ANÁLISIS DE GESTIÓN DE RIESGOS DE INFORMACIÓN BASADO EN EL PROCESO DE GOBIERNO DE INFORMACIÓN PARA TOMA DE DECISIONES: CASO CENTRO NACIONAL DE MEMORIA HISTÓRICA

FLOR ENITH GUTIÉRREZ RIVERA

JOHANA CATALINA MURCIA MENDOZA

PONTIFICIA UNIVERSIDAD JAVERIANA

FACULTAD DE COMUNICACIÓN Y LENGUAJE

CARRERA CIENCIA DE LA INFORMACIÓN, BIBLIOTECOLOGÍA Y ARCHIVÍSTICA

BOGOTÁ, D.C.

2021

Reglamento de la Pontificia Universidad Javeriana

Artículo 23

"La Universidad no se hace responsable por los conceptos emitidos por los alumnos en sus trabajos de grado, solo velará porque no se publique nada contrario al dogma y la moral católicos y porque el trabajo no contenga ataques y polémicas puramente personales, antes bien, se vean en ellas el anhelo de buscar la verdad y la justicia"

Nota de aceptación

_____

_____

_____

_____

_____

Presidente del jurado

_____

Jurado

_____

Jurado

Agradecimientos

Gracias a Dios por permitirme alcanzar este logro trazado hace 5 años y que hoy se hace realidad. A cada uno de los profesores por su paciencia y dedicación los cuales hicieron parte de esta formación profesional y de manera muy especial a Luis Gabriel Peñaloza, director del presente trabajo de grado por su apoyo y acompañamiento en esta etapa.

Agradezco a mis hermanos; Martha, Elizabeth, Alberto, Liliana y Alexandra por el apoyo que me brindaron desde el inicio de mi carrera y la culminación de ella. A mi hermanita Nancy Gutiérrez Rivera, aunque no está con nosotros nos sigue acompañando en cada uno de nuestros logros, a mis hijos Andrés Felipe Moreno y Juan Sebastian Moreno que han sido el motor que me impulsan a lograr cada meta. A mi compañero de vida Juan Sora Gómez. A la profesora Lida villa por impulsarme a realizar mis sueños profesionales. A cada uno de mis compañeros que hicieron parte de este proceso de formación personal, de manera muy especial a mis amigos y compañeros de experiencia; Oscar Andrés Guzmán, Johana Catalina Murcia y Magnolia Cerquera, por su apoyo incondicional. Finalmente agradezco a la Pontificia Universidad Javeriana por darme la oportunidad de alcanzar este tan importante logro. ¡Mil gracias!

Flor Enith Gutiérrez

“Él es fuerzo, disciplina, constancia, sumado a la pasión por tu lo que haces, siempre te llevara a cumplir tus metas”

Johana Catalina Murcia Mendoza

Título

“Análisis de gestión de riesgos de información basado en el proceso de gobierno de información para toma de decisiones: caso Centro Nacional de Memoria Histórica”

Contenido

Lista de tablas

Lista de figuras

Resumen

El presente trabajo de grado tiene como objetivo presentar un análisis de gestión de riesgos de la información, con base en un modelo de gobernanza de información aplicado en el Centro Nacional de Memoria Histórica (CNMH). Para ello se define y se desarrolla el concepto de información, partiendo de su evolución a través del tiempo y los ciclos que tienen estos datos. Asimismo, se contextualiza la importancia de la información en las organizaciones y, a su vez, la implantación de un modelo de gobierno de información, a través de una mirada analítica en la gestión de riesgos.

Para tal fin se presentan unas herramientas que abarcan el concepto de información en la gestión de riesgos, que se identifican mediante el análisis de diferentes metodologías y normas. De este modo se pueden mapear los riesgos de información teniendo en cuenta los datos recolectados por medio de una entrevista y un inventario de información.

Al realizar dicho análisis de riesgos, se establecieron los riesgos en una matriz con sus respectivos factores, eventos, causas y consecuencias, teniendo en cuenta escalas de valoración y la proyección de controles para mitigar la materialización de estos sucesos. Finalmente, el resultado de este trabajo es una guía básica para la gestión del riesgo de información en unidades especializadas en el tema.

Palabras clave: riesgos de información, gobernanza de información, matriz de riesgos, metodologías de riesgos, información.

Abstract

The present degree work aims to present an information risk management analysis, based on an information governance model, applied in the case of the National Center for Historical Memory; where the concept of information is defined and developed, based on its evolution over time and the cycles that these data have, likewise, the importance of information in organizations is contextualized and in turn the implementation of a governance model of information, giving an analytical look at risk management.

For this purpose, tools are presented that cover the concept of information in risk management, which are identified through the analysis of different methodologies and standards, in this way the information risks can be mapped taking into account the data collected through an interview and an inventory of information.

When carrying out this risk analysis, the risks were established in a matrix with their factors, events, causes and consequences, this with assessment scales and the projection of controls to mitigate the materialization of these events. Finally, this work has as a product a basic guide for the management of information risk in units specialized in this subject.

Keywords: information risks, information governance, risk matrix, risk methodologies, information.

Introducción

La gestión de riesgos en las diferentes organizaciones ha venido ganando protagonismo a través de los años, debido a factores como los sistemas de calidad, los entes reguladores, las normativas que aplican al core de las entidades nacionales e internacionales, los estándares de buenas prácticas, etc. Así, se han establecido marcos generales, principios básicos y lineamientos para la gestión de riesgos de todo tipo. En la actualidad, la información es uno de los objetos intangibles a los que se asigna un valor estratégico, ya que por medio de sus flujos se puede identificar la creación de contenido propio y la recepción de información, así como los procesos para la gestión de la información y su finalidad, bien sea concebida como gestión de conocimiento para toda la organización o como un producto para un público objetivo o una entidad externa.

El análisis de riesgo de información se abordará desde un marco de gobernanza de información, a través del caso de estudio del CNMH. Las variables de análisis para la identificación de los posibles riesgos son la captura, el procesamiento, las entradas, las salidas, la confidencialidad, la integridad y la disponibilidad de la información, desde el enfoque de la ciencia de la información, el análisis de la información y la importancia de salvaguardar y conservar la información en un contexto organizacional.

La investigación parte de la problemática del conocimiento de la información que manejan las unidades de información, cómo se mueven los datos y los medios donde se almacenan, y cómo esto se debe controlar por medio de la gestión de riesgos, para dar como resultado una gobernanza de la información que sirva de fuente para la toma de decisiones.

Planteamiento del problema

Protágoras, el gran sofista griego, postulaba un hecho esencial para la vida de la sociedad: es el ser humano el que le pone nombre a las cosas (también el que las mide). En relación con la construcción de términos, sus definiciones y conceptualización, esto depende y es para la sociedad un constructo social a partir del grado de argumentos que sustentan una realidad o acción y sus intereses (culturales, políticos, económicos, entre otros). Un ejemplo de ello obedece a lo que actualmente se ha denominado *gobernanza de información*, problemática sobre la cual gira el presente estudio.

Paternina (2018) hace referencia a la posible alteración de la evidencia debido a errores metodológicos en el procedimiento empleado para su obtención y resguardo. La flexibilidad de la evidencia digital y su facilidad para ser duplicada y modificable es lo que la hace vulnerable a perder su valor probatorio. Esto garantiza que no existan suplantaciones, modificaciones, alteraciones, adulteración o destrucción de los indicios materiales relacionados con un hecho delictivo.

A partir de un conocimiento exacto, la gobernanza de información se analiza en la nueva era de lo análogo y lo digital, con el propósito de conocer cómo se mueven los datos y la información en los diferentes medios y contextos actuales, generando inquietudes frente a la manera en que las organizaciones manejan sus flujos de información, y cómo esto contribuye a la toma de decisiones y su proyección en el futuro en el ámbito organizacional.

La gobernanza de la información puede definirse como un plan de administración de la información para controlar, valorar, capturar, almacenar, usar, archivar y eliminar la información,

que se basa en la construcción del conocimiento en los procesos y toma como referentes los estándares y lineamientos en el tema, con el fin de garantizar el uso eficaz y eficiente de la información (García-Morales, 2012). Gracias a esto, las organizaciones pueden tomar decisiones fundamentadas en indicadores de gestión de la información, riesgos de información, cumplimento de normativas o estándares transversales a la organización (ISO 31000; ISO 22301; MinTIC, 2019).

Al momento de implementar un gobierno de información, muchas organizaciones ignoran si su información es análoga, digital o electrónica, o si esta fluye por medio de entradas y salidas. Esto se convierte en un riesgo para las organizaciones, las cuales deben gestionar sus metodologías de riesgo corporativo, pues no hacerlo puede implicar daños económicos, reputacionales, procedimentales, fugas de información parcial o total y, finalmente, problemas de gestión de conocimiento. Muestra de ello son los casos de Canon, Ransomware y la página oficial de la Presidencia de Colombia en 2020 y 2021, donde se evidenció el robo de información con datos personales y documentos catalogados como privados, lo que generó pérdida intelectual y daño reputacional por no tener control sobre su información. De igual manera, la Dijín de la Policía Nacional de Colombia reportó desde su Centro de Ciberdelincuencia un total de 5.051 casos de robo de información para el año 2020 (Policía Nacional, 2020). Al respecto, Temesio (2019) afirma:

> El problema que se plantea en cualquier organización y en particular en instituciones de gobierno es que la información está dispersa en diversos formatos y medios, en variedad de dispositivos, los contenidos son de diverso tipo (texto, imagen, información geográfica), no es estática, sino que se encuentra adosada a procesos y actividades y va

> sufriendo transformaciones a lo largo de estos trayectos. Existe también información tácita que está en las personas o en aplicaciones tanto técnicas como administrativas. El resultado es una gran dispersión informacional. (p. 34)

Lo anterior muestra que la gobernanza de información es una fuente de proyección y avance corporativo para las organizaciones, ya que el éxito y crecimiento de una entidad es proporcional al aumento de la información. Por esa razón, el modelo de gobernanza de información debe estar atado a la metodología de análisis de riesgos de la corporación.

Soler-Gonzalez, Varela-Lorenzo, Oñate-Andino y Naranjo-Silva (2018) definen el riesgo como

> [...] una posible pérdida producida por eventos peligrosos e inciertos ligados a vulnerabilidades existentes. Pueden ser considerados escenarios con posibilidad de pérdida, es la probabilidad que un peligro ocasione un incidente con consecuencias no factibles de ser estimadas en una actividad determinada durante un periodo definido, es el potencial de pérdidas que existe asociado a una operación productiva, cuando cambian en forma no planeada las condiciones antes definidas. (p. 54)

En ese sentido, los riesgos se analizan desde la probabilidad de ocurrencia de materialización del evento tomando como fuente la causa y su efecto, que puede ser parcial o total. En el contexto de la información, un evento puede ser, por ejemplo, la pérdida de información en la captura o la pérdida parcial del documento. Según la usabilidad de los datos, los procesos que interactúan con la información y la ubicación organizacional de los datos, se podrá clasificar el riesgo, aplicar el control y determinar el riesgo residual. Todo este proceso debe ser plasmado y documentado en una herramienta llamada *matriz de riesgos*.

Dentro de sus fases, el gobierno de información contempla el diseño de la planeación estratégica, en la cual debe estar el inventario y clasificación de información, los sistemas de información utilizados en la organización, los mapas del flujo de la información donde se identifiquen entradas, proceso y salidas, y demás herramientas que ayudan a la gestión de información desde la gobernanza. Soler-Gonzalez et. al (2018) enfatizan que la planeación debe tener las siguientes características:

> Todas las empresas necesitan de una planeación estratégica para definir los rumbos futuros de la organización […]. Una planeación estratégica no es un ejercicio fortuito y causal, es un ejercicio recurrente del día a día. (p. 59)

En la actualidad, en Colombia las organizaciones están implementando modelos de gobierno de información –también denominado gobierno de datos–, con el fin de gestionar la información de sus organizaciones, mediante documentación que permita establecer directrices para las fases del modelo. Cabe mencionar la *Política de gobierno de datos* del Instituto Distrital de Gestión de Riesgos y Cambio Climático (Idiger, 2018), cuyo objetivo es:

> Aportar en el desarrollo de Gobierno de Datos como parte del Gobierno de TI dentro de la entidad, generando herramientas para la verificación, control y mejoramiento de la calidad de los datos. Esta política establece los mecanismos para lograr que los datos relacionados con los procedimientos de la entidad eleven su nivel de calidad. (p. 1)

Por su parte, las *Políticas de gestión de la información geocientífica* del Servicio Geológico Colombiano (2017) tienen el propósito de:

> Establecer las políticas de la información geocientífica del Servicio Geológico Colombiano (SGC) para entregar a los actores interesados productos que son generados mediante la investigación y gestión integral del conocimiento geocientífico a través de la planeación, adquisición, recibo, generación, administración, depuración, archivo, conservación, uso y difusión de servicios para contribuir al desarrollo económico y social del país. (p. 3)

Así pues, cada entidad estipula el objetivo de su gobierno de información según sus políticas organizacionales, las herramientas para el desarrollo del modelo y el alcance organizacional, con el fin de tomar decisiones estratégicas en periodos de corto, mediano y largo plazo. Esto abre otra arista de la gobernanza como lo es la continuidad del negocio, que enmarca planes de contingencia frente a diferentes eventualidades, resiliencia empresarial e innovación y sostenibilidad.

Recientemente, la sociedad tuvo un cambio drástico con la pandemia causada por el covid-19, que obligó a trasladar el trabajo de oficina a la casa. Esto evidenció las falencias de las corporaciones colombianas, pues en su mayoría no contaban con planes de continuidad, lo que generó pérdidas e incluso el cierre de muchas de ellas. El Departamento Administrativo Nacional de Estadística (DANE) registró la liquidación de 509.370 micronegocios de enero a octubre de 2020, y en consecuencia aumentó el índice de desempleo (*Portafolio*, 2021).

Sumado a esto, las organizaciones debieron alinear la gobernanza con la continuidad para proteger su bien intangible más preciado: la información. Bautista (2014) define la continuidad del negocio como “un proceso interactivo que es diseñado para identificar los procesos de misión crítica del negocio y desarrollar políticas, planes y procedimientos para asegurar la continuidad de estos procesos en el caso de un evento imprevisto” (p. 201).

