con los roles establecidos en la normatividad vigente y en Plan Anual de Auditoría, la asesora de control interno realizó la evaluación a la gestión de riesgos del INCI, con corte al 31 de agosto de 2019.

2. OBJETIVOS.

- Verificar la existencia y aplicación de políticas, normas internas, controles y demás mecanismos que den cuenta la gestión de riesgos en el Instituto Nacional para Ciegos, en cumplimiento de las normas dictadas por el Gobierno Nacional en esta materia.
- Emitir recomendaciones que coadyuven al mejoramiento del Modelo Integrado de Planeación y Gestión (MIPG) en las Dimensiones 2: Direccionamiento estratégico y planeación, Definir lineamientos para la administración del riesgo; Dimensión 4, Evaluación de resultados, Valores, transparencia y cambio cultural, evaluar resultados de gestión del riesgo y Dimensión 7, Control interno, Componente Evaluación del riesgo de la Entidad.

3. MARCO LEGAL.

- **Ley 87 de 1993, Literal a y f del Art.2** “Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones”.
- **Decreto 1083 de 2015 Art.2.2.21.5.4** “Administración de riesgos. Como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas las autoridades correspondientes establecerán y aplicarán políticas de administración del riesgo. Para tal efecto, la identificación y análisis del riesgo debe ser un proceso permanente e interactivo entre la administración y las oficinas de control interno o quien haga sus veces, evaluando los aspectos tanto internos como externos que pueden llegar a representar amenaza para la consecución de los objetivos organizaciones, con miras a establecer acciones efectivas, representadas en actividades de control, acordadas entre los responsables de las áreas o procesos y las oficinas de control interno e integradas de manera inherente a los procedimientos”.
- **Decreto 648 de 2017** Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública”. Artículo 17°. Modifíquese el artículo 2.2.21.5.3 del Decreto 1083 de 2015, el cual quedará así:

"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.

- **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”.
- **INCI. Resolución 20171010004373 Del 14/11/2017.** Se conforma el Comité de Gestión y Desempeño, se integra el Comité Institucional de Gestión y Desempeño, encargado de orientar la implementación y operación del MIPG.
- **INCI. Resolución 20171010002193 Del 13/07/2017.** Por la cual se modifica el Modelo de operación por procesos del INCI.
- **INCI. Resolución 20171000004803 Del 13/12/2017.** Se constituye el Comité Institucional de Coordinación del Sistema de Control Interno en el Instituto Nacional para ciegos INCI.
- Guía de Administración del Riesgo y el Diseño de Controles en entidades públicas del DAFP. Versión 4 2018

4. METODOLOGÍA.

Para la realización del presente informe, se aplicó la siguiente metodología:

- Revisión del soporte normativo establecido en materia de Administración de riesgos, aplicable al INCI.
- Procedimientos analíticos de validación del Mapa de Riesgos del INCI, conforme a la información suministrada por las áreas responsables, dueños de los 15 procesos.
- Consulta de la información en la página web de la entidad.
- Verificación de procesos, procedimientos, formatos documentos en la carpeta pública del Sistema Integrado de Gestión (SIG).
- Entrevista con los líderes y/o responsables de los procesos.
- Remisión de Informe Preliminar de resultados del seguimiento a los líderes y/o responsables de los procesos para sus observaciones y para la remisión de las evidencias solicitadas.
- Consolidación de la información y análisis.

5. DOCUMENTOS EXAMINADOS

- Mapa de riesgos Institucional.
- 15 Caracterizaciones de los procesos y procedimientos relacionados.
- Portal web de la entidad.
- Resultados Medición FURAG II 2018.
- Política de Administración de Riesgos vigente y anterior.
- Resoluciones INCI (Enunciadas en el Marco Legal).
- Listas de publicación contratación INCI.
- Manual del Sistema Integrado de Gestión.
- Seguimiento Al Plan Anual de Actividades del INCI
- Carpeta Pública del SIG.

