EVALUACIÓN A LA GESTIÓN DE RIESGOS EN LAS TIC EN EL INSTITUTO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES

AGUSTÍN ALBERTO TORRES AGUDELO[1]

Resumen

Este artículo presenta una evaluación a la gestión de riesgos del proceso de tecnología de la información y las comunicaciones del Instituto Nacional de Medicina Legal y Ciencias Forenses, cuya base es el estándar ISO (International Organization for Standardization) 31000:2018 y la Guía para la administración del riesgo y el diseño de controles en entidades públicas. Teniendo en cuenta que estos lineamientos indican que se requiere para la gestión de riesgos, más no indican como se puede realizar esta gestión, se aplica una fase al proceso consistente en la revisión de la política de gestión de riesgos, identificación de riesgos, análisis y valoración de los riesgos, monitoreo y seguimiento, comunicación y consulta. Finalmente, y de acuerdo con los resultados del análisis y evaluación de los riesgos, se proponen recomendaciones a la gestión de riesgos al proceso de TIC.

Palabras Claves: Tecnología de la Información, Comunicaciones, Evaluación, Gestión de Riesgos, Vulnerabilidad, Amenazas.

Abstract

This document presents the evaluation of risk management to the information and communication technology process of the National Institute of Legal Medicine and Forensic Sciences. Whose basis is the ISO standard (International Organization for Standardization) 31000: 2018, considering that these indicate "what" is required for risk management but not indicated "how" this management can be carried out. In addition, it includes an analysis and recommendations for risk management.

The analysis is developed for the ICT process since the increase in

The use of information technologies in institutions requires the application of risk management for taking preventive measures and continuous improvement.

[1] Agustín Alberto Torres Agudelo, Ing. De Sistemas, Universidad Antonio Nariño, toagal@hotmail.com.

Key words**.** Information Technology, Communications, Evaluation, Risk Management. Vulnerability, Threats.

Introducción

Actualmente es tendencia que en las organizaciones, la alta dirección y los responsables de los distintos procesos, gestionen los riesgos para lograr el cumplimiento de los objetivos corporativos, es por esto que para el sector Gobierno, a través del decreto 1599 de 2005, la Función Pública decreta: "*El modelo estándar de control interno para el estado colombiano MECI 1000:2005, el cual determina las generalidades y la estructura necesaria para establecer, documentar, implementar y mantener un sistema de control interno en las entidades y agentes obligados conforme al artículo 5º de la Ley 87 de 1993".* (Departamento Administrativo de la Función Pública, 2005) Determinando que las entidades del estado deberían realizar la implementación del modelo, para de esta manera gestionar la calidad a través de una estrategia de mejoramiento que tangencialmente involucraba el análisis de riesgos. Esta normativa ha evolucionado al día de hoy con requerimientos legales explícitos para la gestión de las organizaciones enfocadas al riesgo, buscando cumplir los objetivos de las instituciones de modo que se pueda evaluar y mejorar la efectividad de los procesos, mediante la identificación de los riesgos internos y externos que logren influir en los resultados del plan estratégico establecido por la institución.

Para este artículo se refiere como se gestionaron los riesgos al proceso de TIC en el Instituto Nacional de Medicina Legal y Ciencias Forenses, es de anotar que el proceso de gestión de tecnología de la información y las comunicaciones es trasversal a los otros procesos de la institución. Donde los sistemas de información, los datos contenidos en ellos y la información son los activos más valiosos para la organización.

Desde la perspectiva teórica "la tecnología ha sido una fuerza poderosa en el desarrollo de la civilización, de la cual se ha servido el ser humano para acondicionar su entorno a fin de que se adapte mejor a sus necesidades (Ramírez, 2009)*."*

La relación entre la sociedad y la tecnología es enunciada por el filósofo alemán Nicholas Rescher de la siguiente manera: *"Por una parte, sólo ella [la tecnología] es capaz de proporcionarnos los requisitos para hacer posible la vida humana dentro de las condiciones del mundo moderno. Por otra parte, la tecnología misma hace que, de muchas maneras, la vida sea*

más complicada, menos agradable y más peligrosa" (Rescher, 1999, p.46). Los avances tecnológicos dentro de la institución son ahora objeto de análisis, pues su implantación dentro el contexto interno ha dejado de ser herramientas de apoyo para convertirse en funcionamientos colaterales de los procesos y con ellos, lograr garantizar la consecución de los objetivos misionales. Por otra parte, la tecnología de la información y las comunicaciones, "*no trae consigo únicamente un conjunto de beneficios, sino también una serie de riesgos e incluso incertidumbres que, de concretarse, pueden desencadenar efectos adversos sobre la salud humana y el ambiente en general, así como sobre la infraestructura. De esta manera, con la aparición y extensión de la tecnología a todos los ámbitos de la vida, nace para la sociedad un potencial de riesgo tecnológico o un nuevo escenario de riesgo de desastres: el riesgo tecnológico* (Ramírez, 2009)".

La característica principal del artículo es evaluar la gestión de riesgos del Instituto Nacional de Medicina Legal y Ciencias Forenses al proceso de TIC.