Según lo anterior, la planeación de simulación de eventos críticos hace la diferencia entre continuar con las operaciones que inicialmente generan un impacto, y su control y estabilización al cien por ciento en la operación original, siguiendo el plan de continuidad, con el apoyo de los procesos y la alta gerencia de la organización, lo que fortalece la cultura organizacional y la resiliencia de la corporación.

Frente a la gestión de la información y del conocimiento se traza una línea transversal cuya última fase es el gobierno de información. En este se refleja precisamente el fortalecimiento de la cultura organizacional, por medio de la creación de conocimiento, con miras a mejorar los procesos y la calidad de sus colaboradores. Así lo explica Aja (2002):

> Las organizaciones basadas en el aprendizaje soportan su desarrollo en la gestión de información, son por excelencia organizaciones de conocimiento, que aprenden con sentimientos de pertenencia, de colectivo, que perfeccionan su cultura como organización, independientemente de su ejecutividad, competitividad y ganancia, que se regeneran a sí mismas mediante la creación de conocimientos, a partir de un aprendizaje a nivel de sistema. En la gestión del conocimiento existen factores comunes, imprescindibles para la supervivencia y el progreso de cualquier organización, entre los cuales se identifican la innovación, la capacidad de respuesta, la productividad y la competencia. (p. 3)

Así pues, teniendo en cuenta que la información es el activo más importante para una organización, ignorar sus volúmenes la pone en situaciones de riesgo que pueden generar pérdidas en diferentes aspectos. En ese sentido, es imprescindible generar y construir conocimiento basado en hechos de la organización, como un factor fundamental para la toma de decisiones que aportan a la

continuidad del negocio. De esta manera se evitará darle prevalencia a una problemática que afecta en la actualidad a varias corporaciones.

Dicho esto, un análisis de gestión de riesgos y continuidad de negocio basado en el modelo de gobierno de información conlleva el siguiente interrogante: ¿Cómo garantizar una buena toma de decisiones desde la administración de los riesgos informacionales bajo el modelo de gobierno de información?

Justificación

En la era actual de la información, mediada por tecnologías de la información y las comunicaciones (TIC), los datos viajan a través de diferentes medios y diversos formatos. Por eso, desde la Ciencia de la Información, Bibliotecología y Archivística se abordan problemáticas como la gestión de la información y sus flujos. Rivero, Díaz, López-Huertas y Rodriguez definen la gestión de la información desde dos aspectos: el "sintáctico de la información", el cual analiza los flujos de la información bajo una muestra de volumen de información, teniendo en cuenta su formato, almacenamiento y medio de repositorio, y el "semántico de la información", donde se genera el conocimiento como fuente intelectual de una organización y se analiza su interacción en los sistemas de información.

Según lo anterior, las organizaciones pueden identificar la información que poseen, sus características y cómo esta interactúa en todos sus procesos organizacionales. Para ello se hace indispensable plantear la solución de gestionar y analizar los riesgos de información, teniendo en cuenta un modelo de gobierno de información que responda con una mirada global hacia y desde la entidad, cuyo resultado sea el control total de su información y cuyo producto final sean los lineamientos en los que se apoyen los procesos estratégicos para la toma de decisiones, y a su vez se mitigue la pérdida de información en tanto fuente principal del conocimiento intelectual de la organización. Por esta razón se toman como referentes las entradas, los procesos, las salidas y los flujos de información de cada uno de los procesos que componen el entorno corporativo.

Desde siempre, la sociedad ha experimentado un crecimiento exponencial de la información debido a las necesidades informacionales que demanda cada individuo. Por eso, las investigaciones de mercado y el análisis de dichas necesidades van gestionando información que pueda satisfacer

esta incertidumbre informacional, con el fin de reducir su entropía. Es así como la gobernanza de información, a través de lineamientos, permite apoyar la gestión y administración de la información que gestionan las entidades de manera análoga, digital y electrónica, mediante la identificación de riesgos de información y con miras a su protección, conservación y preservación a largo plazo.

El presente trabajo de grado toma como objeto de estudio el Centro Nacional de Memoria Histórica (CNMH) para examinar su modelo de gobernanza de información, con el propósito de generar conciencia al interior de sus direcciones sobre temáticas relacionadas con la gestión del riesgo de información, según lo establecido en la política pública de archivos vinculados a las graves y manifiestas violaciones a los derechos humanos e infracciones al derecho internacional humanitario ocurridas con ocasión del conflicto armado interno. Para ello se identifican los flujos de información que genera cada una de las direcciones y su interacción en las entradas, procesos y salidas, haciendo un análisis de los riesgos de la información, para obtener finalmente un complemento al plan estratégico de continuidad para la entidad como recurso estratégico de toma de decisiones.

Objetivo general

Diseñar una metodología de análisis de riesgos de información con base en un modelo de gobernanza de información para el Centro Nacional de Memoria de Histórica, cuyo fin sea crear una cultura organizacional frente al buen manejo de la información, como fuente principal para la toma de decisiones.

Objetivos específicos

- Identificar los flujos de información al interior de las cinco direcciones con las que cuenta el Centro Nacional de Memoria Histórica.
- Comparar las metodologías de riesgos con base en modelos de gobierno de información.
- Realizar una matriz de riesgos de información que permita establecer criterios para la identificación de riesgos en la cadena de custodia de información.
- Diseñar una guía que permita adaptar la metodología de análisis de riesgo en el marco de la gobernanza de información, aplicable a las direcciones del CNMH.

Marco teórico

La información como medio del conocimiento

La producción y consumo de la información es directamente proporcional al contexto, el autor y el emisor, ya que el análisis de los datos pasados a conocimientos que se interpretan son un constructo de investigaciones sobre un tema, donde se toma como base las problemáticas del contexto, para gestionar el conocimiento por medio de la recolección de la información y generar así nuevos conocimientos. Con respecto a la comunicación, la información tiene dos puntos de vista: el contextual, que expresa el conocimiento de forma verbal y no verbal para el receptor, por medio de gráficos y locuciones orales y escritas, y el analítico, donde a partir de estas fuentes se construyen nuevos productos informativos basados en el conocimiento de un profesional y la interpretación de información anteriormente procesada. De la misma manera se crean productos informacionales que se transforman en cultura, donde el receptor es capaz de interpretar los significados de otra comunidad para establecer relaciones comunicativas con esa nueva sociedad.

La información desde la ciencia, el arte y la cultura

En cuanto a la investigación científica, la información comprende conocimientos *teóricos* y *prácticos* que varían según el área de estudio donde se realice la indagación de un tema en concreto. Estos dos componentes son requisitos inamovibles, ya que constituyen las herramientas, los conceptos y los argumentos del autor.

La ciencia moderna habla de un *paradigma dominante* para hacer referencia a la introducción del método, mientras que el posmodernismo surge a raíz de la necesidad de los individuos, las organizaciones y la sociedad de elaborar nuevos conocimientos:

> Las ciencias se han caracterizado por una competencia continua entre una serie de concepciones distintas de la naturaleza, cada una de las cuales se derivan parcialmente de la observación y del método científicos y hasta cierto punto, todas eran compatibles con ellos. (Kuhn, 1995, p. 25)

Frente al camino de la información, cabe resaltar que este se construye bajo una realidad, un contexto y una necesidad de conocer e interpretar lo que nos rodea. El hombre siempre ha buscado explicar lo que observa y, a través del tiempo, se han establecido modelos concretos de investigación con un conjunto de reglas y normas para la práctica científica. Así han evolucionado los datos, convertidos primero en información y luego transformados en conocimiento. Para Kuhn (1995, p. 35), "el paradigma compartido es una unidad fundamental para el desarrollo científico [y] la ciencia normal es un concepto asociado al paradigma, que como un tipo esotérico de investigación permite un signo de madurez". En otras palabras, la información es un ciclo cuyo producto final es el conocimiento.

De otra parte, la información llevada a la gestión del conocimiento se establece desde los creadores de conocimiento llamados investigadores y sus objetos de estudio, ya sean complejos o no complejos, abordados desde diversas disciplinas, lo cual la hace acreedora de un acervo amplio, con un objetivo principal: la solución de problemáticas en todas las áreas del conocimiento. Allí, la lingüística es una herramienta fundamental para el análisis de documentos que poseen un lenguaje específico, que permite interpretar el contenido de un documento. Asimismo, la semiótica identifica, por medio de los signos (signo = significante y significado), las características de un texto para su representación hasta llegar al receptor. "Los libros de texto mismos tienen como meta

el comunicar vocabulario y la sintaxis de un lenguaje científico contemporáneo" (Kuhn, 1995, p. 213).

En la producción de información hay una relación intrínseca autor/emisor, puesto que se construye conocimiento mediante la interpretación personal del emisor. En ese sentido, la información es esencial en la producción de conocimiento, ya que representa un todo de un área de estudio en particular. Así, el consumo y producción de la información están ligados a la necesidad de conocimiento por parte de comunidades de investigación, y la recuperación de información es primordial en el momento de una consulta, para lo cual se han creado sistemas de clasificación decimales, tesauros, terminologías y ontologías.

Cuando la información es codificada a conocimiento puede ser visualizada en diferentes formatos. En el arte, por lo general, se habla de comunicación no verbal, puesto que una época, una ideología o un pensamiento se representan por medio de pinturas, imágenes, dibujos, gráficos, etc., a través de un contexto. Del mismo modo en que se sintoniza la información para la transmisión de cultura, así mismo el individuo entra en contexto con una nueva sociedad cultural, donde el ejercicio de comunicación será más acertado. De esta forma, la ciencia de la información como área del conocimiento, por medio de la transmisión de información y conocimiento, se encarga de conservar la cultura en las sociedades.

Martínez (2012) define la *información* como "un dato que ha sido transformado de manera significativa. […] la información es un conjunto de datos que permite su uso mediante la comunicación; la esencia de ella es que el significado se ha agregado a los datos brutos" (p. 6).

Según esto, la información tiene la cualidad de poseer significado, es decir, transfiere una idea cuya finalidad es generar conocimiento y, de esa forma, responder inquietudes personales y colectivas luego de ser utilizada, organizada y sistematizada (Zhang y Benjamin, 2007, citados por Martínez, 2012). Es por esto que la información se piensa como aquellos recursos creados con la intención de ser analizados y generar un efecto en un público objetivo.

Los datos le permiten al ser humano tomar decisiones y emprender acciones, pues gracias a la información verídica las personas pueden mantenerse enteradas de manera clara, precisa y objetiva, lo que les ayuda a comprender la magnitud de determinado problema sin caer en pánico o en irresponsabilidades, debido al desconocimiento o al amarillismo presentes en la desinformación. Al respecto, Ponjuán y Torres (2020) plantean:

> La información, como dato significativo, necesita tener significado para las personas que acceden a ella. Sin este significado se puede decir que no es información. Por tanto, la información tiene una gran influencia en las personas y conlleva un impacto ético, reconocido durante décadas, y al cual se han referido varios autores. (p. 4)

La información como un ciclo

En la actualidad, la información se mueve en todas partes, está almacenada en diferentes formatos como bases de datos, documentos análogos, digitales y electrónicos, redes sociales y sistemas de información, entre otros. Ello evidencia su crecimiento, fluctuación y rápido avance, con factores como el aumento de la población y sus necesidades informacionales, el crecimiento empresarial, la gestión del conocimiento y la investigación científica. Es por esto que las organizaciones toman cada vez más conciencia sobre el manejo de su información, y se están preocupando por identificar

sus ciclos de información y cómo estos flujos interactúan en sus procesos internos y externos, con el fin de mapearlos en su gestión documental, teniendo en cuenta su clasificación, uso, control, almacenamiento y disponibilidad. García-Morales muestra un claro ejemplo desde su caso de análisis frente a la estrategia de control de la información y habla de

> [...] la gestión del almacenamiento de grandes masas de datos con la finalidad última de ahorro de costes y sin considerar las actividades de disposición y conservación. La puesta en práctica de esta estrategia requiere la definición de una política, el análisis y clasificación de los datos, la determinación de su ciclo de vida en función de las necesidades de uso y disponibilidad por parte de la empresa, y el control sobre la información almacenada. (p. 99)

Vale decir, entonces, que la información siempre será un insumo con el cual se gestionan riesgos y se da alcance a normativas y estándares que apliquen en la organización y su gestión del conocimiento para el crecimiento mismo de la entidad. A continuación, la figura 1 presenta un ciclo propuesto para la información audiovisual, que también puede ser replicable en nuestro análisis:

Figura 1. Ciclo de vida de la información audiovisual

Fuente: elaboración propia.

Tener seguridad en la información es el objetivo del siglo XXI

En una era donde la información está expuesta a través de diferentes medios, asegurar la información es uno de los factores que todas las organizaciones están contemplando, mediante la implementación de medidas para salvaguardar la información desde su integridad hasta su medio almacenamiento. Por esa razón, la información se convirtió en un activo de prioridad en las organizaciones, pues como explican Martelo, Madera y Betín (2015),

> [...] cuando es completa, precisa y actualizada es fundamental en la toma de decisiones de las mismas. La importancia de la información se fundamenta en la teoría de la organización, la cual se define como un sistema conformado por personas, recursos materiales e información. (p. 130)

La información se asegura en primera medida desde su integridad, es decir que desde la creación de los datos hasta el transcurso de su gestión estos deben mantener su originalidad, evitando y controlando la pérdida de información. Como segunda medida deben asegurarse los medios de almacenamiento, como archivos para la información análoga, sistemas de información y servidores para la información en la nube. Para ello es necesario que la organización diseñe un plan de seguridad con estas dos medidas, basado en estándares y normas que contribuyan a fundar lineamientos según sus necesidades:

> Los Sistemas de Gestión de la Seguridad de la Información bajo los requerimientos que exige la norma ISO 27001 constituyen la base para la gestión de la seguridad de la información; dicha norma define un SGSI que garantiza el conocimiento, apropiación, gestión y disminución de riesgos de seguridad de la información para la organización, de forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a cambios que se produzcan en los riesgos, entorno y tecnologías. (Martelo, Madera y Betín, 2015, p. 130)

Cubrir esos dos factores (integridad y almacenamiento) es el primer insumo para identificar los riesgos desde el aseguramiento de la información, los cuales son llevados a la matriz de riesgos correspondiente para determinar los controles aplicables a cada uno de ellos.

Un enfoque hacia el entendimiento de las organizaciones

Idalberto Chiavenato (2009) sugiere autores clásicos para definir y dividir una organización, como segmentación del trabajo, especialización, jerarquía, autoridad, responsabilidad, coordinación, etc. Esta se compone de niveles jerárquicos o funcionales establecidos por el organigrama, cuyo interés se concentra en funciones y tareas.