6. RESULTADOS DEL SEGUIMIENTO Y ANÁLISIS.

6.1. LA ADMINISTRACIÓN DE RIESGOS EN LA ENTIDAD.

Control Interno realizó la evaluación con el fin de determinar el avance en la implementación del sistema de administración de riesgos de la entidad y la madurez del mismo con corte a agosto de 2019, verificando los resultados de la gestión realizada sobre los riesgos de gestión y seguridad digital identificados en el mapa de riesgos institucional. De acuerdo con lo anterior, se evidencia y concluye lo siguiente:

- Mediante Resolución 20151000000563 de 13/03/2015, se adopta y reglamenta la Política de administración de Riesgos en el INCI, con base en lo establecido en el Sistema Integrado de Gestión y Control – SIG que tiene como objetivo proteger a la organización de las situaciones indeseables que impidan el cabal cumplimiento de su misión u objetivos institucionales, así como evitar que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular (riesgos de corrupción).
- A través de la Resolución 20191010001973 de 12/08/2019 se actualiza la Política de Administración de Riesgos del INCI, con el propósito de establecer el marco general de actuación para la gestión de los riesgos a los que puede enfrenarse la entidad en el desarrollo de sus acciones. Se establece que la política de administración de riesgos es aplicable a todos los procesos de la entidad y a las acciones ejecutadas por los servidores públicos y contratistas durante el ejercicio de sus funciones.
- La entidad estableció un modelo de operación por procesos en cumplimiento de la normatividad vigente, para los procesos Estratégicos, Misionales, de Apoyo y de Control y Evaluación, evidenciándose 15 procesos, los cuales se encuentran documentados en la carpeta pública del SIG. En agosto 30 de 2019 se actualiza el mapa de procesos de la entidad.
- Se evidencia MAPA DE RIESGOS INSTITUCIONAL 2019 en la carpeta pública del SIG, con seguimiento para el primer y segundo cuatrimestre efectuado por los líderes y/o responsables de proceso.
- Se realiza seguimiento periódico a los riesgos a través del Mapa de Riesgos Institucional, por parte de los líderes de proceso. La evaluación a la gestión de Riesgos de corrupción del INCI, se realizó en desarrollo del seguimiento al Plan Anticorrupción y de Atención al Ciudadano y al Mapa de Riesgos de Corrupción, establecido en la Ley 1474 de 2011, para el segundo cuatrimestre de 2019, por lo tanto, no se incluyen en el presente informe.

6.2. INDICADOR DE DESEMPEÑO DEL REPORTE FURAG II 2018

Con base en los lineamientos contenidos en el Manual Operativo de MIPG; se realizó una medición a través del FURAG II, bajo los lineamientos e instrumentos establecidos por el

DAFP en el mes de febrero de 2019, con el fin de medir el estado de implementación de las 7 dimensiones y las 16 políticas del Modelo Integrado de Planeación y Gestión.

Los resultados de la medición realizada fueron presentados por el DAFP en el documento Reporte de Resultados de Desempeño Institucional MIPG 2018. Este índice refleja el grado de orientación del grupo de entidades de la rama ejecutiva del orden nacional hacia la eficacia (medida en que se logran los resultados institucionales), eficiencia (medida en que los recursos e insumos son utilizados para alcanzar los resultados) y calidad (medida en que se asegura que el producto y/o prestación del servicio responde a atender las necesidades y problemas de los grupos de valor).

El índice de desempeño institucional de las entidades nacionales fue de 74,3 y para el INCI de 73.7. De acuerdo con lo reportado en el mismo informe, uno de los índices desagregados de desempeño que tuvieron calificación baja corresponde **a la evaluación estratégica del riesgo con un puntaje de 65.8** lo que indica que la entidad debe establecer acciones de mejora frente a la gestión de los riesgos identificados. Este índice mide la capacidad de la entidad de identificar, evaluar y gestionar eventos potenciales, tanto internos como externos, que pueden afectar el logro de los objetivos institucionales.

De acuerdo con lo anterior, se recomienda avanzar en la revisión, ajuste e implementación de las políticas y dimensiones del MIPG y del MECI, teniendo en cuenta las debilidades presentadas en la medición realizada a través del FURAG II, con el fin de asegurar la adecuada gestión y administración de los riesgos institucionales y por ende fortalecer el Sistema de Control Interno de la entidad.