Se identificará y evaluará su sistema de gestión de riesgos y los controles al proceso de tecnología de la información y las comunicaciones, con el fin de determinar qué elementos podrían tener un impacto significativo en el sistema de control interno, teniendo en cuenta la normatividad vigente y los procesos de análisis y evaluación de riesgos realizado, tomando como referencia el decreto 1499-2017 (Funcion Publica , 2017) y el procedimiento de gestión de riesgos, implementando los riesgos de gestión en el aplicativo ISOLUCIÓN[2] y los de corrupción a través de la *herramienta Integral de Riesgos*, cumpliendo así con el marco legal establecido por el estado, con el fin de comprender el proceso y proponer recomendaciones al mismo.

Objetivos

Objetivo general

Evaluar la gestión de riesgos al proceso de TIC del Instituto Nacional de Medicina Legal y Ciencias Forenses.

[2] Isolucion: es un software para la administración del sistema de gestión de Medicina Legal, está orientado a dar cumplimiento a la normatividad MECI y NTCGP 1000.

Objetivos específicos

- Describir el proceso de gestión de riesgos y controles definido por el Instituto Nacional de Medicina Legal y Ciencias Forenses para el proceso de tecnología de la información y las comunicaciones.
- Analizar la política de administración, la identificación y la valoración de riesgos del Instituto Nacional de Medicina Legal y Ciencias Forense al proceso de tecnología de la información y las comunicaciones.
- Proponer recomendaciones al Instituto Nacional de Medicina Legal y Ciencias Forenses al proceso de tecnología de la información y las comunicaciones.

Metodología

El enfoque de este artículo es de carácter descriptivo y explicativo considerando el modelo para la gestión del riesgo y controles, previamente desarrollado por el Instituto Nacional de Medicina Legal y Ciencias Forenses, relacionado en el mapa de riesgo institucional dentro del proceso de gestión de infraestructura tecnológica y servicios informáticos. Se toma como referencia para comprender los controles definidos con el fin de llevar a cabo una evaluación descriptiva y proporcionar recomendaciones para incluir al sistema de gestión de riesgo y controles dentro del proceso de la entidad.

Marco Contextual

En la Ley 938 de 2004 en **Artículo 33**. (Senado de la Republica, 2004), se ordena al Instituto Nacional de Medicina Legal y Ciencias Forenses como entidad adscrita a la Fiscalía General de la Nación como estructura orgánica perteneciendo a la Rama Judicial, como establecimiento público del orden nacional, dotado de personería jurídica, patrimonio propio y autonomía administrativa.

Artículo 34. El sistema de Medicina Legal y Ciencias Forenses en todo el territorio nacional, es organizado y controlado por el Instituto Nacional de Medicina Legal y Ciencias Forenses.

Artículo 35. La misión fundamental del Instituto es prestar auxilio y soporte científico y técnico a la administración de justicia en todo el territorio nacional, en lo concerniente a medicina legal y las ciencias forenses.

Artículo 36. En desarrollo de su misión, el Instituto Nacional de Medicina Legal y Ciencias Forenses tiene las siguientes funciones relacionadas en la **Tabla 1.**

Tabla 1. Funciones Institucionales- INMLCF[3]

1	Organizar y dirigir el Sistema de Medicina Legal y Ciencias Forenses y controlar su funcionamiento.
2	Prestar servicios médico-legales y de ciencias forenses que sean solicitados por los Fiscales, Jueces, Policía Judicial, Defensoría del Pueblo y demás autoridades competentes en todo el territorio nacional.
3	Desarrollar funciones asistenciales, científicas, extra-periciales y sociales en el área de la medicina legal y las ciencias forenses.
4	Prestar asesoría y absolver consultas sobre medicina legal y ciencias forenses a las unidades de fiscalías, tribunales y demás autoridades competentes.
5	Definir los reglamentos técnicos que deben cumplir los distintos organismos y personas que realicen funciones periciales asociadas con medicina legal, ciencias
6	Servir de organismo de verificación y control de las pruebas periciales y exámenes forenses practicados por los cuerpos de policía judicial del Estado y otros organismos a solicitud de autoridad competente.
7	Servir como centro científico de referencia nacional en asuntos relacionados con medicina legal y ciencias forenses.
8	Ser organismo de acreditación y certificación de laboratorios, pruebas periciales y peritos en medicina legal y ciencias forenses, practicadas por entidades públicas y privadas.
9	Coordinar y adelantar la promoción y ejecución de investigaciones científicas, programas de postgrado, pregrado, educación continuada y eventos educativos en el área de la medicina legal y ciencias forenses.
10	Ser organismo de acreditación y certificación de laboratorios, pruebas periciales y peritos en medicina legal y ciencias forenses, practicadas por entidades públicas y privadas.
11	Coordinar y adelantar la promoción y ejecución de investigaciones científicas, programas de postgrado, pregrado, educación continuada y eventos educativos en el área de la medicina legal y ciencias forenses.
12	Coordinar y promover, previa existencia de convenios, las prácticas de docencia de entidades educativas aprobadas por el ICFES.
13	Divulgar los resultados de las investigaciones, avances científicos, desarrollo de las prácticas forenses y demás información del Instituto considerada de interés para la comunidad en general.

[3] **INMLCF**: El significado de la sigla es el acrónimo (Instituto Nacional de Medicina Legal y Ciencias Forenses).