De acuerdo a la estructura y gestión de los procesos de trabajo, tanto específicos como generales, dentro de las organizaciones es importante definir los horarios y diseñar los puestos y los cargos de los empleos, con el objetivo de aclarar las funciones de cada persona y la intención de actuar de una manera coordinada para conseguir su propósito.

> La vida de las personas está conformada por una infinidad de interacciones con otras personas y con organizaciones. El ser humano es eminentemente social e interactivo; no vive aislado sino en convivencia y en relación constante con sus semejantes. Debido a sus limitaciones individuales, los seres humanos se ven obligados a cooperar unos con otros, formando organizaciones para lograr ciertos objetivos que la acción individual, aislada, no podría alcanzar. Una organización es un sistema de actividades conscientemente coordinadas de dos o más personas. La cooperación entre estas personas es esencial para la existencia de la organización. (Chester, 1971, citado en Chiavenato, 2009, p. 6)

Según Chiavenato, una organización existe solo cuando:

1. Hay personas capaces de comunicarse.

2. Las personas están dispuestas a contribuir en una acción conjunta.

3. Las personas trabajan por alcanzar un objetivo común.

Por otro lado, tanto las entidades como las organizaciones funcionan a través de una serie de normas que han sido fijadas previamente para el cumplimiento de los objetivos; por esto, es necesario que dentro de las entidades haya una comunicación ordenada que permita lograr la finalidad propuesta en la organización.

Qué tan complejas son las organizaciones

> Las organizaciones se diferencian de los grupos y de las sociedades por su complejidad estructural, la cual se refiere a la existencia de distintos niveles horizontales y verticales dentro de ella. A medida que hay división del trabajo, aumenta la complejidad horizontal de la organización conforme surgen nuevos niveles jerárquicos para un mejor control y regulación, aumenta la complejidad vertical. Así, muchos autores se refieren a organizaciones altas (con muchos niveles jerárquicos) y organizaciones planas (con pocos niveles jerárquicos). (Kenneth, 1968, citado en Chiavenato, p. 6)

Es bien sabido que las entidades deben colaborarles a sus empleados con el fin de asegurar el cumplimiento de las metas organizacionales y minimizar su deserción, con lo cual se mantendrá un ambiente laboral sano. Para Chiavenato (2009), los principios organizacionales son:

Anonimato: se da importancia a las tareas y operaciones, no a las personas. Lo que importa es que la operación sea realizada, sin importar quién la realice.

Rutinas estandarizadas para procedimientos y canales de comunicación: a pesar del ambiente laboral impersonal, las organizaciones tienden a formar grupos informales personalizados dentro de ellas.

Estructuras personalizadas no oficiales: constituyen la organización informal, que funciona paralelamente a la estructura formal.

Tendencia a la especialización y a la diversificación de funciones: tiende a separar las líneas de autoridad formal de aquellas de competencia profesional o técnica.

Tamaño: es un elemento final e intrínseco de las grandes organizaciones, ya que resulta del número de participantes y de las áreas que forman su estructura organizacional

Vale aclarar, no obstante, que las organizaciones sufren cambios y transformaciones progresivamente, ya sea con la introducción de tecnologías nuevas o diferentes, modificando sus productos o servicios, con la alteración del comportamiento de las personas o el cambio de sus procesos internos.

En la actualidad, las organizaciones se componen de sistemas complejos, debido a las diferentes tareas humanas: la manera como las personas se alimentan, viven, compran, trabajan, se visten, sus expectativas y convicciones es la base fundamental para conocer quiénes conforman la organización.

El mundo evoluciona y las organizaciones también

Actualmente hay diferentes tipos de organizaciones que están enfocadas en distintos tipos de productos. Entre ellas existen las pequeñas y medianas empresas y las grandes empresas y las

multinacionales, cada una de las cuales ofrecen y brindan al mercado variedad y servicios, debido a la manera de pensar, sentir y reaccionar de las personas.

Entre los siglos XX y XXI, las organizaciones pasaron por tres transiciones diferentes: la era de la industrialización clásica, la era de la industrialización neoclásica y la era de la información

● **Era de la industrialización clásica:** inició con la Revolución Industrial, cuyo periodo se identifica por el formato piramidal y centralizador, la departamentalización funcional, el modelo burocrático, la centralización de las decisiones en la alta dirección, el establecimiento de reglas y regulaciones internas para disciplinar y estandarizar el comportamiento de los integrantes. Las personas eran consideradas recursos de producción, junto con otros recursos organizacionales como las máquinas, el equipo y el capital; dentro del plan organizacional existían tres factores tradicionales de producción: naturaleza, capital y trabajo. Todo estaba al servicio de la tecnología. El hombre era considerado un apéndice de la máquina (Drucker, 1995, citado en Chiavenato, 2009).

● **Era de la industrialización neoclásica:** inicia a finales de la Segunda Guerra Mundial. El mundo empezó a cambiar rápidamente; los cambios se hicieron más rápidos e intensos y poco previsibles. La velocidad de cambio aumentó. Las transacciones comerciales pasaron de locales a regionales, de regionales a internacionales y se volvieron gradualmente más complejas. El antiguo modelo burocrático y funcional, centralizador y piramidal, utilizado para dar forma a las estructuras organizacionales, resultó lento y demasiado rígido frente a los movimientos que se producían en el ambiente. Las organizaciones probaron nuevos modelos de estructura que les proporcionaran mayor innovación y mejor adaptación a las nuevas situaciones. Surgió la

organización matricial para tratar de adaptar y revivir la vieja y tradicional organización funcional (Drucker, 1993, citado en Chiavenato, 2009).

● **Era de la información:** comienza alrededor de 1990 y es la época actual. Su característica principal son cambios rápidos, imprevisibles e inesperados. Drucker (1993, citado en Chiavenato, 2009) previó esa poderosa transformación mundial. La tecnología produjo desarrollos por completo imprevistos y transformó el mundo en una aldea global. La información logró recorrer el planeta en milésimas de segundo. La tecnología de la información provocó el surgimiento de la globalización de la economía: la economía internacional se transformó en economía mundial y global. La competitividad entre las organizaciones se hizo más intensa. El mercado de capitales pudo emigrar en cuestión de segundos de un continente a otro en forma volátil, en busca de nuevas oportunidades de inversión, aunque transitorias (Drucker, 1993, citado en Chiavenato, 2009).

Las organizaciones como sistemas abiertos

Miller y Rice(1957, citado en Chiavenato, 2009) definen las organizaciones como un

> [...] sistema abierto, con características comunes a un organismo biológico. Un sistema abierto existe, y solo puede existir, mediante el intercambio de materiales con su ambiente. Importa materiales, los transforma por medio de procesos de conversión, consume parte de los productos de conversión para su mantenimiento interno y exporta el resto. Directa o indirectamente, intercambia sus resultados (salidas) para obtener nuevos insumos (entradas), con la inclusión de recursos adicionales para poder mantenerse. Estos procesos de importación, conversión y exportación constituyen el trabajo que la empresa tiene que hacer para vivir. (p. 13)

En relación con lo anterior, en el futuro se identificarán, se cultivarán y explorarán las competencias esenciales que hagan posible el crecimiento en una organización. Por lo tanto, un sistema está compuesto por cuatro elementos esenciales:

a. Entradas o insumos: todo sistema recibe insumos provenientes del ambiente externo, a través de las entradas.

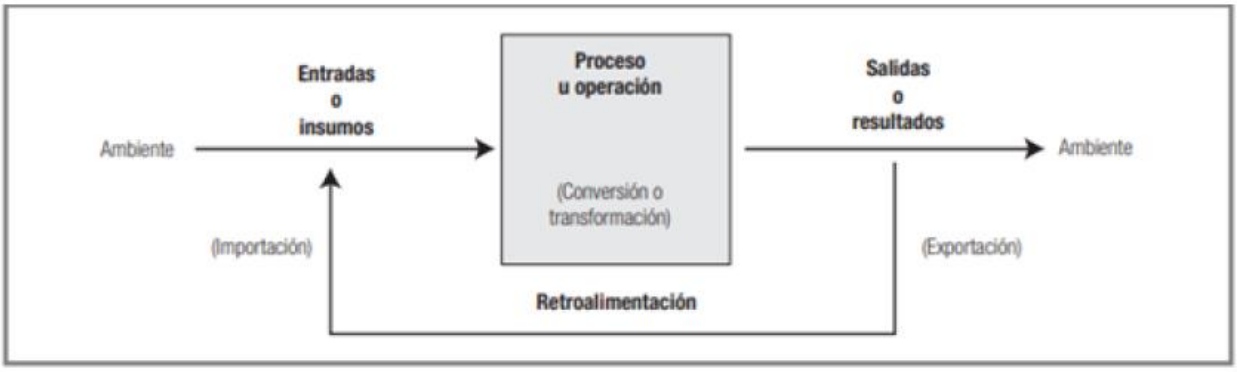
b. Proceso u operación: es el núcleo del sistema en el que las entradas son procesadas o transformadas.

c. Salidas o resultados: es el resultado de la operación del sistema, que se realiza cuando se envía de nuevo el producto de su operación.

d. Retroalimentación: es una acción que clasifica tanto lo positivo como lo negativo dentro de una organización, la cual debe ser inherente a cada unidad de información.

Es necesario recalcar que todo sistema opera en un ambiente y este facilita resultados, los cuales manifiestan conformidad o inconformidad, dependiendo de su entorno y su experiencia en la organización. La figura 2 muestra los anteriores elementos:

Figura 2. Elementos de un sistema



Fuente: *El sistema y sus cuatro elementos esenciales*.

● Los participantes de las organizaciones

Las organizaciones existen gracias a sus colaboradores, que mantienen los objetivos trazados desde el inicio de la organización, mediante una actividad organizada que permite el crecimiento y desarrollo de cada empleado, a través de su formación y capacitación.

En la actualidad, los socios o altos ejecutivos utilizan diferentes métodos ya estructurados y organizados para la toma de decisiones.

Las organizaciones son creadas para lograr objetivos definidos. Esto significa que se construyen de manera planeada y organizada, con el fin de lograr los retos trazados desde el inicio de su creación. Con el propósito de procurar costos bajos y con menor esfuerzo, las entidades buscan mantener una asociación mutua y que sus funcionarios estén sujetos a cambios constantes realizados dentro de las organizaciones, para un bien común.

La gobernanza en el siglo de la información

> La "gobernanza" se utiliza ahora con frecuencia para indicar una nueva manera de gobernar que es diferente del modelo de control jerárquico, un modo más cooperativo en el que los actores estatales y los no estatales participan en redes mixtas público-privadas. La gobernanza se caracteriza por adoptar una perspectiva más cooperativa y consensual que la que se había dado en los modelos tradicionales de gobernar.
>
> La gobernanza está ganando terreno en los últimos años y se está imponiendo a otros sistemas de gobierno como la jerarquía o el mercado, que habían sido ampliamente utilizados anteriormente, aunque ello no significa una superación de los anteriores modos de gobernación, sino una modulación y un reequilibrio. (Meyntz, citado en Cerrillo, 2005, p. 12)

El mundo es hoy en día más complejo, dinámico y diverso, lo que no admite una visión única, sino que requiere de una unión numerosa. Por ello, los sistemas de gobierno tradicionales, basados en la jerarquía y la unilateralidad, no son suficientes, ni siquiera capaces de hacer frente a los problemas, desafíos y retos que surgen.

Por otro lado, la gobernanza significa una nueva forma de gobernar y asociar las instituciones tanto públicas como privadas, las cuales son desafiadas a participar y cooperar en la representación y aplicación de las nuevas políticas dentro de las organizaciones.

Gobernanza como medio de administración de la información

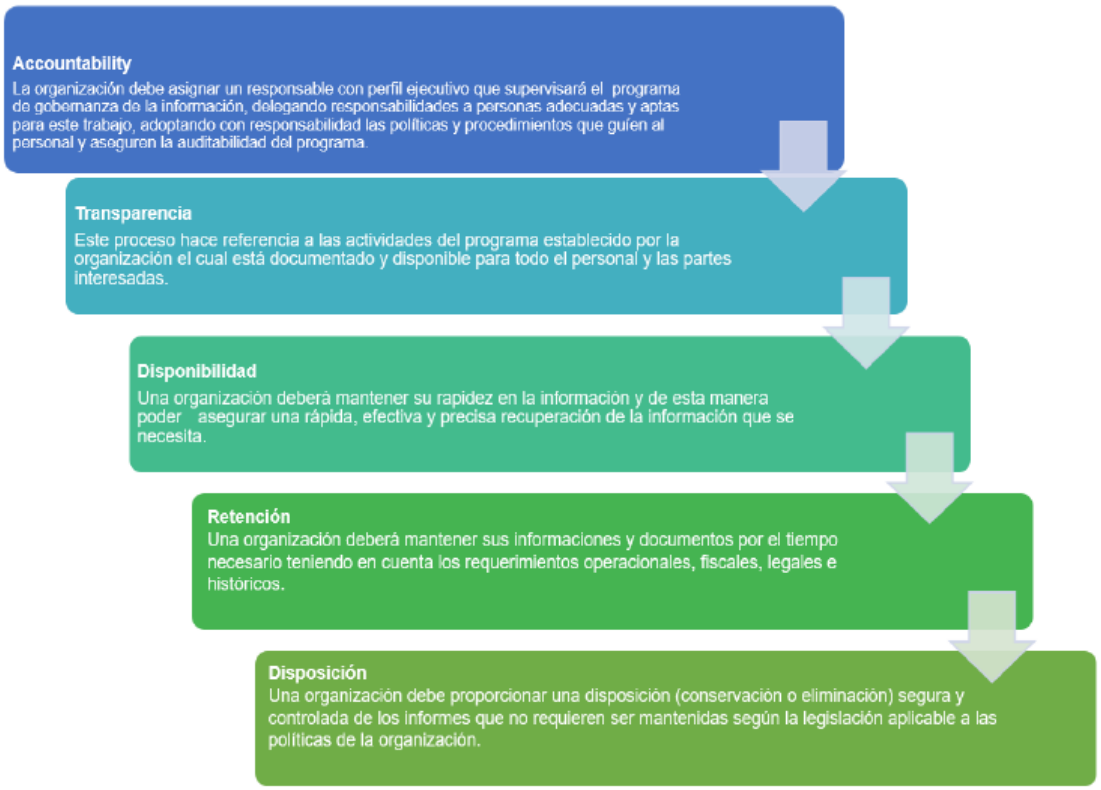
> La gobernanza de la información es dinámica, proactiva y enfocada al negocio mientras que el *records management* es estático, reactivo y enfocado en la retención. (Perrein, 2011, citado en García-Morales, 2012, p. 101)

Elisa García-Morales (2012), especialista en gestión documental, gestión de contenidos y *records management*, define la gobernanza de información como un término que cada día toma más importancia y parece crecer en el ámbito profesional, empresarial y especialmente en el mercado tecnológico. La autora analiza diferentes aproximaciones conceptuales a su significado y desarrollo, justificando su interés ya que facilita posicionar la información en un nivel estratégico, y de esta forma responder a las necesidades reales de establecer reglas y políticas que permitan el uso efectivo de la información dentro de una organización.