6.3. ANÁLISIS DE LOS RIESGOS DE GESTIÓN Y SEGURIDAD DIGITAL 2019.

De acuerdo con la revisión realizada al Mapa de Riesgos Institucional y los seguimientos publicados en la página web de la entidad, teniendo en cuenta los soportes documentales evidenciados y aportados por los líderes y/o responsables de los procesos, se concluye:

1. Riesgos identificados.

En esta etapa se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas, y las necesidades de las partes interesadas. Se incluyen en esta etapa el contexto interno, externo, de proceso, que se considerarán para la administración del riesgo, así como los activos de seguridad digital.¹

En la verificación realizada no se evidenció el análisis del contexto interno, externo, de proceso, ni la identificación de los activos de seguridad digital. Sin embargo, se evidencian las caracterizaciones de los procesos institucionales, donde se pueden encontrar algunos de estos elementos del contexto interno, externo y de proceso, aunque no se tienen identificados para ningún proceso los activos de seguridad digital, así mismo, se observó

¹ Guía para la administración del riesgo y el diseño de controles en entidades públicas- Riesgos de gestión, corrupción y seguridad digital. Versión 4. Octubre de 2018.

que al 30 de agosto de 2019 se actualizaron gran parte de los procedimientos, quedando pendientes de actualización algunos procedimientos de los procesos: Administrativo, Gestión Documental, Gestión Humana, Atención al Ciudadano e Informática y Tecnología .

El INCI tiene definidos 15 procesos, aprobados según Resolución 20171010002193 del 13/07/2017 Por la cual se modifica el Modelo de operación por procesos del INC, que fue actualizado en agosto 30 de 2019, según se evidencia en la carpeta pública SIG. Los 15 procesos tienen definidos 33 riesgos, 22 de gestión, 10 de corrupción y 1 riesgo de seguridad digital, como se observa:

No.	RIESGOS POR PROCESO	GESTIÓN	S.DIGITAL	SUBTOTAL	CORRUPCIÓN	TOTAL
	DIRECCIONAMIENTO ESTRATEGICO	2	0	2	0	2
1	PLANEACIÓN	1		1		1
2	COMUNICACIONES	1		1		1
	MISIONALES	7	0	7	6	13
3	ASISTENCIA TECNICA	2		2	1	3
4	PRODUCCIÓN Y MERCADEO	2		2	5	7
5	INCI RADIO	2		2		2
6	CENTRO CULTURAL	1		1		1
	DE APOYO	11	1	12	3	15
7	G.CONTRACTUAL	3		3	2	5
8	G. JURÍDICA	2		2	1	3
9	FINANCIERA	1		1		1
10	ADMINISTRATIVA	1		1		1
11	G.DOCUMENTAL	1		1		1
12	G.HUMANA	2		2		2
13	ATENCION AL CIUDADANO	1		1		1
14	INFORMATICA		1	1		1
15	EVALUACION Y MEJORAMIENTO	2		2	1	3
	GRAN TOTAL	22	1	23	10	33

Fuente: Mapa de Riesgos Institucional 2019 SIG. Cálculos propios.

En la identificación de los riesgos, se evidencian debilidades en el análisis de causas, como consecuencia de la falta del análisis de vulnerabilidades del contexto interno, externo, de proceso, y de identificación de los activos de seguridad digital, que pueden afectar el logro de los objetivos de los procesos.

Dentro de la evaluación realizada a la identificación del riesgo, se presentan las siguientes observaciones generales, las cuales se precisan en el mapa de riesgos para cada uno de los procesos:

- Se plantean como riesgos las mismas causas, con lo cual no se identifican adecuadamente los controles, incidiendo en la materialización del riesgo. (Proceso de Gestión Humana. Riesgo: Fallas en el software de liquidación de la nómina.)