14	Delegar o contratar en personas naturales o jurídicas la realización de algunas actividades periciales y controlar su ejecución

Fuente: Elaboración propia

Actualmente el instituto cuenta con dieciséis procesos internos para la toma de decisiones. En el Mapa de proceso institucional se detalla los procesos estratégicos, los misionales y de apoyo, es allí, donde se encuentra el proceso de gestión de infraestructura tecnológica y servicios informáticos tal como se muestra en la **Figura 1.**

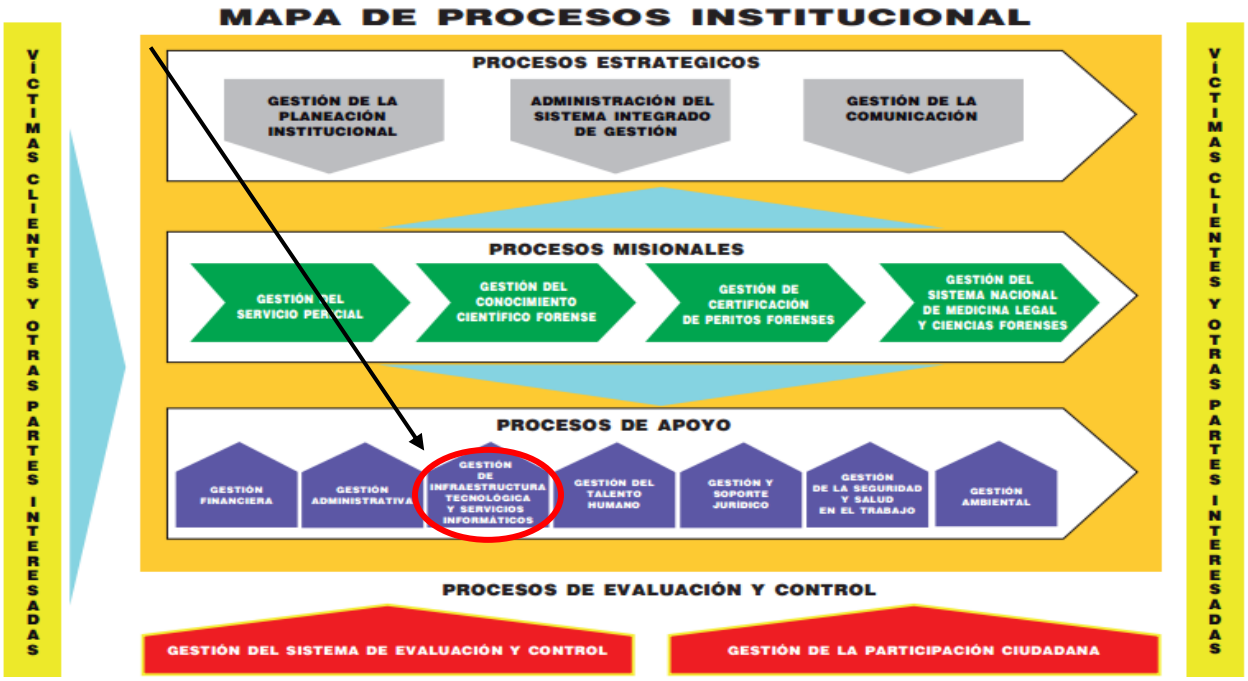


Figura 1*: "*Mapa de Procesos Instituto Nacional de Medicina Legal y Ciencias Forenses*"*

Fuente*: https://www.medicinalegal.gov.co/procedimientos-internos-para-la-toma-de-decisiones*

El proceso de gestión de tecnología de la información y las comunicaciones, es la tercera línea de defensa dentro del instituto en el marco del modelo integrado de planeación y gestión MIPG; se promueve la gestión TIC como la encargada de generar e implementar soluciones que provean en forma oportuna, eficiente y transparente; la información necesaria para el cumplimiento de los fines misionales del Instituto Nacional de Medicina Legal y Ciencias Forenses y formular lineamientos de estándares de calidad, seguridad y buenas prácticas para el manejo de la información en cumplimiento de la misión institucional.

Marco Legal o Normativo:

Se pudo analizar que, para el Instituto Nacional de Medicina Legal y Ciencias Forense, rigen diferentes leyes y normas que actualmente la administración de gestión de riesgo les establece a las entidades públicas, pero para este artículo describiremos las normas que aplican para este proceso, detallada en la siguiente Tabla.

Tabla 2. Normatividad Relacionada con el Proceso de TIC.