La gobernanza de información es un tema que está ganando auge dentro de las organizaciones, y es aquí donde se entra a evaluar e identificar las normas y reglas que rigen, guían y dirigen a las entidades, pues estas buscan estrategias de información en los entornos directivos para el control y la toma de decisiones.

Como ya se ha dicho, las entidades deben proteger la calidad de los procesos de gobernanza de la información y de esta forma asegurar el cumplimiento y minimizar los riesgos. La figura 3 describe los roles y responsabilidades en la gobernanza de la información propuestos por García-Morales (2012):

Figura 3. Organización de roles y responsabilidades en gobernanza de información



Fuente: elaboración propia.

La gobernanza de la información es la especificación de los derechos de decisión y de una estructura de responsabilidades y control, que busca fomentar la cultura deseada para la valoración, captura, almacenamiento, uso, archivo y eliminación de la información. Ello incluye procesos, roles, estándares y medidas que aseguren el uso efectivo y eficiente de la información y que permitan a una organización conseguir sus objetivos de negocio (Cárdenas, Wilches, Peñate & Lozada, 2018).

Es aquí donde las organizaciones implementan programas para el desarrollo de la gobernanza de información, con el objetivo de cumplir con las metas propuestas. Estos modelos ayudan a las

entidades a establecer análisis y prioridades cuya finalidad se establece desde la responsabilidad, las políticas, la integración de personas y de la tecnología hasta el ciclo de vida de la información.

Una mirada analítica en los riesgos del gobierno de información

Los ataques a los sistemas informáticos han aumentado progresivamente en la última década, como resultado de los avances en los servicios y modelos de comunicaciones e información y el *boom* de las nuevas Tecnologías de la Información y la Comunicación (TIC), así como por el uso continuo y generalizado a nivel global de la Internet. Esto ha obligado a las empresas a buscar estrategias que les permitan ejecutar análisis que prevengan, controlen y reduzcan los riesgos asociados a la violación o vulnerabilidad de su información. Entre los elementos que componen cada modelo se encuentran los recursos del sistema de información necesarios para que la organización funcione correctamente y el alcance de los objetivos propuestos, los eventos que pueden desencadenar un incidente que produzca daños en sus activos, la posibilidad de la materialización de una amenaza y sus consecuencias, la posibilidad de que se genere un impacto en los bienes de la organización y, finalmente, los procedimientos que se llevan a cabo para reducir los riesgos (Daltabiut, Hernández, Mallén & Vásquez, 2009). “El análisis de riesgos pretende dar respuesta a tres interrogantes: saber qué se quiere proteger, contra quién y cómo se va a hacer”. (Areitio, 2008).

En este sentido, las organizaciones están expuestas diariamente a amenazas tanto internas como externas, a pérdida de credibilidad y a daños financieros que también pueden afectar la sostenibilidad de la entidad.

Con lo anterior se cuestiona si las organizaciones conocen y aplican metodologías para la búsqueda de peligros inminentes y custodia de los inicios de estabilidad de la información, con el fin de prevenir el hurto de identidad e información, bases de datos, información sensible de funcionarios. El caso de estudio del CNMH expone las razones por las que es importante aplicar dichas metodologías y, finalmente, sugiere recomendaciones que brindan una mejor oportunidad en la toma de decisiones ante un riesgo inminente.

Gestión de riesgos: un enfoque en la información

La gestión de riesgos en las organizaciones se volvió uno de los lineamientos empresariales más importantes, ya que contar con un mapeo de riesgos permite tomar decisiones para el presente y futuro de la empresa. Esta gestión debe aplicarse de conformidad con lo dispuesto en la misión, visión y valores de la organización y teniendo en cuenta su *core* en todos los procesos de la empresa, según los roles y responsabilidades que se definan desde sus objetivos y las normas que les apliquen. Así lo plantean Guerrero-Aguiar, Medina-León & Nogueira-Rivera (2020):

> Gestionar los riesgos, con orientación a procesos, contribuye a una mejor identificación y tratamiento de estos, a tener mayor precisión de las actividades a realizar y a la consecución de los objetivos. Los riesgos están presentes en cualquier tipo de actividad, por simple que sea. A tal efecto, se deben establecer mecanismos de control para su correcta administración. En referencia, la gestión de riesgos se incorpora, como una buena práctica, en la planeación estratégica y es parte de una de las etapas del ciclo de planificación. (p. 2)

Al implementar estas metodologías se garantiza que los riesgos relevantes para la organización sean identificados, analizados, evaluados, controlados y comunicados. Es necesario plantear objetivos para el éxito de esta gestión, más cuando se planifica en pro del control de la información. La gestión de riesgos debe contribuir al mejoramiento continuo y demás propuestas de valor de la organización; fortalecer el buen gobierno; preservar la integridad de los recursos de la entidad (en este caso de la información); incrementar la ventaja competitiva frente a otras unidades; garantizar la sostenibilidad y continuidad de la organización por obtener una visión global de los riesgos de toda naturaleza que afectan el cumplimiento de las propuestas de valor; adoptar la gestión de riesgos como una herramienta de dirección y de administración que permita diseñar estrategias y acciones tendientes a evitar, reducir, transferir o aceptar riesgos, y, por último, fomentar la cultura de la gestión de riesgos como parte del sistema de control interno y del autocontrol.

. Para entender qué significa la gestión de riesgos es necesario analizar los términos de *riesgo*, los *eventos de riesgos* y las *vulnerabilidades* que estos contemplan:

> La definición de un riesgo no es un análisis mecanicista de una situación dada. Un riesgo es una posible pérdida producida por eventos peligrosos e inciertos ligados a vulnerabilidades existentes. Pueden ser considerados escenarios con posibilidad de pérdida, es la probabilidad que un peligro ocasione un incidente con consecuencias no factibles de ser estimadas en una actividad determinada durante un periodo definido, es el potencial de pérdidas que existe asociado a una operación productiva, cuando cambian en forma no planeada las condiciones antes definidas. (Soler-Gonzalez at al, 2018, p. 53)

Una vez se comprenda qué es un riesgo, deben crearse los principios para su gestión , que debe estar orientada a la creación de valor en la organización y demás partes interesadas. De este modo

se establece la autogestión, bajo una mirada interna y externa, a fin de identificar oportunidades y amenazas.

La gestión de riesgos se realizará con base en criterios metodológicos que correspondan a las mejores prácticas reconocidas y aplicables a la entidad, y debe ser permanente, ya que debe hacerse de forma continua y oportuna, buscando la mejor información disponible con la cual se mantienen canales adecuados para su comunicación a nivel interno y externo. Asimismo, la gestión de riesgos debe ser dinámica y receptiva al cambio, para que pueda transformarse de manera oportuna y facilitar la mejora continua de la organización, adaptándose al contexto externo e interno de la empresa. Anualmente debe realizarse un ciclo completo de administración y gestión de riesgos, con lo cual se promueve la cultura de la autogestión del riesgo dentro de la organización.

En la gestión de riesgos es fundamental definir una serie de roles y responsabilidades donde los procesos estratégicos puedan revisar los insumos documentales y el conocimiento que se va creando con esta gestión, para que puedan ser adicionados al plan estratégico y la toma de decisiones, así como a los procesos misionales donde está ubicado el área o proceso de riesgos. Esta área monitorea los riesgos dentro de los límites establecidos; participa en la identificación, cuantificación y reporte de riesgos críticos; propone a los órganos de gerencia o directivas la tolerancia y capacidad del riesgo; plantea acciones sobre los riesgos; define los facilitadores que harán el control interno para generar las acciones de mejora y los demás procesos para el cumplimento de la metodología que se establezca, y formula políticas, procedimientos y demás insumos producidos para la ejecución, cumplimento y divulgación de la gestión de riesgos (figura 4).

Figura 4. Organización de roles y responsabilidades para la gestión de riesgos

Fuente: elaboración propia.

Así pues, se requiere crear una metodología de riesgo que se adapte a las necesidades de la organización, estipulando las variables que se deseen medir y las normas o estándares que se quieran incorporar. Soler-Gonzalez et al. (2018) proponen unas variables basadas en un estándar general de riesgos:

> Para el desarrollo de la gestión de riesgos son necesarias diferentes herramientas que propicien la medición. La norma ISO 3010 recomienda las técnicas de apreciación de acuerdo a la etapa que se desarrolle. Para estos procesos de evaluación de riesgos se

> deben determinar los criterios de aceptación para las variables de riesgo que se regulan por las empresas como el impacto, frecuencia, vulnerabilidad y velocidad del evento y otras. (p. 57)

Cada organización puede establecer variables generales para la implementación de una metodología que contribuya con la gestión de riesgos y pueda proyectarse a largo plazo, mediante la identificación y clasificación de los riesgos más importantes y su posible incidencia sobre las propuestas de valor planteadas por la organización, su estructura organizacional, la gestión del conocimiento, la sostenibilidad y el plan de mejoramiento para la entidad en la toma de decisiones. A continuación, se proponen estrategias para la consecución de una adecuada gestión de riesgos:

● Proponer una estructura con políticas y procedimientos que garantice mecanismos de aprobación y cumplimento que permitan una eficaz gestión de riesgos dentro de la cantidad de riesgos de la organización, incluyendo planes de mejora.

● Medir y controlar los riesgos por medio de procedimientos de general aceptación que garanticen su consolidación y monitoreo.

● Adoptar sistemas de información y control interno para una evaluación y comunicación periódica y transparente en todos los procesos de la organización.

● Establecer roles y responsabilidades en cada nivel de la organización para el reporte de eventos que permita mapearlos en la formulación de los riesgos.

● Implementar y administrar el Sistema de Gestión de Riesgos, donde cada proceso pueda gestionar sus riesgos internos.

● Actualizar anualmente las herramientas de gestión de riesgos desde la gestión documental con insumos como matriz, análisis de contexto o sistemas, de la mano de los procesos y el experto encargado.

● Capacitar y socializar las políticas, métodos y procedimientos aplicables a la gestión de riesgos.

Clasificar los riesgos permite agruparlos para poderlos tratar y determinar su volumen, la pertenencia a determinado proceso o si son transversales a la organización. A estos se les asigna un valor, una probabilidad o frecuencia, un impacto o consecuencia, un control y, finalmente, se evalúan. En el ámbito empresarial, los más conocidos son los riesgos financieros debido a la magnitud del sector bancario, pero el contexto de riesgos se ha ampliado a los otros sectores:

> Existen varias clasificaciones de riesgos como son los casos de los riesgos internos o externos que están en función de cómo se analice el impacto o la causa que genera el impacto. Generalmente se analiza en estos casos el riesgo en función de la causa. Existe otra clasificación de los riesgos relacionados al riesgo financiero y al riesgo puro. El riesgo financiero es aquel riesgo en el cual existe la posibilidad de ganar o perder. En cambio, el riesgo puro posibilita no perder, pero nunca ganar. (Soler-Gonzalez et al., 2018, p. 55)

La clasificación, entonces, es acorde con las necesidades de la entidad y sus objetivos desde la propuesta de valor y servicios, siendo esta la fuente cualitativa para redactar el riesgo que aplique a cada evento que se pueda presentar, seguido del análisis cuantitativo, por medio de escalas porcentuales o numéricas y de colorimetría en el valor asignado, probabilidad o frecuencia y el impacto o consecuencia.

Las siguientes son las normativas y estándares comúnmente más utilizados como insumo para la gestión de riesgos. Cabe aclarar que estos se aplican según lo mencionado anteriormente con respecto a las necesidades de la organización:

Internacionales:

● NC ISO 31000:2018, Gestión de riesgos: este documento proporciona directrices para gestionar el riesgo al que se enfrentan las organizaciones, las cuales pueden adaptarse a cualquier empresa y a su contexto para gestionar cualquier tipo de riesgo y no son específicas de una industria o un sector.

● NC ISO 9001, Riesgos asociados a la calidad de los productos y servicios: En organizaciones de ámbito público y privado se puede aplicar esta norma si se desea implantar o mantener un sistema de gestión relacionado con la calidad, independientemente del sector al que pertenezcan, para garantizar a sus usuarios que la calidad de los servicios o productos ofrecidos cuentan con la calidad exigida a nivel internacional.

● NC ISO 14001, Riesgos ambientales: esta norma internacional especifica los requisitos para un sistema de gestión ambiental que una organización puede usar para mejorar su desempeño ambiental, y abarca los efectos potenciales adversos (amenazas) y los efectos potenciales beneficiosos (oportunidades).

● NC ISO 45001, Riesgos de seguridad y salud del trabajo (SST): el objetivo y los resultados previstos del sistema de gestión de la SST es prevenir lesiones y deterioro de la salud relacionados con el trabajo a los trabajadores y proporcionar lugares de trabajo seguros y saludables; en

consecuencia, es de importancia crítica para la organización eliminar los peligros y minimizar los riesgos para la SST, tomando medidas de prevención y protección eficaces.

● NC ISO 22001, Riesgo relacionado con la inocuidad de los alimentos: establece los requisitos para un sistema de gestión de la inocuidad de los alimentos (SGIA) y está dirigida a las organizaciones involucradas directa o indirectamente en la cadena alimentaria.

● NC ISO 27001, Riesgos de seguridad de la información: permite la gestión y control de los riesgos de la seguridad de la información en las organizaciones para las cuales la información y la tecnología son activos importantes de su negocio.

● COSO ERM, Marcos reguladores básicos de riesgo y cumplimiento en temas de control interno: la gestión de riesgos corporativos se debe a que las entidades existen con el fin último de generar valor para sus grupos de interés. Todas se enfrentan a la ausencia de certeza y el reto para su dirección es determinar cuánta incertidumbre se puede aceptar mientras se esfuerzan en incrementar el valor para sus grupos de interés.