- Se plantean causas externas no controlables por la entidad que dieron origen a controles (externos) no ejecutados por la entidad. (Proceso de biblioteca Virtual. Control: Gestión con Google).
- Débil análisis de causas que no facilita el establecimiento de controles efectivos, conllevando a la materialización del riesgo. (Proceso de Atención al Ciudadano – Riesgo: No dar respuesta oportuna a las PQRS).
- Se identifican como riesgos factores externos que no son controlables por la entidad (Proceso Asistencia Técnica. Riesgo: no se puede garantizar la implementación de criterios de accesibilidad... posterior a la asesoría del INCI).
- En general se identifican riesgos que no están claramente asociados al cumplimiento del objetivo del proceso, así como riesgos que no están claramente descritos, por lo que se dificulta su seguimiento y control.

Se observa que se han tipificado 3 tipos de riesgo: Gestión, Seguridad Digital y Corrupción, conforme lo dispone la Guía del DAFP, sin embargo, no se establecen para los riesgos de gestión otras tipologías tales como: Riesgos estratégicos, gerenciales, de cumplimiento, operativos, de imagen, establecidas en la misma guía.

No se identifican adecuadamente los riesgos de seguridad digital de acuerdo con lo establecido en la Guía del DAFP, en la cual se indica que este riesgo es una combinación de amenazas y vulnerabilidades en el entorno digital que incluye aspectos del ambiente físico, digital y las personas. Establece la guía que para la identificación de los riesgos de seguridad digital es condición necesaria identificar los activos dentro de los procesos que se ven afectados teniendo en cuenta criterios de confidencialidad, integridad y disponibilidad, tales como como aplicativos, software, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital, para lo cual se recomienda tener en cuenta el modelo de privacidad y seguridad de la información de la estrategia Gobierno Digital del Ministerio de las Tics.

De acuerdo con lo anterior, se recomienda fortalecer el análisis de causas, con el fin de lograr una identificación de los riesgos más adecuada, teniendo en cuenta los factores críticos internos, externos y de proceso que afectan el objetivo del proceso.

2. Valoración del Riesgo.

- La siguiente es la valoración de los riesgos de gestión y seguridad digital identificados, teniendo en cuenta la probabilidad de ocurrencia.

De los veintitrés (23) riesgos identificados, doce 15 (65%) se consideran con posibilidad de materializarse y seis (6) (26 %) son probables de ocurrencia, 1 (4%) es casi seguro que ocurra y 1 (4%) es raro que ocurra, sin que se hayan aplicado los controles (riesgo inherente). El riesgo calificado con probabilidad casi segura de ocurrencia se encuentra en el proceso de Producción y Mercado Social.

RIESGO INHERENTE (Antes control)			
PROBABILIDAD		Cantidad Riesgos	% part
1	Raro	1	4%
2	Improbable	0	0%
3	Posible	15	65%
4	Probable	6	26%
5	Casi seguro	1	4%
Total		23	100%

Fuente: Mapa de Riesgos Institucional

RIESGO RESIDUAL			
PROBABILIDAD		Cantidad Riesgos	% part
1	Raro	10	43%
2	Improbable	5	22%
3	Posible	7	30%
4	Probable	1	4%
5	Casi seguro	0	0%
Total		23	100%

Aplicados los controles (riesgo residual) disminuyeron a 7 (30%) los posibles, a 1 (4%) los probables, 5 bajan su probabilidad a improbables y 10 se consideran de ocurrencia rara.

El riesgo calificado como probable de ocurrir corresponde al proceso financiero, en tanto que los riesgos posibles se encuentran en los procesos de Gestión Humana, Producción y Mercadeo Social, Asistencia Técnica, Comunicaciones y Direccionamiento Estratégico.

- En la valoración de riesgos teniendo en cuenta el impacto que tendría su materialización en la entidad, vemos lo siguiente:

RIESGO INHERENTE (Antes control)			
IMPACTO		Cantidad Riesgos	% part.
1	Insignificante	0	0
2	Menor	0	0%
3	Moderado	3	13%
4	Mayor	16	70%
5	Catastrófico	4	17%
Total		23	100%

Fuente: Mapa de Riesgos Institucional

RIESGO RESIDUAL			
IMPACTO		Cantidad Riesgos	% part.
1	Insignificante	0	0%
2	Menor	0	0%
3	Moderado	10	43%
4	Mayor	10	43%
5	Catastrófico	3	13%
Total		23	100%

El 70% (16) de los riesgos, tienen un impacto mayor, el 17% (4) catastrófico y el 13% (3) Moderado, sin aplicar controles. Sin embargo, una vez aplicados los controles (riesgo residual), se mantienen 3 (13%) riesgos con impacto catastrófico, 10 (43%) con impacto mayor, valorándose los restantes 10 (43%) riesgos con impacto moderado. Se observa que con la aplicación de los controles no se reduce significativamente el impacto de materialización de los riesgos identificados pues el 56% se mantienen con impactos altos.