Normas	Descripción
Decreto 1499-2017	"Por medio del cual se modifica el Decreto número 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."
Decreto 1078 de 2015	"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"
NTC-ISO-IEC 31000-2018	"Es un estándar que proporciona los principios y directrices para la Gestión de Riesgos. Es aplicable a cualquier tipo de organización, independientemente del sector, tamaño o actividad que realice.
NTC-ISO-IEC 27001.2013	"Es un estándar para la seguridad de la información específica los requisitos necesarios para establecer, implantar, mantener y mejorar un (SGSI) según el conocido como "Ciclo de Deming": PDCA - acrónimo de Plan, Do, Check, Acta (Planificar, Hacer, Verificar, Actuar).
NTC-ISO-IEC 9001-2015	"Es una norma internacional que se centra en todos los elementos de la gestión de la calidad con los que una empresa debe contar para tener un sistema efectivo que le permita administrar y mejorar la calidad de sus productos o servicios.
Resolución No. 000729 del 29 de agosto de 2016	"Por la cual se adopta el Sistema Integrado de Gestión."
La resolución No. 000198 de 01 de abril de 2019	"Por la cual se adopta el Sistema de Gestión de la Seguridad de la Información-SGSl, la Política de Seguridad de la Información y se establecen los controles del Sistema"
La resolución No. 000837 de 22 noviembre de 2019	"Por lo cual se adopta el Sistema de Gestión de la Seguridad de la información-SGSI, la Política de Seguridad de la información y se establecen lineamientos Para Su uso y manejo.

El Procedimiento de Gestión de riesgos	INMLCF "Gestionar los diferentes riesgos que puedan presentarse en la entidad mediante mecanismos de prevención y detección, de tal manera que las actividades de monitoreo, seguimiento y evaluación de las acciones, permitan reducir efectivamente la incidencia negativa de eventos no deseados en los procesos institucionales."

Fuente: Elaboración Propia

Metodologías de análisis de riesgos.

La metodología de análisis de riesgos tiene como objetivo la identificación, evaluación, tratamiento y monitorización de los riesgos asociados a una actividad, función o proceso, los riesgos no tienen el mismo origen ni la misma naturaleza, por lo tanto, existen varias estrategias para su gestión, es importante dejar claro que las metodologías de análisis de riesgos se dividen en dos grupos principales: cualitativos y cuantitativos, detalladas en la siguiente tabla.

Tabla 3. Descripción de los Análisis de riesgo Cualitativos y Cuantitativos.

Análisis de Riesgos	Ventajas	Desventajas	Forma de realizar el Análisis
Cualitativos	• Son sencillos de realizar • Poco costosos • Utilizan la experiencia de los especialistas.	• Son subjetivos • Los resultados pueden variar según las personas involucradas • Se requiere un análisis cuantitativo posteriormente para complementar el análisis	• Preguntas precisas acerca de la actividad y los resultados. • Desarrollar modelos matemáticos que vinculan la Actividad y los resultados • Obtener evidencias pertenecientes al modelo • Asignar valores cuantitativos • Calcular resultados • Analizar resultado.
Cuantitativos	• Emplean métodos probabilísticos y estadísticos para la determinación de riesgos. • Los resultados son más exactos. • Son objetivos.	• Son más costosos • Requieren de mayor tiempo • No son recomendables para procesos simples.	• Lista de verificación (Checklists). • Análisis preliminar • ¿Qué paso aquí? • Análisis de modo de fallo y efecto (FMEA).

Fuente: elaboración Propia con base en (Jorge Montoya Martínez, 2008)

Los estándares recomendados para el análisis de riesgos son ISO 31000, COBIT 5, ISO 27005, ISM3, AS/NZS 4360, SDMAP, MAGUERIT, OCTAVE, MEHARI, SP800-39. La cual adoptada de acuerdo a las necesidades de cada organización en la tabla 4, se realiza una comparación de los estándares vs sus propósitos.

Tabla 4. Comparativo Estándares VS Propósitos

Propósito de la Norma	ISO 31000	COBIT 5	ISO 27005	ISM3	AS/NZS 4360	SP800-30 4360	SDMAP	MAGUERIT	OCTAVE	MEHARI	SP800-39
Establecer el contexto. Medir y caracterizar el estado actual de los sistemas y la organización.	X	X	X	X	X	X				X	X
Identificar y valorar los activos críticos	X	X						X	X		
Identificar las amenazas y las vulnerabilidades de la Organización	X	X				X		X	X		
Identificar los componentes claves y las vulnerabilidades técnicas que ocasiona los riesgos		X		X	X	X		X	X		
Evaluar el riesgo. Identificar el riesgo. Estimar el riesgo. Valorar el riesgo.	X	X	X		X	X	X	X	X		X
Determinar y evaluar el impacto	X	X						X		X	
Evaluar la gravedad del escenario	X	X								X	
Tratar el riesgo. Identificar las exigencias de seguridad y las normas existentes. Desarrollar estrategias de protección basadas en buenas prácticas. Implementar protecciones	X	X	X	X	X	X	X	X	X		X
Aceptar el Riesgo	X	X	X	X						X	X
Comunicar el riesgo.	X	X	X							X	
Realizar seguimiento al riesgo. Monitorear y revisar	X	X	X	X	X	X	X	X	X	X	X
Documentar resultados	X	X				X					X

Nota: *Las X corresponde al propósito incluido en la Norma***.**

Fuente: Elaboración Propia con base Guerrero en (2010).

Cada institución puede elegir una metodología o una guía de buenas prácticas a seguir o bien definir una propia que esté acorde con su particularidad. En el caso particular de este artículo se tuvo como punto de partida el documento "Manual para el Sistema de Administración de Riesgos en el Instituto Nacional de Medicina Legal y Ciencias Forenses" en el que en la entidad plasma la política y la matriz de riesgos publicada en la herramienta de gestión ISOLUCION.