Nacionales, de lo cual se desprenden decretos y planes para esta gestión de riesgos:

● Ley 1523 de 2012, Gestión del Riesgo de Desastres y Sistema Nacional de Gestión del Riesgo de Desastres: la gestión del riesgo de desastres es un proceso social orientado a la formulación, ejecución, seguimiento y evaluación de políticas, estrategias, planes, programas, regulaciones, instrumentos, medidas y acciones permanentes para el conocimiento y la reducción del riesgo y para el manejo de desastres, con el propósito explícito de contribuir a la seguridad, el bienestar, la calidad de vida de las personas y al desarrollo sostenible.

Diseño metodológico

De acuerdo con los objetivos y la pregunta de investigación que se plantearon en el presente trabajo de grado, se consideró que el diseño metodológico pertinente para su desarrollo correspondía a una investigación con enfoque cualitativo, basado en un modelo de gobernanza de información para el Centro Nacional de Memoria de Histórica, cuyo fin es crear una cultura organizacional frente al buen manejo de la información

> El momento de aplicar los instrumentos de medición y recolectar los datos representa la oportunidad para el investigador de confrontar el trabajo conceptual y de planeación con los hechos. (Hernández-Sampieri, s. f., p. 1)

De acuerdo con Hernández-Sampieri (s. f.), para un método cualitativo se deben tener en cuenta los siguientes ítems:

a. Enfoque:

Este proyecto tiene un enfoque cualitativo, ya que se analizarán las características y propiedades de la información recolectada, donde

> la investigación cualitativa es un producto resultante de los valores culturales y del investigador, la cual, da respuesta a los intereses individuales y colectivos de los sujetos, con base a sus creencias, vivencias e ideologías, marcando una singular particularidad de este paradigma investigativo. Inclusive, es menos estática en comparación a la cuantitativa, ya que ésta última se rige por un proceso rígido y meticuloso para aceptar o rechazar hipótesis. (Corona & Maldonado, 2018, p. 3)

Lo anterior estará plasmado en la estructuración de la matriz de riesgo de información y el análisis realizado a cada documento en el inventario general.

Así pues, por medio de entrevistas a diferentes colaboradores del CNMH, se obtendrán datos que son tributos de esta información documentada que hace parte de esta reconstrucción de memoria.

Por otra parte, se tomarán como fuentes de datos los flujos de información en las principales direcciones, abordando desde los procesos macro hasta llegar a lo micro, con lo cual podremos entender e identificar el manejo de la información en esta entidad, y evidenciar a su vez la importancia de la información en la organización y cómo puede estar expuesta si no es sometida a un control.

b. Tipo de investigación:

De acuerdo a lo planteado en los objetivos trazados en el presente trabajo para el análisis de gestión de riesgos de información basado en el proceso de gobierno de información para toma de decisiones en el Centro Nacional de Memoria Histórica, esta investigación se plantea a partir de un método cualitativo, cuyos procesos de recolección de datos se harán a través de las entrevistas, el flujograma y la matriz de riesgos.

c. Fases de la investigación:

Fase 1: Identificar los flujos de información		
Descripción: en esta fase se pretende identificar, en las cinco direcciones del CNMH, cómo se maneja la información a nivel interno y externo, estableciendo el tipo de información, las entradas de los datos, los procesos que interactúan con esta información y sus salidas. El insumo será el análisis de gestión de riesgos de información.		
Actividad	**Técnica**	**Producto**

Elaboración de consentimiento manejo de la información y su usabilidad.	No aplica.	Formato de consentimiento manejo de la información y su usabilidad.
Diseño de entrevista para los colaboradores del CNMH.	Entrevista.	Banco de preguntas.
Mapeo de las direcciones que manejan la información y los flujos de la información.	No aplica.	Organigrama de la entidad - Flujograma.
Aplicación de la entrevista.	No aplica.	Video e inventario de respuestas.
Inventario de información de la Dirección de Derechos Humanos.	No aplica.	Cuadro de inventario consolidado.
Fase 2: Análisis de metodologías de riesgos basados en modelos de gobierno de información		
Descripción: para el análisis de gestión de riesgos de información basado en el proceso de gobierno de información para toma de decisiones: caso CNMH, es necesario comparar las diferentes metodologías que se abordaron con anterioridad y con esto crear una que se adapte a la entidad frente a la gestión de riesgos de información y sus variantes, y que a su vez esta pueda ser replicada en este tipo de entidades.		
Actividad	**Técnica**	**Producto**
Comparación de las metodologías.	No aplica.	Cuadro comparativo, con descripción, sector aplicable y normativa.
Diseño de cuestionario para el encargado del proceso.	Encuesta.	Cuestionario de preguntas.
Fase 3: Matriz de riesgos de información		
Descripción: esta herramienta nos permitirá registrar, analizar, evaluar y tratar los riesgos identificados de la información, y con esto la entidad tendrá un insumo para el control de su información, la cual deberá ser actualizada anualmente por el CNMH.		
Actividad	**Técnica**	**Producto**
Homologación del inventario a la matriz.	No aplica.	Cuadro de inventario consolidado.
Diseño de la matriz de riesgos de información.	No aplica.	Matriz de riesgos de información.
Fase 4: Guía para establecer la metodología de análisis de riesgo en el marco de la gobernanza de información		
Descripción: esta guía será utilizada para detallar la ejecución de la metodología, que se hacer necesaria debido a su grado de complejidad o para mayor comprensión. Este documento también se utiliza para describir las variables de la gestión de riesgos de información bajo el marco de gobernanza.		
Actividad	**Técnica**	**Producto**
Diseño de guía.	Tipo instructivo.	Guía metodología de análisis de riesgo en el marco de la gobernanza de información.

Herramientas de recolección de datos

"Un instrumento de recolección de datos es en principio cualquier recurso de que pueda valerse el investigador para acercarse a los fenómenos y extraer de ellos información" (Sabino, 1992, p. 88).

Esta noción aclara que se trata de mecanismos y sistemas para reformular y transmitir los datos de la información obtenida a través de la investigación.

Para el licenciado Hernández-Sampieri (s. f.), se deben tener en cuenta los siguientes puntos para seleccionar las herramientas de recolección de datos:

- Se derivan de los objetivos y preguntas de la investigación.
- Se revisa la literatura y se construye un marco o una perspectiva teórica.
- De las preguntas se establecen hipótesis y determinan variables.
- Se traza un plan para probarlas (diseño).
- Se miden las variables en un determinado contexto.

Siguiendo este planteamiento, una investigación es válida al estar protegida por información verificable, que manifieste lo que se pretende demostrar con la hipótesis formulada. Para ello, es necesario realizar un proceso de recolección de datos en forma planeada y teniendo objetivos claros sobre la información a recoger.

En ese sentido, el enfoque cualitativo de la metodología se seleccionó para la búsqueda de aspectos relevantes al momento de clasificar la información, evaluación y descripción, ya que se encuentra directamente en el contenido.

Como se viene mencionando, se debe crear un diseño para la recolección de información. Para este trabajo se utilizaron las siguientes herramientas: entrevistas, flujogramas, cuadros de inventarios consolidados y matriz de riesgos.

La entrevista

Es una herramienta primordial para este trabajo de grado, que permite recuperar la información y facilita el mapeo de datos exactos.

> Es un método cómodo para obtener datos referentes a la población, facilitados por individuos y que nos sirven para conocer el entorno en el que se encuentra la persona. Estos datos podrían observarse directamente a través de la observación, pero serían subjetivos de los investigadores [...]. La entrevista es el instrumento más importante de la investigación, junto con la construcción del cuestionario. (Torres, Paz & Salazar, s. f., p. 13)

Además, las preguntas presentadas de forma definitiva por el encuestador no dan lugar a ambigüedades, la entrevista es personal y no anónima, por lo que no deja al encuestado consultar las respuestas.

Las entrevistas se pueden clasificar según su grado de estandarización. Una entrevista no estructurada, sin cuestionario, permite al investigador delimitar el problema a resolver. La

entrevista estandarizada realizada con cuestionario se realiza de forma oral, planteando sujeto, y aumenta la fiabilidad y comparación de los resultados. Con esto se pretende obtener una información más completa (Torres et al., s. f.).

● La entrevista se puede aplicar tanto a individuos alfabetos como a analfabetos.

● Se obtienen mayor número de respuestas de los encuestados que con los cuestionarios.

● Se recogen tanto las respuestas del encuestado como información complementaria del entrevistador.

● Mientras que un cuestionario recibido por correo puede ser olvidado o borrado en el acto, a una persona hay que recibirla y atenderla siendo más comprometido el hecho de no responder.

Diseño de un cuestionario o banco de preguntas

"Es un conjunto de preguntas sobre los hechos o aspectos que interesan en una investigación y que son contestadas por los encuestados. Se trata de un instrumento fundamental para la obtención de datos" (Torres et al., s. f.). Con lo anterior se evidencia que las herramientas de recolección de información proporcionan datos estadísticos viables para esta investigación, lo cual permite un muestreo más amplio a la pregunta de investigación.

En ese mismo contexto, el objetivo del diseño de una encuesta es minimizar los errores de no muestreo que pueden ocurrir. Debido a esto, los cuestionarios deben reunir las siguientes características (Torres et al., s. f.):

● Operativos, de fácil acceso y uso.

● Fidedignos: que sean confiables y reales.

● Válidos: que sean concisos, firmes, que no se presten a ambigüedades y que sean claros.

Para realizar un cuestionario, es importante tener en cuenta:

● El tipo de preguntas.

● La formulación de las preguntas.

● La organización del encuestado y su material.

Cabe resaltar que para cada herramienta de recolección de datos es importante conocer con detalle el objetivo de investigación y poder llevar un orden en el muestreo de los datos obtenidos.

Otras herramientas

En ese mismo sentido, para este trabajo de grado se utilizarán otras herramientas que ayudarán a recolectar la información, como son el cuadro de inventario consolidado, el flujograma y la matriz de riesgo.

Cuadro de inventario consolidado

Con este cuadro de inventario consolidado se analizarán las posibles soluciones a los problemas que puedan surgir dentro del control de riesgo de información, con el fin de buscar correctivos y formular un plan de mejoramiento a los problemas encontrados durante el proceso de investigación aplicado al CNMH.

> Garantizar la seguridad de la información en la entidad, mediante la definición, implementación, seguimiento y mejoramiento de elementos (herramientas, controles, procedimientos, etc.) que permitan proteger la información frente a la posible materialización de riesgos que afecten su disponibilidad, confiabilidad e integridad. (Sistema Integrado de Gestión Distrital, 2015).

Con lo anterior se pretende garantizar la usabilidad de los procedimientos adecuados y de esta manera proteger la información recolectada.

De conformidad con la GTC-ISO/IEC 27003, se recomienda identificar e incluir la siguiente información:

• El nombre único del proceso.

• La descripción del proceso y las actividades asociadas (creadas, almacenadas, transmitidas, eliminadas).

• La criticidad del proceso para la organización (si es crítico, importante, de apoyo).

• El dueño del proceso (unidad de la organización).

• Los procesos que proveen entradas y salidas de ese proceso.

• Las aplicaciones de tecnologías de información (IT) que apoyan este proceso.

• La clasificación de la información (confidencialidad, integridad, disponibilidad, control de acceso, no repudio u otras propiedades importantes para la organización, por ejemplo, cuánto tiempo puede almacenarse la información).

A partir de esto, el estudio de caso que se realizará en el CNMH será para uso exclusivo estudiantil y solo se usará para la realización del presente trabajo de grado de las estudiantes de la Pontificia Universidad Javeriana, que se comprometen a hacer un uso adecuado a esta información, la cual se utilizará exclusivamente para fines estudiantiles.

> La Comisión Distrital de Sistemas (CDS), con el fin de formalizar las políticas de seguridad de la información y los estándares planteados en las normas NTC-ISO/IEC 27001, que señala los requisitos del Sistema de Gestión de Seguridad de la Información y NTC/ISO IEC 17799 con su equivalente NTC-ISO/IEC 27002, que establece las mejores prácticas para la implementación del Sistema de Gestión de Seguridad de la Información, define los objetivos, alcances e importancia de la seguridad, como mecanismo para proteger la información y determinar las responsabilidades generales y específicas para la gestión de dicha seguridad, definir y adoptar los lineamientos a seguir para la implementación del Sistema de Gestión de Seguridad de la Información. (Alcaldía Mayor de Bogotá, Res. 305 de 2008, art. 15),

Por otra parte, esta herramienta es utilizada dentro del trabajo para consolidar los datos de forma precisa y no alterar la información dada por los funcionarios de la organización,

Flujograma

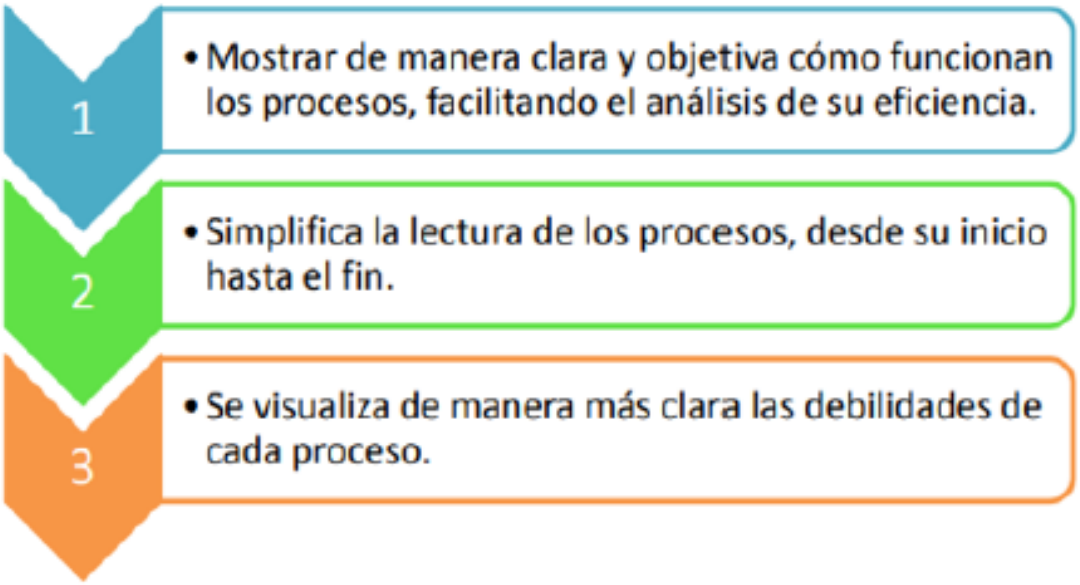
Es el análisis determinado de los procesos para la identificación de las entradas, los procesos y las salidas de aquellos puntos críticos dentro de una organización. También se emplea para comprender un proceso e identificar las oportunidades de mejorar en las entidades.