Los procesos que valoran los riesgos con impacto catastrófico a pesar de los controles aplicados son: Biblioteca Virtual para Ciegos (Centro Cultural), Emisora INCI Radio (producción radial y audiovisual), e Informática y tecnología. Los riesgos calificados con impacto Mayor corresponden a los procesos de Asistencia Técnica, Direccionamiento

De acuerdo con lo anterior, se recomienda realizar un análisis individual a los riesgos que tienen un impacto catastrófico y mayor con el fin de establecer controles más efectivos, que permitan disminuir las consecuencias (impacto) en caso de materialización.

- Teniendo en cuenta la zona de criticidad en la que se ubican los riesgos identificados, observamos:

RIESGO INHERENTE			
ZONA DE RIESGO		Cantidad Riesgos	% Part.
1	Baja	0	0
2	Moderada	1	4%
3	Alta	2	9%
4	Extrema	20	87%
Total		23	100%

RIESGO RESIDUAL			
ZONA DE RIESGO		Cantidad Riesgos	% Part.
1	Baja	0	0%
2	Moderada	6	26%
3	Alta	10	43%
4	Extrema	7	30%
Total		23	100%

Fuente: Mapa de Riesgos Institucional

El 87% (20) riesgos inherentes identificados se encontraban en zona extrema los cuales disminuyeron al 30% (7) una vez aplicados los controles (riesgo residual) y se distribuyeron en las zonas alta y moderada. La baja efectividad de algunos controles determina que, a pesar de su aplicación, el 73% de los riesgos continúen en las zonas alta y extrema de criticidad, con lo cual se recomienda su revisión y fortalecimiento.

Los siete (7) procesos que tienen riesgos residuales ubicados en la zona extrema son: Asistencia técnica, Centro Cultural, Direccionamiento Estratégico, Emisora INCI RADIO, Financiero, Gestión Humana e Informática y Tecnología. A su vez los riesgos que se encuentran en zona alta corresponden a los procesos: Asistencia Técnica, Comunicaciones, Evaluación y Mejoramiento, Gestión Humana, Gestión Contractual, Gestión Jurídica, Informática y Tecnología, Producción y Mercadeo Social, Servicio al Ciudadano, por lo que se recomienda fortalecer los controles, de tal manera que se logren bajar a zonas de menor riesgo.

3. Evaluación de controles.

De acuerdo con lo registrado en el Mapa de Riesgos Institucional, se han establecido 45 controles para los 23 riesgos de gestión y seguridad digital identificados.

PROCESOS	GESTIÓN	SEGURIDAD DIGITAL	CONTROLES
Administración documental	1		2
Administrativo	1		3
Asistencia técnica	2		4
Centro Cultural	1		1
Comunicaciones	1		2
Direccionamiento Estratégico	1		1
Emisora INCI Radio	2		3
Evaluación y mejoramiento	2		4
Financiero	1		1
Gestión Contractual	3		6
Gestión humana	2		4
Gestión Jurídica	2		4
Informática y tecnología		1	4
Producción y mercadeo social	2		4
Servicio al ciudadano	1		2
(en blanco)			
Total general	22	1	45

Fuente: Mapa de Riesgos Institucional

Las debilidades observadas en la identificación de los riesgos y el correspondiente análisis de causas, se reflejan en el establecimiento de controles adecuados que subsanen las causas originadoras del riesgo, observaciones que se detallaron en el mapa de riesgos para cada uno de los procesos.