Resultados

Proceso de gestión de riesgos de Tecnología de la Información y las Comunicaciones del Instituto Nacional de Medicina Legal y Ciencias Forenses.

El grupo nacional de tecnología de la Información y las comunicaciones del Instituto Nacional de Medicina Legal, es el encargado de desarrollar el proceso de evaluación de riesgos, puestos que para el proceso de TIC determina unas actividades que hacen parte de la etapa de desarrollo de la gestión, tal como se detalla en la tabla 5.

Tabla 5. Etapa para el Desarrollo de Gestión de Riesgos al Proceso de TIC.

Actividad	Descripción de la Actividad
Establecer la política de gestión del riesgo	1. Revisión de la normativa y directrices del Gobierno Nacional, relacionadas con la gestión del riesgo y analizar su alineación con la planeación estratégica institucional: Misión, Visión y objetivos estratégicos. 2. Analizar el contexto para el proceso de TIC. 3. Divulgar a su equipo de trabajo los lineamientos determinados en la Política de Gestión del Riesgo en el Instituto Nacional de Medicina Legal y Ciencias Forenses que contiene las siguientes Políticas: **Política de Protección de Datos** **Política de Datos Abiertos** **Política de Seguridad de la Información**
Identificar los Riesgos	1. Realizar y participar en la identificación de causas de acuerdo al contexto e identificar los riesgos de TIC.
Análisis y Valoración del Riesgos	1. Analizar la probabilidad e impacto de los riesgos identificados para el proceso de TIC 2. Establecer las actividades de control y sus acciones asociadas idóneas que permitan administrar los riesgos identificados para el proceso de TIC.
Monitoreo y seguimiento	1. Realizar el seguimiento correspondiente al mapa de riesgos de TIC. 2. Tomar la responsabilidad frente al seguimiento de los controles que están a su cargo a las funciones que realiza y realizarlo en los tiempos estipulados.
Comunicación y Consulta	1. Participar en los procesos de aprendizaje que se programan y facilitar la asistencia de los profesionales u trabajadores de su equipo de trabajo.

Fuente: Elaboración Propia con base Rodrigo (2020).

El procedimiento de gestión del riesgo, se incluye en la *herramienta integral de riesgos* – HIR. V05 de ISOLUCION (Sistema de Información de Gestión) por el responsable del proceso. En este caso el coordinador(a) nacional de tecnología de la información y las comunicaciones y sus colaboradores, realizan la construcción del mapa de riesgos, identificación, tratamiento y monitoreo, así como evaluación de controles y acciones de mejora, tanto a nivel regional como a nivel central, apoyados por la oficina de planeación y los facilitadores del sistema integrado de gestión – SIG quienes asesoran metodológicamente dichas actividades.

Análisis a la gestión de riesgos al proceso de TIC en el Instituto Nacional de Medicina Legal y Ciencias Forenses

De acuerdo con las particularidades del Instituto Nacional de Medicina Legal y Ciencias Forenses en el proceso de TIC, se contempla la NTC-ISO 27005 que va de la mano con su SGSI[4] y una que es muy específica en la gestión de riesgos que es la norma ISO 31000:2018. Como se detalla en la **Figura 2**.

Figura 2 ISO 31000:2018

Fuente: Tomada https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

En este sentido la estructura de la norma, responde adecuadamente como insumo para la gestión de riesgos impuesta por la función pública, ya que sus principios abarcan de manera sistémica la

[4] SGSI: Es la abreviatura usada para referirse al Sistema de Gestión de la Seguridad de la Información e ISMS son las siglas equivalentes en ingles a (Information Security Management System)

gestión de riesgo en las operaciones del proceso de tecnología de la información y las comunicaciones del instituto, las cuales pueden ser utilizadas por cualquier otro tipo de proceso ya que es de carácter genérico. Se llevará a cabo el proceso de la gestión de riesgos de cada una de las fases de la ISO 31000:2018, las cuales son: establecer la política de gestión de riesgos, identificación de riesgos, analizar y valorar los riesgos, monitoreo y seguimiento, comunicación y consulta.

a) Fase Establecer la política de gestión del riesgo.

Se evidencia que no hubo comunicación y consulta para definir un alcance, o criterios más limitado, por parte del equipo de trabajo de TIC. Por ejemplo; un análisis de riesgos sobre los sistemas de información de TIC relacionado con la página web del Instituto, SIRDEC[5], etc.

b) Fase Identificación de riesgos

Para el levantamiento de esta fase al revisar la lista de posibles riesgos, así como la experiencia y el conocimiento del equipo de TIC no se incluyó reunión de experticia para el análisis de riesgo. (ej. Intercambio de información interna y externa).

También se puede evidenciar que no se consideró la identificación de algunos riesgos potenciales como caídas de sistemas, virus, daños a activos materiales, fallas o errores en procesos de seguridad digital y riesgos de seguridad de la información de manera clara que permitiera hacer la categorización de los riesgos.

El análisis de causa y de efectos relacionadas con la etapa de *identificación de riesgos* en el aplicativo ISOLUCION Módulo Riesgos DAFP. Como se evidencia en la Tabla 6.