Un flujograma es una representación gráfica de un proceso, y en los últimos años se ha convertido en un instrumento que se usa en el análisis de los sistemas de las empresas.

Según Estupiñán (2006), los flujogramas facilitan una impresión visual del movimiento o flujo de la información desde su origen, de manera clara, lógica y concisa. Habitualmente son utilizados por los analistas de sistemas como lenguaje universal y son cada vez más utilizados por los auditores para la evaluación de los sistemas de control interno.

La figura 5 muestra las ventajas de los flujogramas, cuyo uso apropiado permitirá:

Figura 5. Ventajas del uso de flujogramas



Fuente: Estupiñán (2006).

Con esta herramienta se visualizan los procesos por los cuales pasa toda la información, y esto ayudará al momento de realizar la migración y la integración de la información, dentro de las direcciones del CNMH.

Matriz de riesgos

Según Ortiz (2016), la inexistencia de políticas de seguridad de la información y la falta de controles que evidencien los procesos realizados son factores relevantes que dificultan la ejecución y administración del modelo de gestión. Sin embargo, la metodología COBIT (Control Objetives for Information and related Technology) corrige determinados procesos y realiza de manera correcta los procesos que presentan riesgos. La aplicación de la normativa COBIT garantiza una disponibilidad de los servicios informáticos en la organización que permite generar confianza y credibilidad de los usuarios y las partes interesadas (Carpio, 2015).

Marco contextual

El Centro Nacional de Memoria Histórica (CNMH) es una de las unidades de información más importantes del país. Fue creado por la Ley 1448 de 2011 o Ley de Víctimas, que dictamina "medidas de atención, asistencia y reparación integral a las víctimas del conflicto armado interno". Su función es velar por la construcción y reparación integral así como por el derecho a la verdad de poblaciones que han sido vulneradas y desplazadas por el conflicto interno colombiano, por medio de la recuperación, reconstrucción, conservación y almacenamiento de documentos análogos, digitales, electrónicos y testimonios orales, con el fin de crear repositorios documentales que sirvan como testimonio de estos hechos que han marcado a nuestra sociedad, conocer la verdad de las víctimas y generar conciencia para evitar la repetición de estos actos.

El CNMH está compuesto por cinco direcciones apoyadas por procesos que gestionan la información y cada una tiene un rol para conservar y salvaguardar la memoria, disponiendo a la sociedad colombiana de documentos, libros, la revista *Conmemora*, podcasts y especiales digitales, que son testimonio de comunidades con problemáticas de vulnerabilidad.

De este modo, la Dirección de Archivo de los Derechos Humanos (DADH) se encarga de recolectar, ordenar, clasificar y realizar la conformación y puesta al servicio de documentos que relatan hechos de violación de los derechos humanos e infracciones al derecho internacional humanitario de las comunidades afectadas, con la misión de garantizar la custodia, preservación y acceso a la información a investigadores y público en general.

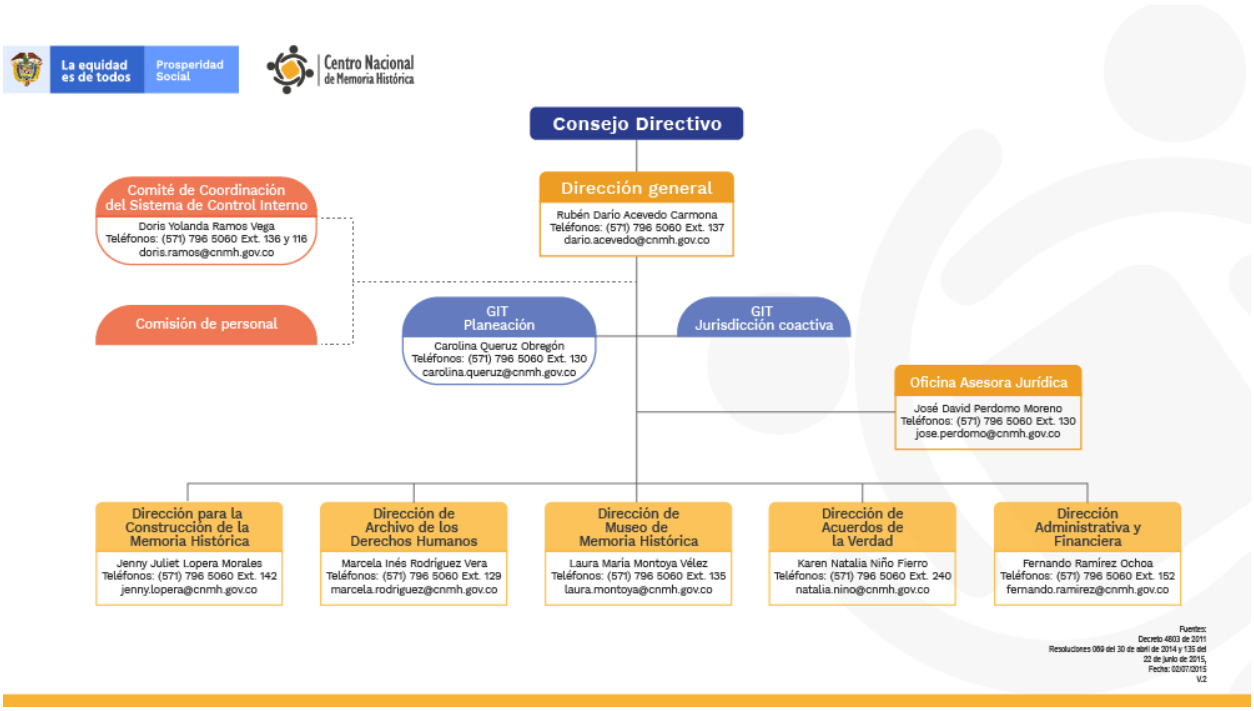
Al tiempo, DADH está conformada por talento humano capacitado en el tema, entre estos profesionales de Ciencia de la Información, quienes aplican los más altos estándares de calidad

para la recuperación y custodia de la información, basados en lineamientos de confidencialidad y buen manejo de la información, con el fin de evitar alteraciones, pérdida parcial o total de los datos, así como asegurar los procesos de acopio, registro, procesamiento técnico, conservación, preservación a largo plazo, uso social y apropiación de los archivos.

Finalmente, el CNMH debe garantizar y seguir con esta labor de procesamiento técnico, manejando excelencia en la catalogación y normalización de términos de los documentos, con lo cual se fortalecen las bases de datos y sistemas de información y se conserva la gestión del conocimiento de las colecciones sobre DD. HH. y DIH, para el libre acceso de toda la comunidad.

La figura 6 presenta el organigrama del CNMH:

Figura 6. Organigrama del CNMH



Fuente: https://centrodememoriahistorica.gov.co/organigrama/

Desarrollo de la investigación

Identificar los flujos de información

En esta primera fase se identificaron los flujos de información de la Dirección de Archivo de los Derechos Humanos (DADH) del Centro Nacional de Memoria Histórica (CNMH), cuya organización está conformada por varias direcciones, las cuales están compuestas por procesos que ayudan a las actividades que les han sido asignadas para procesar la información y salvaguardarla como patrimonio de la memoria de nuestro país.

En este sentido, se da una mirada general hasta llegar a la especificidad de los flujos de información, reflejando el movimiento de la información y los sujetos que allí interactúan desde un contexto interno y externo. Al respecto, Pomim (2009) indica:

> Los flujos informacionales transitan con datos e información con el fin de apoyar la construcción del conocimiento en los individuos organizacionales, orientado a una acción. Explica que el valor de la información es directamente proporcional al contexto del uso. Ciertamente, la necesidad de información del sujeto cognoscente es la que, de hecho, caracteriza el valor que la información tiene para dicha persona, en aquel contexto y para aquella acción. (p. 57)

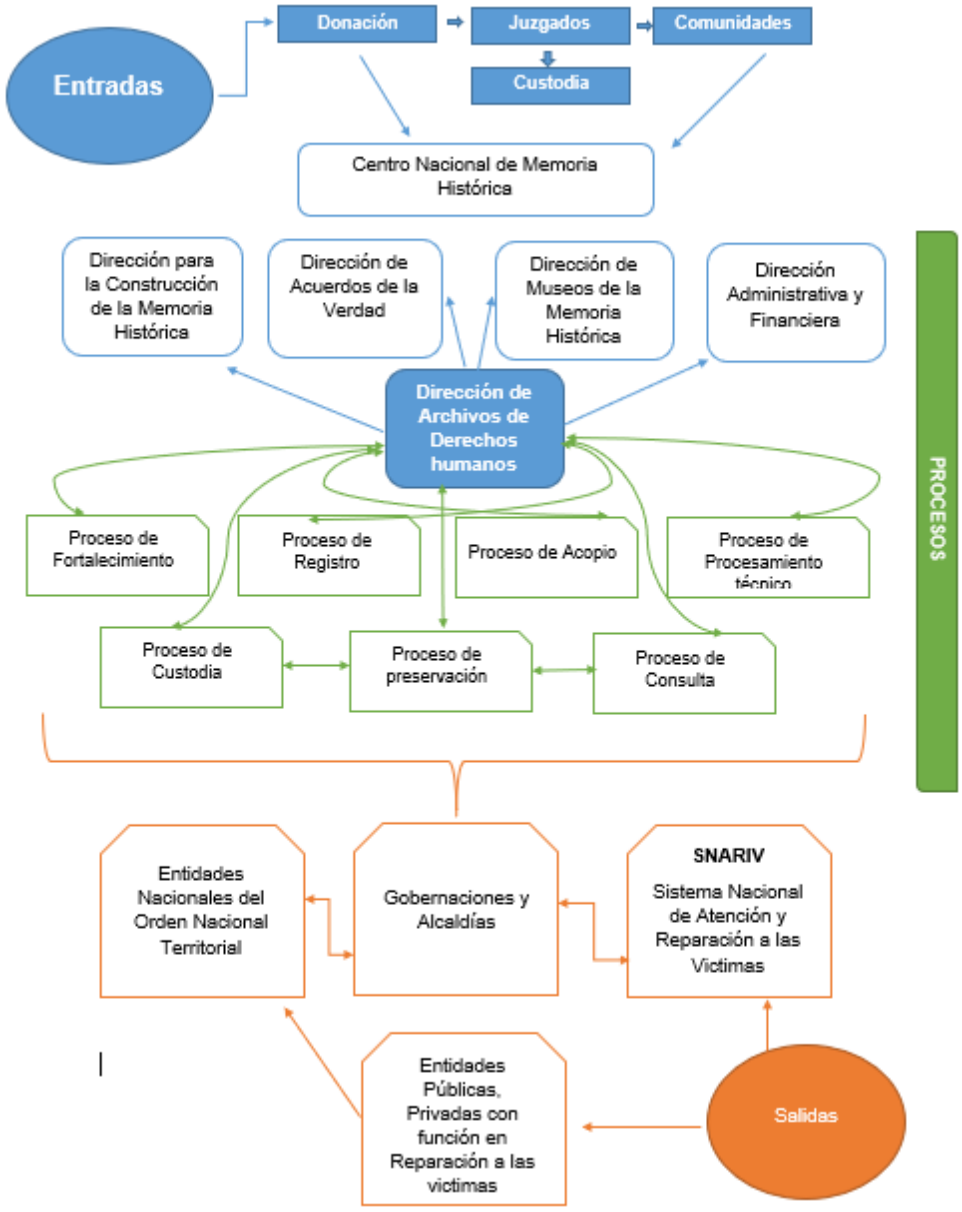
Se puede observar cómo se forman los canales de comunicación entre las diferentes direcciones, a pesar de encargarse de temáticas diferentes para el manejo de la información. Cabe anotar que en esta identificación se presentó una particularidad en la Dirección de Archivo de Derechos Humanos, ya que esta tiene participación con todas las direcciones y es la que mayor información maneja desde las entradas, los procesos que se gestionan y las salidas hacia otros entes.

En el flujograma (figura 7) se pueden identificar tres momentos. El primero, en color azul, indica las principales categorías para remitir la información, que se asocian en cuatro grupos. A su vez, las flechas representan el flujo de la información, que inicia con las entradas de los objetos de información a la unidad, en este caso el Centro Nacional de Memoria Histórica (CNMH) y sus cinco direcciones, y se resalta la Dirección de Archivo de los Derechos Humanos (DADH), donde se concentran en mayor medida los datos. En el segundo momento, en color verde, están los procesos que componen la DADH y cómo todos interactúan entre sí, ya que los datos pueden estar en diferentes procesos y los flujos de información van y vienen según la gestión que se esté realizando. Finalmente, el tercer momento, en color naranja, indica las salidas de la información hacia a los entes externos, según sea su función y gestión.

Flujograma

A continuación, se muestra la representación gráfica de los flujos de información:

Figura 7. Flujograma del CNMH



Fuente: elaboración propia.

Alcance del flujograma basado en tres tipologías

Para el diseño del flujograma se realizó una entrevista a seis de los colaboradores de la Dirección de Archivo de Derechos Humanos los cuales interactúan en todos los procesos de la dirección las

preguntas de la entrevista reposan el en anexo de “Entrevista” donde se pueden identificar; esto con el propósito de identificar los flujos de información y los objetos de información que interactúan en la dirección, por medio de los procesos que la componen y las tipologías principales que manejan.

● **Captura:**

La forma de captura de los datos ayuda a identificar el tipo de información y el formato en el cual se conservará. La DADH hace referencia al tipo de información cuando indica: *“Por supuesto, tenemos material de archivo, análogo, CD’s, otros soportes como VHS, Betamax y la colección que tenemos en la biblioteca”* (comunicación personal).