Frente a los controles establecidos se realizaron las siguientes observaciones generales:

- Se establece como control acciones que corresponden al riesgo ya materializado (Proceso de comunicaciones)
- Se establece como control una acción que no es competencia de la entidad. (Proceso de Biblioteca virtual)
- Se incluyen como controles Procedimientos que no se encuentran actualizados y/o que se ejecutan parcialmente.
- Se establecen controles que no apuntan a subsanar la causa raíz del riesgo.
- Se establecen controles que no se ejecutan o se ejecutan parcialmente (Proceso Gestión Humana – Liquidación de la Nómina en Excel.)

La Guía para la gestión de riesgos y el diseño de controles expedida por el DAFP, Vigencia 2018, establece como criterios para evaluar el diseño de los controles, los siguientes aspectos:

- Identificar el Responsable de realizar la actividad de control.
- Definir la Periodicidad para su ejecución.
- Indicar cuál es el propósito del control.

Código: SG-110-FM-037-Versión: 7– Vigencia: 29/01/2019

- Establecer cómo se realiza la actividad de control.
- Indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.
- Dejar evidencia de la ejecución del control.

De la evaluación realizada se pudo evidenciar que la matriz utilizada por el INCI para la elaboración del mapa de riesgos objeto de evaluación, no contempla estos aspectos con precisión, por lo que el diseño y documentación de los controles establecidos no se ajusta a lo dispuesto por el DAFP en la Guía para la gestión de riesgos y el diseño de controles, lo que dificulta su seguimiento y evaluación, por lo que se recomienda su aplicación.

Esta debilidad ha sido subsanada ajustando la matriz Mapa de Riesgos Institucional DG-100-FM-281. V.4, en 19/09/2019, publicada en la carpeta SIG, en la cual se incluyen estos criterios, así como el análisis de contexto para la identificación de los riesgos, la cual servirá de base para la revisión y actualización de los riesgos institucionales para la vigencia 2019.

6.4. LINEAS DE DEFENSA

Las líneas de defensa miden la capacidad de la entidad pública para cumplir las responsabilidades asignadas en la gestión del riesgo y del control, de acuerdo con los roles establecidos. En el presente informe se realiza una verificación general del cumplimiento de las responsabilidades asignadas a las líneas de defensa en ejecución de los principios de autorregulación, autogestión, autocontrol y evaluación independiente del sistema de control interno de la entidad.

LÍNEA ESTRATÉGICA.

- Principio que ejecuta: Autorregulación
- Responsables:
 - Director General del INCI
 - Comité Institucional de Coordinación de Control Interno
- Responsabilidades:
 - Define el marco general para la gestión del riesgo y el control. Se da cumplimiento a través de la Política de Administración de riesgos de la entidad, establecida mediante Resolución 2015100000563 de 13/03/2015, actualizada mediante Resolución 20191010001973 de 12/08/2019.
 - Analiza los riesgos y amenazas al cumplimiento de los planes. Se verifica en las sesiones del Comité Institucional de coordinación de control interno. Durante la vigencia 2019 se han realizado en enero 31 de 2019, febrero 14 de 2019 y agosto 8 de 2019.
 - Garantiza el cumplimiento de los planes de la entidad. Se verifica en las sesiones del Comité de Gestión y Desempeño.
- Recomendaciones:
 - Fortalecer la gestión del CICCI en el análisis de riesgos y amenazas al cumplimiento de los planes de la entidad.