[5] SIRDEC: Es un Sistema de Información del Instituto donde se registra información de Red Desaparecidos y cadáveres http://sirdec.medicinalegal.gov.co:8083/sirdec

Tabla 6: Riesgos Creados

Núm.	Nombre	Clasificación del Riesgo	Etapa	Fecha de Creación	Responsable	Proceso	Regional-Seccional-Unidad Básica	Causa	Efecto	Unidad Organizacional	Agente Generador
GITS-11	Incumplimiento de las normas de seguridad de la información	Operativo		2020		Gestión de Infraestructura Tecnológica y Servicios Informáticos	Dirección General	C1: Falta de cultura en temas relacionados con la seguridad de la información. C2: Falta de divulgación, socialización y apropiación de las políticas de seguridad de la información.	E1-C1- Vulnerabilidad en los activos de información. E2-C2- Incumplimiento de la políticas o directrices establecidas.	Grupo Nacional de Tecnologías de Información y Desarrollo	Persona, Proceso
GITS-12	Manejo inadecuado del recurso informático	Operativo		2020		Gestión de Infraestructura Tecnológica y Servicios Informáticos	Dirección General	C1: Desactualización o desconocimiento de los procesos y procedimientos establecidos por TI.	E1-C1- Incumplimiento de las directrices, políticas, procesos y procedimientos establecidos.	Grupo Nacional de Tecnologías de Información y Desarrollo	Persona, Proceso
GITS-13	Inoportuna prestación de servicios informáticos	Operativo		2020		Gestión de Infraestructura Tecnológica y Servicios Informáticos	Dirección General	C1- Falta de creación de Acuerdos de Niveles de Servicio de Tecnologías de Información.	E1-C1- Demora en la atención de incidentes y requerimientos de TI.	Grupo Nacional de Tecnologías de Información y Desarrollo	Proceso
GITS-14	Inestabilidad de la plataforma tecnológica	Operativo		2020		Gestión de Infraestructura Tecnológica y Servicios Informáticos	Dirección General	C1- Falta de esquemas procedimentales para el manejo de la continuidad de TI y recuperación de desastres.	E1-C1- Perdida total o parcial de la continuidad de TI que afecta ka prestación de los servicios institucionales.	Grupo Nacional de Tecnologías de Información y Desarrollo	Proceso, Tecnología

GITS-15	Vulnerabilidad de la información contenida en los aplicativos y sistemas de información institucionales	Corrupción		2020		Gestión de Infraestructura Tecnológica y Servicios Informáticos	Dirección General	C1 - (H) - Falta de conocimiento e incumplimiento de las políticas de seguridad de la información institucionales. C2 - (H) - Falta de metodología para el desarrollo de Sistemas de Información institucionales. C3 - (H) - Falta de adopción de lineamientos establecidos por los entes de control de TI.	E1-C1- Afectación en la integridad, disponibilidad y confiabilidad de los datos contenidos en los sistemas de información. E2-C2- Incumplimiento en el entendimiento de los requisitos, patrones de diseño, calidad, modularidad, diseños agiles y documentación. E3-C3- Incumplimiento de las normas y lineamientos establecidos.	Grupo Nacional de Tecnologías de Información y Desarrollo	Persona, Proceso

Fuente: Sistema de Información ISOLUCION http://192.168.1.160:9126/IsolucionMedicinaLegal/RiesgosDafp/frmRiesgoConsultar.aspx?IdRiesgo=MzEx.

Es importante señalar, que la matriz nos permite llevar el registro de los riesgos detectados, para contar con un inventario de los mismos, al establecer el objetivo, proceso o plan que puede verse afectado por un determinado riesgo, así como las causas y el impacto posible, de allí, el alcance que se tiene en un adecuado levantamiento de activos entrada/salida al sistema de gestión, el cual tiene las siguientes ventajas, por ejemplo: reduce altos costos económicos ocasionados por mantener cantidades excesivas de inventarios, reduce el riesgo de corrupción, robos o daños físicos, amenaza a la seguridad digital, a estos controles pre-operativo es que se conoce como control preventivo, por eso la importancia de la interrelación con otros procesos e indicadores dentro del instituto.

c) Fase Analizar y Valorar los Riesgos.

Para esta etapa del análisis y la evaluación se prestó especial atención en el aplicativo ISOLUCIÓN, a las preguntas de cómo se identificaron y se evaluó el impacto a los riesgos del proceso de TIC, pudiendo haber un sesgo en el resultado de la calificación, considero que se debe incluir otros tipos de preguntas acorde al proceso, ya que las preguntas de evaluación de riesgos descritas son muy generales al contexto.