Como se ha descrito anteriormente, para una efectiva gestión de riesgos basada en una gobernanza de información, es necesario conocer a profundidad los objetos de información que hacen parte de la unidad y la forma como esta se va moviendo por todas las direcciones hasta llegar a los procesos para su respectiva gestión, formado así los flujos de información. Una vez esto sea identificado, se puede iniciar con el mapeo de los posibles riesgos de información y los controles que se les puedes llegar a plantear. Asimismo, la clasificaron de la información es el inicio de la gobernanza, frente a lo cual los colaboradores aseguran que *“se tiene una clasificación de la información, ya que esto hace parte de la DADH y todo lo que tiene datos personales, mejor dicho, toda esa información que nos llega y que producimos se maneja con base en la Ley de Transparencia y la Ley Habeas Data”* (comunicación personal).

Con lo anterior es claro que, además de tener un control de la información y conocer sus objetos, se cuenta con lineamientos para la captura de estos datos basados en normas y el manejo adecuado de la información.

Al haber identificado y clasificado la información, se utilizan varias herramientas como las tablas de retención, donde los datos se ordenan según la gestión documental que maneje la unidad. Este es otro insumo para la elaboración de la matriz de riesgos de información.

● **Procesamiento:**

La información que llega a la DADH tiene varias entradas (donación, entes gubernamentales, comunidades y custodia) y esta pasa por varios procesos, como lo indican los colaboradores: *"La información llega por medio del proceso de acopio y pasa por el proceso de procesamiento técnico, donde le damos la debida gestión a los datos y de igual forma, si es necesario, pasa por otros procesos"* (comunicación personal). Es aquí donde los sistemas de información toman un rol importante en el desarrollo del procesamiento de los datos, ya que se conserva la información en diferentes formatos, con el fin de salvaguardar los datos y evitar la pérdida de su integridad. Estos datos también se consideran objetos de información y por lo tanto se identifican los posibles riesgos en ellos, desde un enfoque informacional y tecnológico, teniendo en cuenta factores los sistemas libres o de licencias pagadas. Al respecto, los colaboradores indican: *"Nuestros sistemas son de licencias libres, pero desde el área de tecnología se aplican técnicas de seguridad de la información y se realizan mantenimientos de estos sistemas con una prioridad establecida. De igual forma, nosotros trabajamos con las recomendaciones del MinTIC"* (comunicación personal). En tal sentido, el monitoreo del acceso a la información es uno de los controles para evitar un posible evento o mitigar un riesgo ya materializado, con lo cual la gestión de usuarios

toma un sentido para salvaguardar la información en los diferentes sistemas que se puedan utilizar. Ello se evidencia en el siguiente testimonio: *"¡Claro! Se hace un control de los usuarios y sus accesos y están segmentados por roles y delimitados a la información que necesitan consultar; este control es riguroso, ya que se maneja información confidencial y datos personales, pero hay que aclarar que también debemos dar acceso a la comunidad, por medio de nuestra página mediante datos en línea ya clasificados como públicos para su visualización"* (comunicación personal).

- **Flujos de información:**

La información no es ni tendrá un estado estático, al contrario, es totalmente dinámica y evoluciona de acuerdo al contexto. Entonces, las unidades de información van recepcionando información nueva y, a su vez, van creando información por medio de su gestión del conocimiento, pero no toda se distribuye para toda la unidad; es decir, en el caso de la DADH se maneja la totalidad de los flujos de información, porque esta dirección interactúa con todas las demás en un porcentaje mayor, y no solo de forma interna, sino también con entes externos, como lo son entidades gubernamentales, entidades públicas y privadas y otras unidades de información, las cuales constituyen entradas y salidas de información. Este proceso organizacional se implementa de la siguiente manera: *"Las comunicaciones internas y externas son controladas desde nuestro modelo de calidad atado al sistema de gestión integral, donde están documentados nuestros procedimientos para el manejo de la información y para cuando se comparte con entidades externas"* (comunicación personal).

Con estas tres tipologías se da un acercamiento para la identificación y análisis de los posibles riesgos que se puedan mapear, y sobre esto iniciar con el análisis de riesgos de información y la gobernanza de los datos.

Inventario básico de objetos de información

La tabla 1 indica el tipo de información que maneja el CNMH y los formatos donde esta se almacena.

Tabla 1. Objetos de información por tipo y formato

Tipo de Información	Formato
Hechos de violación de los Derechos Humanos de las comunidades afectadas	Análogo, PDFa, audios, Publicaciones Seriadas, videos y fotografías.
Infracciones al Derecho Internacional Humanitario de las comunidades afectadas	Análogo, PDFa, audios, Publicaciones Seriadas, videos y fotografías.
Expedientes Jurídicos	Análogo y PDFa
Informes de entes Gubernamentales	Análogo y PDFa
Testimonios de Comunidades	Análogo, PDFa, audios, videos y fotografías.
Publicaciones sobres Derechos Humanos	Publicaciones Seriadas
Podcast	Audios, canciones.

Fuente: elaboración propia.

La gestión de riesgos en las unidades de información están enfocadas desde un alcance de la gestión cultural y el acceso de los usuarios a la información. Allí, el contenido, la usabilidad, el almacenamiento y la custodia son procesos para la identificación de riesgos internos y externos, los cuales están atados a sus respectivos controles que permiten mitigar dichos riesgos, y son

variables de análisis para evitar la materialización de eventos donde se generan vulnerabilidades. Así pues, los medios de almacenamiento y custodia de la información cuentan con controles enfocados en la seguridad e infraestructura para salvaguardar la información.

En concordancia con la norma técnica,

> se deberían establecer los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retirada o destrucción de activos no autorizadas. (NTC-ISO/IEC 27002, 2007, p. 34)

El CNMH está en la obligación de divulgar la información de forma efectiva y asertiva, por lo que es necesario contemplar los riesgos desde todas las direcciones, identificando unos riesgos generales hasta llegar a los riesgos particulares de cada dirección, como se representa en la DADH, por medio de un análisis *conspectus* de su profundidad, a través de un inventario que será registrado y tratado en una matriz de riesgos de información, salvaguardando a su vez recursos de la unidad.

Al ser una entidad pública y dado el manejo de los flujos de información, sus procesos y el tipo de información sensible que maneja, el CNMH se rige bajo la Ley 1266 de 2008 de Habeas Data (Sentencia T-729 de 2002 Habeas Data), la Ley 1581 de 2012 de Protección de Datos Personales, la Ley 1712 de 2014 de Transparencia del derecho de acceso a la información pública nacional y la NTC/ISO 27001:2013 como marco de referencia internacional para la Gestión de la Seguridad de la Información y la protección de la información desde su captura, procesamiento, entradas y salidas.

Análisis de metodologías de riesgos basados en modelos de gobierno de información

Metodología COBIT

Control Objetives for Information and related Technology (COBIT) es la normativa aceptada internacionalmente como una buena práctica para el control de la información, TI y los riesgos que conlleva. Este modelo se utiliza para implementar el gobierno de TI y mejorar los controles de TI.

- **Riesgos de TI:**

La evaluación del riesgo identifica situaciones que podrían tener un impacto negativo en los procesos críticos, intenta cuantificarlo y establece su probabilidad de ocurrencia.

- **Seguridad de la información:**

La seguridad de la información es el conjunto de medidas que previenen a las organizaciones y los sistemas tecnológicos mediante el resguardo y la protección de la información de agentes externos e internos que quieran sustraer de forma ilegal la confidencialidad, la disponibilidad y la integridad de datos.

- **Tecnologías de la información (TI):**

Es la terminología asociada al almacenamiento, protección, procesamiento y transmisión de la información. Es decir, enmarca todo lo relacionado con la informática, la electrónica y las telecomunicaciones, y los avances tecnológicos como el Internet, las comunicaciones móviles, los satélites, etc.

- **Modelo de gestión:**

Los modelos de gestión son procesos, metodologías, normativas y esquemas fundamentados por estudios científicos que proporcionan a investigadores y organizaciones el mejor plan estratégico en función de la problemática.

- **Planeación estratégica:**

Son las actividades proyectadas al logro de los objetivos institucionales de la empresa y tiene como finalidad básica el establecimiento de guías generales de acción.

- **Análisis FODA:**

Es un análisis integral y situacional de la empresa en la cual se consideran factores externos e internos como las fortalezas, oportunidades, debilidades y amenazas.

- **Principios y habilitadores de COBIT:**

Los principios y habilitadores de COBIT son genéricos y útiles para las organizaciones de cualquier tamaño, bien sean comerciales, sin fines de lucro o del sector público.

- **Gobierno de TI según COBIT:**

Asegura el cumplimiento de objetivos empresariales, evalúa necesidades, condiciones y opciones de los interesados. A través de la priorización y toma de decisiones, supervisa (monitor) el desempeño y cumplimiento de la dirección y los objetivos acordados.

- **Gestión de TI según COBIT:**

La gestión planea, construye, opera y supervisa (monitor) las actividades fijadas y acordadas por el cuerpo de gobierno.

• COBIT 5, objetivos y componentes:

Según la Isaca, COBIT 5 se actualizó para:

• Agilizar el intercambio de información a través de una organización.

• Alcanzar objetivos corporativos incorporando TI en la estrategia.

• Minimizar y controlar la seguridad de la información y la gestión de riesgos.

• Optimizar el coste que rodea la TI y la tecnología.

Es por esto que las organizaciones hoy en día necesitan permanecer en un modo de defensa constante, protegiendo la información que se comparte y gestiona, la cual se mueve a través de las nuevas tecnologías. Por tanto, la seguridad que se brinda a los interesados, así como los requisitos reglamentarios, son factores del día a día de las organizaciones, de ahí que deban ser resistentes a cualquier problema de comunicación.

Esta herramienta permite registrar, analizar, evaluar y tratar los riesgos identificados, desde los procesos hasta llegar a la totalidad de la organización, y a su vez es fuente para implementar controles de prevención y ayuda a la toma de decisiones.

Finalmente, se toma como recolección de información la matriz de riesgo, la cual permite evidenciar la totalidad de los procesos y toma de decisiones en una organización, y asimismo

facilita a la investigación el registro de los riesgos y su identificación, con el fin de mitigar los procesos que se encuentren en peligro.

Norma ISO 31000:2009

> La norma ISO 31000 es una herramienta que establece una serie de principios para la implementación de un Sistema de Gestión de Riesgos en las empresas. Como se dijo antes, puede aplicarse a cualquier tipo de organización independiente de su tamaño, razón social, mercado, fuente de capital, espectro comercial o forma de financiación. No especifica ningún área o sector en concreto. (Norma ISO 31000, p. 8)

La norma ISO 31000 sirve de referencia para otros modelos de Sistema de Gestión de Riesgos. Además, completa la información de otras normativas en el plano local, regional, nacional o incluso continental. En este apartado se explica no solo la eficacia de dicha norma, sino que se puntualizan las buenas prácticas que se deben tener en cuenta en cualquier organización. Los 11 principios expuestos son (Norma ISO 31000, p. 9):

- La gestión crea valor a la organización.

- Debe estar integrada a los procesos.

- Forma parte de la toma de decisiones en la empresa.

- Trata de forma explícita la incertidumbre.

- Debe ser sistemática, estructurada y adecuada.

- Es necesario que esté basada en la mejor información disponible.

- Debe adaptarse a la medida de cada caso.

- Implica la inclusión de factores humanos y culturales.

- Debe ser transparente, eficaz e inclusiva.

- Es necesario que sea iterativa y sensible al cambio.

- Tiene que ir orientada a la mejora continua de la organización.

Dentro de esta normativa se derivan dos causas fundamentales:

- **Consecuencia:**

La norma la define como la derivación de causa-efecto, es decir, aquellos elementos que provienen directa o indirectamente de otros. Así pues, se trata de ajustar los riesgos que cumplen con la premisa de causa-efecto. Ello significa que no siempre se pueden vaticinar las consecuencias de una acción o decisión, pero este solo hecho es el origen de cualquier Sistema de Gestión de Riesgos.

- **Probabilidad:**

Para la gestión de riesgos es fundamental que las empresas contemplen la entrada de hechos que puedan derivarse o no de las decisiones de la empresa. Nunca se está preparado para los eventos, menos si estos provienen de elementos externos, pero el solo hecho de pensar en su realización ya es un buen indicador en el Sistema de Gestión de Riesgos.

Metodologías de Sistema de Gestión de Riesgos - Norma ISO 31000:2009

> Son aquellas que están orientadas a la identificación, evaluación y el posterior tratamiento de los riesgos derivados de una actividad. Entre ellas está, como es obvio, la norma ISO 31000. También se encuentran otros estándares, como por ejemplo la norma AS/NZS 4360, que plantea un modelo de análisis centrado en los principios de la familia normativa ISO 9000. Otras de las metodologías más reconocidas son el sistema APPCC (Análisis de Peligros y Puntos Críticos de Control) y el método del ARO (Administración del Riesgo Operacional), los cuales operan en el mismo sentido. (Norma ISO 31000, p. 10)

En ese mismo sentido, y según la normativa, los riesgos no tienen el mismo origen ni la misma naturaleza, por lo cual existen estructuras en la actividad de producción y el sector en el que operan. Para ello es importante aclarar los métodos de análisis de riesgos que fueron utilizados para el siguiente trabajo de grado.

- **Métodos cualitativos:**

Con esta herramienta se realizó el trabajo de grado de las estudiantes de la Pontificia Universidad Javeriana, y su objeto de estudio fue el Centro Nacional de Memoria Histórica. Se utilizó una entrevista a algunos funcionarios de la institución, para un análisis más detallado del Sistema de Gestión de Riesgo global en la organización.

Los métodos cualitativos incluyen:

- *Brainstorming* o lluvia de ideas.

- Cuestionario y entrevistas estructuradas.

• Evaluación para grupos multidisciplinarios.

Los datos recolectados sirvieron para hacer un mapeo específico del objeto de estudio, lo cual facilitó la recolección de la información.

La norma contempla los siguientes aspectos.