PRIMERA LÍNEA DE DEFENSA

- Principio que ejecuta: Autocontrol

Código: SG-110-FM-037-Versión: 7- Vigencia: 29/01/2019

- Responsables:
 - Gerentes Públicos. (Subdirector General y Secretario General)
 - Líderes de Proceso. (Líderes y/o responsables de los procesos misionales, estratégicos, de apoyo y de evaluación)
 - Gerentes Operativos de programas y proyectos.
- Responsabilidades:
 - Identificar, evaluar, controlar y mitigar los riesgos: Se ejecuta a través de la identificación, evaluación, seguimiento y gestión de los riesgos identificados en el mapa de riesgos institucional. El seguimiento a los riesgos se realiza periódicamente conforme lo establecido en la Política de administración de Riesgos.
 - Realizar mantenimiento efectivo de los controles internos: Se realiza a través de la ejecución, seguimiento y actualización a los procedimientos, con debilidades en el mantenimiento efectivo de los controles.
 - Ejecutar los procedimientos de riesgo y el control en el día a día. Se realiza a través de la ejecución, seguimiento y actualización a los procedimientos, evidenciándose debilidades en su operación.
- Recomendaciones:
 - Fortalecer la gestión de la primera línea de defensa en la identificación y evaluación de los riesgos, ejecución de los controles, mitigación de riesgos y mantenimiento efectivo de los controles internos, de acuerdo con los resultados de la evaluación a la gestión de riesgos realizada por la asesora de control interno.
 - Fortalecer la documentación de los procesos y procedimientos como elementos de control.

SEGUNDA LÍNEA DE DEFENSA

- Principio que ejecuta: Autogestión
- Responsables:
 - Jefe Oficina Asesora de Planeación
 - Coordinadores de otros sistemas: SGSST, SIG, SGD,
 - Supervisores e Interventores
- Responsabilidades:
 - Su objetivo es asegurar que la Primera Línea de Defensa está diseñada y opera de manera efectiva. Se establece mediante la revisión y actualización del modelo de operación por procesos y la definición de roles y responsabilidades de su ejecución.
 - Realiza Monitoreo y evaluación de controles y riesgos. Se evidencia acciones de monitoreo. No se evidencia evaluación a los controles y riesgos por parte de la segunda línea de defensa.
 - Asegura que los controles y procesos de gestión de riesgos de la Primera Línea de Defensa sean apropiados y funcionan correctamente. No se tiene evidencia de su aplicación.
- Recomendaciones:
 - Fortalecer la gestión de la segunda línea de defensa el monitoreo y evaluación de los controles y los riesgos establecidos por la primera línea de defensa y su funcionamiento efectivo.
 - Se recomienda que la OAP como líder del proceso de direccionamiento estratégico establezca lineamientos técnicos y de apoyo a los líderes de proceso

Código: SG-110-FM-037-Versión: 7- Vigencia: 29/01/2019

en la documentación adecuada de los procesos y procedimientos y en la identificación de los riesgos y controles.

TERCERA LÍNEA DE DEFENSA

- Principio que ejecuta: Evaluación Independiente
- Responsables:
 - Asesor de Control Interno.
- Responsabilidades:
 - Proporciona información sobre la efectividad del SCI. Se realiza a través de las auditorías, evaluaciones, seguimientos realizados en cumplimiento de la normatividad vigente y del Plan Anual de Auditoría basado en riesgos.
 - Proporciona información sobre la operación de la Primera y Segunda Líneas de Defensa con un enfoque basado en riesgos. Se evidencia en la evaluación realizada a la Gestión de Riesgos de la Entidad.
- Recomendaciones:
 - Incluir en las auditorías, evaluaciones y seguimientos realizados, información sobre la operación de las líneas de defensa.

7. CONCLUSIONES

Dado lo anterior, se puede concluir que el Instituto Nacional para Ciegos INCI, viene implementando y actualizando los requisitos establecidos en el MIPG y el Sistema de Control Interno, en relación con la Administración y Gestión de Riesgos, para lo cual ha expedido la Política de administración de Riesgos, actualizada en agosto de 2019.

Se tiene establecido el mapa de riesgos institucional, que incluye riesgos de gestión, de corrupción y de seguridad digital, aunque presenta debilidades en la identificación de los riesgos, análisis del contexto interno, externo y de proceso, así como en la identificación de los activos de seguridad digital, lo cual conlleva a que se presente debilidad en el establecimiento de controles efectivos para mitigar los riesgos identificados.

No se identifican adecuadamente los riesgos de seguridad digital de acuerdo con lo establecido en la Guía del DAFP, en la cual se indica que este riesgo es una combinación de amenazas y vulnerabilidades en el entorno digital que incluye aspectos del ambiente físico, digital y las personas.

Los líderes y/o responsables de procesos realizan seguimiento a los riesgos de corrupción cuatrimestralmente, sin embargo, se evidenciaron debilidades en la ejecución y seguimiento a los controles y acciones preventivas establecidas, originadas por las debilidades en su diseño y documentación.