Ver Tabla 7. Preguntas Impacto de Evaluación de Riesgos

No	Pregunta Si el riesgo de corrupción se materializa podría...	Respuesta	
		Si	No
1	¿Afectar al grupo de funcionarios del proceso?	○	◉
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	○	◉
3	¿Afectar el cumplimiento de misión de la Entidad?	○	◉
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la Entidad?	○	◉
5	¿Generar pérdida de confianza de la Entidad, afectando su reputación?	○	◉
6	¿Generar pérdida de recursos económicos?	○	◉
7	¿Afectar la generación de los productos o la prestación de servicios?	○	◉
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?	○	◉
9	¿Generar pérdida de información de la Entidad?	◉	○
10	¿Generar intervención de los órganos de control, de la Fiscalía, u otro ente?	◉	○
11	¿Dar lugar a procesos sancionatorios?	◉	○
12	¿Dar lugar a procesos disciplinarios?	◉	○
13	¿Dar lugar a procesos fiscales?	○	◉
14	¿Dar lugar a procesos penales?	◉	○
15	¿Generar pérdida de credibilidad del sector?	○	◉
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?	○	◉
17	¿Afectar la imagen regional?	○	◉

Total, Preguntas Afirmativas: 5	**Clasificación del Riesgo:** Moderado ◉ Mayor ○ Catastrófico ○
Total, Preguntas Negativas: 13	**Puntaje: 5**

Fuente: Sistema de Información ISOLUCION

http://192.168.1.160:9126/IsolucionMedicinaLegal/RiesgosDafp/frmRiesgoConsultar.aspx?IdRiesgo=MzEx.

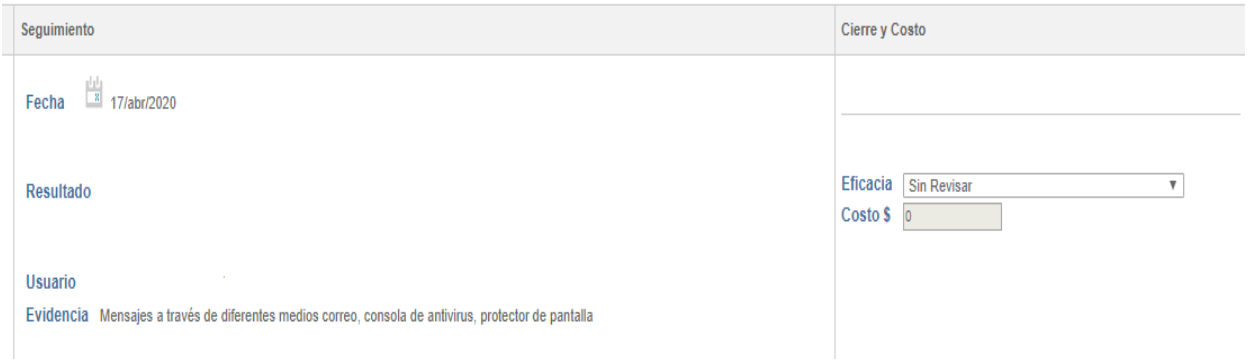
Pues a pesar de tener una estructura definida dentro de sus procesos, el sistema de información ISOLUCION, no permite integrar preguntas asociadas al proceso de TIC. Todo lo anterior, demuestra la necesidad que la alta dirección replantee mejorar el sistema de información o establecer una metodología que supla estas falencias.

Para poder cumplir conforme al alcance del proceso de TIC un adecuado tratamiento a los riesgos.

d) Monitoreo y Seguimiento

Los conceptos, procesos, y actividades presentadas se adecuan a la norma ISO 31000: 2018 como se muestra en la **Figura 2**. El monitoreo y seguimiento es la entrada de verificación continua en todas las etapas del proceso. Por lo que, la *herramienta integral de riesgos* – HIR. V05 de ISOLUCION (sistema de información de gestión) tiene una adecuada labor permitiendo hacer supervisión, revisión sobre el estado actual del riesgo y su gestión a través de alertas y notificación permitiendo tener actualizado el sistema.

Ver Figura 3.



Fuente: Sistema de Información ISOLUCION

http://192.168.1.160:9126/IsolucionMedicinaLegal/RiesgosDafp/frmRiesgoConsultar.aspx?IdRiesgo=MzEx

Adicionalmente, se sugiere llevar un registro documentado del tratamiento del riesgo, así como las acciones realizadas para mitigar el impacto y ver el resultado para futuros hallazgos.

e) Comunicación Y Consulta.

En esta etapa, se informa el riesgo y la forma como será tratado, para todas las áreas operacionales y sus gestores, pero no garantiza que dentro del proceso de TIC se tomen en consideración las necesidades de las partes interesadas, así mismo como los diferentes puntos de vista y le den la importancia durante todo el proceso de administración del riesgo y se fomente que ésta sea una actividad inherente al que hacer del Instituto. La divulgación y consulta del mapa de riesgos se realizará en la página web del INMLCF a través de un enlace directo de fácil acceso al ciudadano y partes interesadas.

Recomendaciones al proceso de TIC.

A pesar de que la alta dirección está comprometida sin embargo hace falta una efectiva comunicación del sistema de gestión de riesgos a todos los niveles de la Institución, se propone una estrategia distribuida de comunicación interna, promover al interior de la organización una cultura basada en riesgos.

Tabla 8. Estrategia de Comunicación

Comunicación oficial de la alta dirección
Campaña de expectativa/e incentivo
Capacitaciones al personal
Informe de avances
Retroalimentación continua

Fuente: Elaboración propia.

Involucrar a los funcionarios que participan en el proceso de TIC, a fin que contribuya al cumplimiento de los controles y en general al fortalecimiento de la gestión de riesgos en el uso de la *herramienta integral de riesgos* – HIR. V05 de ISOLUCION (Sistema de información de gestión), de manera que se conviertan en *gestores de riesgos* al interior del instituto.