Las debilidades evidenciadas en el diseño y documentación de los controles se presentan en los siguientes aspectos: en la definición del propósito de los controles establecidos (Verificar, validar, conciliar, comparar, revisar, cotejar, detectar), teniendo en cuenta que los controles pueden ser preventivos (reducen la probabilidad) o detectivos (reducen el impacto), en la identificación adecuada del responsable de ejecutar los controles, en el establecimiento de la periodicidad de ejecución de los controles, en la descripción de las

actividades que se realizan para ejecutar los controles, en las evidencias de la ejecución de los controles establecidos, para facilitar su trazabilidad y seguimiento.

Se está realizando actualización al mapa de procesos institucional y a la documentación de los procesos y procedimientos, aunque se evidencian debilidades en la documentación que requieren su revisión y ajuste (objetivos Smart, puntos de control, redacción de las acciones). No se evidencia alineación entre los controles establecidos en el mapa de riesgos institucional y los controles referenciados en los procedimientos.

Debe considerarse que el propósito de la gestión del riesgo es llevar los riesgos de la entidad a niveles aceptables, lo que se logra a través de controles internos efectivos, los cuales se despliegan a través de los procesos, procedimientos, políticas, instructivos. Los controles dentro del ciclo PHVA se encuentran identificados en las acciones del Verificar (V), Actuar (A).

De acuerdo a lo establecido en el Decreto 1083 de 2015, Artículo 2.2.21.5.5: Políticas de control interno diseñadas por el Departamento Administrativo de la Función Pública. Las guías, circulares, instructivos y demás documentos técnicos elaborados por el Departamento Administrativo de la Función Pública, constituirán directrices generales a través de las cuales se diseñan las políticas en materia de control interno, las cuales deberán ser implementadas al interior de cada organismo y entidad del Estado.

En cuanto a los riesgos de corrupción no se realizó evaluación y seguimiento en el presente informe, ya que fueron objeto de revisión con el informe del Plan Anticorrupción y Mapa de Riesgos de Corrupción al corte de agosto de 2019.

8. RECOMENDACIONES

- Revisar y ajustar el sistema de administración y gestión de riesgos del INCI, con respecto a las debilidades presentadas en la evaluación del FURAG II, con el fin de fortalecer la implementación de las Políticas y Dimensiones del MIPG y el Sistema de Control Interno de la entidad.
- Fortalecer la institucionalidad del esquema de las líneas de defensa en el INCI, con el fin de asegurar efectividad en el Sistema de Control Interno.
- Realizar análisis individual a los riesgos que tienen un impacto catastrófico y mayor con el fin de fortalecer los controles que permitan disminuir el impacto en caso de materialización.
- Fortalecer el análisis e identificación de los riesgos de seguridad Digital y la identificación de los activos asociados a los procesos institucionales, teniendo en cuenta las vulnerabilidades en cuanto a la disponibilidad, integridad y confiabilidad.
- En vista que el Departamento Administrativo de la Función Pública, expidió la “Guía para la administración del riesgo y el diseño de controles en entidades públicas, riesgos de gestión, corrupción y seguridad digital” en el mes de octubre del 2018, con el fin de que las entidades públicas la implementen y en el principio de la mejora continua, el

Código: SG-110-FM-037-Versión: 7– Vigencia: 29/01/2019

INCI debe ajustar sus mapas de riesgos a la nueva reglamentación y metodologías impartidas.

- Fortalecer las competencias de los líderes y/o responsables de la gestión de riesgos institucional en las metodologías establecidas por el DAFP, así como en la documentación de procesos.
- Implementar las acciones de contingencia establecidas para aquellos riesgos que se han materializado y fortalecer los controles establecidos de tal manera que se logre su mitigación.

Cordialmente,

**INFORME FIRMADO ELECTRONICAMENTE POR
MAGDALENA PEDRAZA DAZA**

Asesor Control Interno

Anexo: Mapa de Riesgos Institucional con seguimiento.

Elaboró y Revisó: Magdalena Pedraza Daza