- Realizar simulacros periódicos para el análisis de riesgos con la información histórica, adoptando el uso de herramientas y técnicas para facilitar el proceso de la valoración de

riesgos como lo recomienda la Función Pública. (consultar anexo 2. Técnicas para Establecimiento del Contexto y Valoración del Riesgo).

- Aunque se cuenta con la *herramienta integral de riesgos* – HIR. V05 de ISOLUCION (sistema de información de gestión); No es eficaz al proceso de TIC, Por tal motivo se hace fundamental que la alta dirección del Instituto respalde al fortalecimiento e integre el modelo de seguridad y privacidad de la información (MSPI) al sistema de Información ISOLUCION, para gestionar cualquier riesgo asociado a esta que se pudiera materializar, sería catastrófico en el equilibrio misional, reputacional y/o de la operación de la organización. Por eso la importancia de los controles sobre la información y sus activos son una responsabilidad de todas y cada una de las personas de la organización y no solo del área de T.I

Conclusiones

Se resalta la importancia de la evaluación del proceso de tecnología de la información y las comunicaciones del Instituto Nacional de Medicina Legal y Ciencias Forenses, en las cuales se implementa la norma ISO 31000:2018 en sus programas de gestión de riesgos de TIC, mediante el proceso del estándar se identifica los aspectos fuertes y débiles de la implementación, y de la misma forma las posibilidades de complementar con los elementos que ofrecen otros estándares como la línea de 27005 donde Instituto lo tiene como referente en SGSI.

La obtención de sinergias demuestra la posibilidad de completar que el modelo de gestión de riesgos de la ISO 31000:2018 y otras como ISO 27005 o los lineamientos del *NIST (National Institute of Standard Technology*) Instituto Nacional de Estándares y Tecnología, en el proceso de TIC, ratifica que ningún estándar de referencia garantiza el éxito de la implementación de un sistema de gestión de riesgos, si no por el contrario, el correcto entendimiento del estándar y la adopción e integración del modelo con la Institución y la alta dirección, son los factores que aumenta la probabilidad de éxito del sistema de gestión de riesgos teniendo en cuenta factores trasversales como el gobierno, la cultura y las TIC.

Finalmente se considera que la utilización del estándar 31000:2018 en el proceso de tecnología de la información y las comunicaciones en el INMLCF, la gestión de riesgos implica una constante evolución y compromiso de los gestores del proceso, con el fin de cumplir con los objetivos y asegurar la información crítica, y adicionalmente la gestión adecuada de los riesgos que permita evitar en gran medida, la ocurrencia de incidentes y con ello cumplir con una activación de planes de continuidad.

Referencias

Castillo, R. P. (18 de Mayo de 2020). Personal . Bogotá, Colombia.

Departamento Administrativo de la Función Pública. (20 de Mayo de 2005). *Decreto 1599*. Bogota, Colombia: http://www.suin-juriscol.gov.co/.

Funcion Publica . (11 de Septiembre de 2017). Decreto 1499 de 2017. *Sistemas de Gestión* . Bogotá , Colombia: Publicado en el Diario Oficial No.50.353.

Funcion Publica . (20 de May0 de 2020). Obtenido de funcionpublica.gov.co: https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view/34316316

Instituto Nacional de Medicina Legal y Ciencias Forense. (08 de Mayo de 2020). Obtenido de Ins.Nal. Medicina Legal y Ciencias Forense: https://www.medicinalegal.gov.co/gestion/ley-1474-de-2011/planes-operativos

Instituto Nacional de Medicina Legal y Ciencias Forense. (08 de Mayo de 2020). *Aplicativo ISOLUCIÓN*. Obtenido de Aplicativo ISOLUCIÓN: http://isolucion.medicinalegal.gov.co:9126/IsolucionMedicinaLegal/PaginaLogin.aspx

Instituto Nacional de Medicina Legal y Ciencias Forense. (08 de Mayo de 2020). *Ins. Nal Medicina Legal y Ciencias Forense.* Obtenido de https://www.medicinalegal.gov.co/procedimientos-internos-para-la-toma-de-decisiones

Instituto Nacional de Medicina Legal y Ciencias Forenses. (8 de Mayo de 2020). Obtenido de https://www.medicinalegal.gov.co/plan-estrategico-2019-2022

ISO 31000. (20 de Mayo de 2020). *IEC 31010, Risk management — Risk assessment techniques*. Obtenido de https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

Jorge Montoya Martínez. (23 de Julio de 2008). *Colección de Tesis Digitales.* Obtenido de Univeridad de las Americas Puebla: http://catarina.udlap.mx/u_dl_a/tales/documentos/lpro/montoya_m_j/capitulo3.pdf

Ramírez, O. (2009). Riesgos de origen tecnológico: apuntes conceptuales para una definición, caracterización y reconocimiento de las perspectivas de estudio del riesgo tecnológico. *Revista Luna Azul*, pp. 82-94.

Rescher, N. (1999). Razón y valores en la era científico-tecnológica. Paidós.

Senado de la Republica. (17 de Diciembre de 2004). *Secretaria del Senado* . Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_0938_2004.html