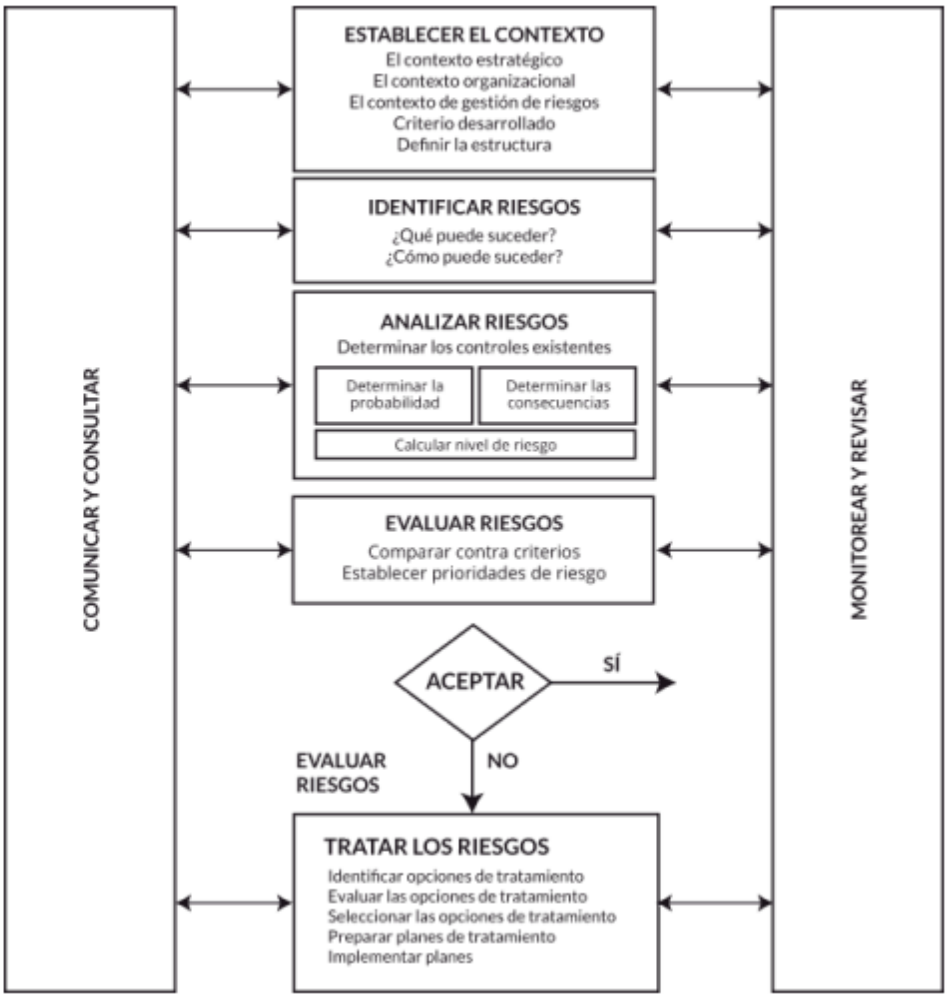
● Se utilizan clasificaciones de palabra como alto, medio o bajo, o descripciones más detalladas de la probabilidad y la consecuencia.

● Estas clasificaciones se demuestran en relación con una escala apropiada para calcular el nivel del riesgo.

● Se debe poner atención en la escala utilizada, a fin de evitar malos entendidos o malas interpretaciones de los resultados del cálculo.

La figura 8 muestra el proceso de identificación, análisis, evaluación y tratamiento de los Sistemas de Gestión de Riesgos en una organización.

Figura 8. Esquema del Sistema de Gestión de Riesgos en una organización



Fuente: Norma ISO 31000, p. 14).

Teniendo en cuenta que los profesionales en Ciencia de la Información son responsables de facilitar información de calidad a los usuarios, y por ende de reconocer sus necesidades informacionales (Gallego & Juncà, 2009), y siguiendo los objetivos presentados por la Norma ISO 31000, se deben implementar criterios dentro de las organizaciones y aplicar las buenas prácticas para la mejora continua de la entidad.

En la tabla 2 se toman los conceptos más relevantes de la ISO 31000:2009.

Tabla 2. Resumen de la Norma ISO 31000:2009

Para qué sirve la norma ISO 31000:2009	**Descripción de la norma ISO 31000:2009**	**Componentes de la norma ISO 31000:2009**
La norma ISO 31000 sirve de referencia para otros modelos de Sistema de Gestión de Riesgos. Además, completa la información de otras normativas en el plano local, regional, nacional o incluso continental. En este apartado se explica no solo su eficacia, sino que también se puntualizan las buenas prácticas que se deben tener en cuenta en cualquier organización (Norma ISO 31000, p. 9).	Son aquellas que están orientadas a la identificación, evaluación y el posterior tratamiento de los riesgos derivados de una actividad. Entre ellas está, como es obvio, la norma ISO 31000. También se encuentran otros estándares, como por ejemplo la norma AS/NZS 4360, que plantea un modelo de análisis centrado en los principios de la familia normativa ISO 9000. Otras de las metodologías más reconocidas son el sistema APPCC (Análisis de Peligros y Puntos Críticos de Control) y el método del ARO (Administración del Riesgo Operacional), los cuales operan en el mismo sentido (Norma ISO 31000, p. 10).	Mejorar la identificación de oportunidades y amenazas. Optimizar la gestión empresarial. Aumentar la confianza en los grupos de interés (*stakeholders*). Establecer una base para la toma de decisiones. Mejorar los controles y los métodos de seguimiento y monitoreo. Optimizar la prevención y la gestión de incidentes. Minimizar las pérdidas asociadas a los procesos empresariales. Fomentar el aprendizaje organizativo en todos sus niveles.
Cabe resaltar que la ISO 31000:2009 no es certificable Y no lo es porque no hace referencia a un sistema de gestión concreto. Vale aclarar que las organizaciones que apliquen los principios de esta norma estarán asumiendo el riesgo en sus procesos, pero no están realizando ningún sistema de gestión.	Como descripción de la norma es importante recalcar la integridad de la gestión del riesgo en todas sus actividades y funciones significativas; esto requiere del apoyo de las partes interesadas, principalmente de la alta gerencia de la organización.	Dentro de los componentes de la ISO 31000:2009 es importante mencionar dos factores que son muy frecuentes dentro de una organización: la probabilidad y el impacto.

El objetivo principal de esta norma es trazar un marco de acción para saber qué aspectos gestionar y cómo hacerlo. Existen dos componentes para ello: consecuencia y probabilidad (Norma ISO 31000, p. 10). **Consecuencia:** la norma la define como la derivación de causa-efecto, es decir, aquellos elementos que provienen directa o indirectamente de otros. **Probabilidad:** para la gestión de riesgos, es fundamental que las empresas contemplen la entrada de hechos que puedan derivarse o no de las decisiones de la empresa.	En ese mismo sentido, y según la normativa, los riesgos no tienen el mismo origen ni la misma naturaleza, para lo cual existen estructuras en la actividad de producción y el sector en el que operan. Por ello, es importante dejar claro que las metodologías de análisis de riesgos se dividen en cuatro grupos principales: - Método de cuantificación. - Métodos cualitativos. - Métodos Delphi - Métodos: semicuantitativos. Para este trabajo solo se nombrará el método cualitativo, que hace referencia a la investigación realizada dentro del trabajo mencionado anteriormente. **Métodos cualitativos:** es la herramienta más utilizada para la toma de decisiones en proyectos empresariales; para ello, los investigadores se apoyan en su juicio, experiencia e intuición para la toma de decisiones (Norma ISO 31000, p. 13).	Es importante mencionar las ventajas de implementar esta normativa dentro de las organizaciones, entre ellas: - Mejorar su eficiencia operativa. - Tener una mejor gobernabilidad interna de la organización. - Aumentar la confianza por partes externas. - Mejorar su rendimiento y la sostenibilidad. - Reducir los costes. - Mitigar o desaparecer de incidentes inesperados.

Fuente: elaboración propia.

Por otra parte, es importante tener en cuenta otras normas y metodologías que aportarán al Sistema de Gestión de Riesgos, las cuales se presentan a continuación.

Metodología COSO de riesgos

> El modelo o metodología COSO surge en el año 1985. Sus siglas responden a Committee of Sponsoring Organizations of the Treadway, que es una organización de carácter voluntario constituida por representantes de cinco organizaciones del sector privado en Estados Unidos. Nace con la misión de crear y proporcionar conocimiento frente a tres grandes temas relacionados. (Ealde Business School, 2020)

Es importante nombrar tres elementos fundamentales de este proceso.

- La gestión del riesgo empresarial (ERM) (*Enterprise Risk Management*).

- El control interno.

- La lucha contra el fraude.

El objetivo principal del COSO es ayudar a las entidades a evaluar y mejorar sus sistemas de control interno.

- **Definición de control interno en el marco COSO:**

> Según el marco COSO de gestión de riesgos, el control interno se define como un proceso llevado a cabo por la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías. (Ealde Business School, 2020)

Cabe resaltar tres componentes que hacen parte de este Sistema de Gestión de Riesgos.

- Eficacia y eficiencia de las operaciones.

- Confiabilidad de la información.

- Cumplimiento de las leyes, reglamentos y normas que sean aplicables.

En 2004 surgió COSO II, que ampliaba el concepto de control interno a la gestión de riesgos. En ella también debe involucrar todo el personal de las entidades, incluidos los directores y administradores.

Dicho estándar está dividido en cinco capítulos:

● Ambiente de control.

● Evaluación de riesgos.

● Actividades de control.

● Información y comunicación.

● Supervisión.

Por último, en 2013 se publicó la tercera versión, COSO III, una revisión del marco COSO de riesgos que se centró en mejorar aspectos como la agilidad de los sistemas de gestión de riesgos, una mayor concreción en lo que se consideraba comunicación e información, un mayor énfasis en la eliminación de riesgos y la incorporación clara del concepto *consecución de los objetivos* (Ealde Business School, 2020).

Para una mejor comprensión de las metodologías COSO de Riesgo, se ha elaborado la tabla 3.

Tabla 3. Resumen de la metodología COSO de Riesgo

Para qué sirve la metodología COSO de Riesgo	**Descripción de la metodología COSO de Riesgo**	**Componentes de la metodología COSO de Riesgo**
"El modelo o metodología COSO surge en el año 1985. Sus siglas responden a Committee of Sponsoring Organizations of the Treadway, que es una organización de carácter voluntario constituida por representantes de cinco organizaciones del sector privado en Estados Unidos. Nace con la misión de crear y proporcionar conocimiento frente a tres grandes temas relacionados" (Ealde Business School, 2020),	El objetivo principal del COSO es el ayudar a las entidades a evaluar y mejorar sus sistemas de control interno.	Las organizaciones deben definir componentes para garantizar que todos los activos relevantes se toman con la importancia al momento de implementar la metodología COSO de Riesgo, los cuales son: ● La gestión del riesgo empresarial (ERM) (*Enterprise Risk Management*). ● El control interno. ● La lucha contra el fraude.
En 2004 surgió COSO II, que ampliaba el concepto de control interno a la gestión de riesgos. En ella también debe involucrar todo el personal de las entidades, incluidos los directores y administradores.	El marco actual vigente para el control interno de los riesgos es el llamado COSO ERM 2017. Esta actualización mantiene el enfoque financiero de sus predecesores, no obstante, su flexibilidad y estructura permite que sea utilizado indistintamente por cualquier tipo de actividad (Ealde Business School, 2020).	Dicho estándar está dividido en cinco capítulos: ● Ambiente de control. ● Evaluación de riesgos. ● Actividades de control. ● Información y comunicación. ● Supervisión.
Por último, en 2013 se publicó la tercera versión, COSO III, una revisión del marco COSO de riesgos que se centró en mejorar aspectos como la agilidad de los sistemas de gestión de riesgos, una mayor concreción en lo que se consideraba comunicación e información, un	El marco de COSO 2013 mantiene la definición de *control interno* y los cinco componentes de control interno, pero al mismo tiempo incluye mejoras y aclaraciones que facilitan su uso y aplicación en las entidades. A través de esta actualización, COSO propone	Según la normativa COSO, es indispensable contar con los siguientes componentes: ● Eficacia y eficiencia de las operaciones. ● Confiabilidad de la información financiera.

mayor énfasis en la eliminación de riesgos y la incorporación clara del concepto *consecución de los objetivos*. (Ealde Business School, 2020).	desarrollar el marco original, empleando *principios* y *puntos de interés*, con el objetivo de ampliar y actualizar el concepto de control interno previamente planteado, sin dejar de reconocer los cambios en el entorno empresarial y operativo (Deloitte, 2015).	● Cumplimiento de las leyes, reglamentos y normas aplicables.

Fuente: elaboración propia.

Metodología de Gestión de Riesgos del MinTIC

> La primera y más importante forma de lograr un adecuado avance en todo el proceso de administración del riesgo es el "compromiso de la alta y media dirección", puesto que, al igual que como se menciona en la guía, tener el verdadero compromiso de los directivos garantiza en gran medida el éxito de cualquier proceso emprendido, puesto que se necesita su aprobación y concurso en el momento de cualquier toma de decisiones, así mismo como se menciona en el MSPI la necesidad de tener aprobación de la dirección en cada etapa es necesaria (Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC], 2019)

El Modelo de Seguridad y Privacidad de la Información (MSPI) es una herramienta creada con el fin de establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las entidades.

En relación con lo manifestado arriba por el MinTIC, cabe resaltar que desde un inicio las organizaciones se deben comprometer y garantizar de forma apropiada su aceptación en el mercado y contribuir en los procesos al momento de tomar cualquier decisión.

Siguiendo con lo estipulado en esta metodología, se debe designar a un dirigente que debe ser el mismo que tiene a cargo el desarrollo o sostenimiento del Modelo Estándar de Control Interno (MECI) y el Sistema de Gestión de la Calidad, que asesore y apoye todo el proceso de diseño e implementación de la gestión integral del riesgo.

El MECI es una herramienta gerencial que tiene como fin servir de control en las entidades del Estado, y a su vez contribuye a que cumplan sus objetivos institucionales en el marco legal que les aplica.

> En segundo lugar se encuentra la "conformación de un equipo MECI o de un grupo interdisciplinario", la idea de una integralidad en el tratamiento de los riesgos para poder tener una visión completa de la entidad y en la cual se pueda tener el aporte de diferentes áreas analizando un mismo proceso, es esencial y ayuda a encaminar correctamente el MSPI, es por esta razón que se deben incluir los riesgos de seguridad en el momento que se hace el análisis para el MECI, o para el modelo de Gestión de Calidad. (MinTIC, 2019)

Es necesario tener en cuenta la creación de este grupo interdisciplinario, pues sus aportes en los procesos serán muy importantes para la toma de decisiones. Las personas que lo conformen deben conocer muy bien la organización y cada unidad de información.

> Finalmente se encuentra la "capacitación en la metodología", este punto es un poco más profundo, porque es claro que el equipo interdisciplinario debe capacitarse para poder analizar ahora los riesgos de seguridad, sin embargo, dicho equipo debe estar integrado por alguno de los integrantes del proyecto MSPI, para tener un contexto organizacional en todos los aspectos del desarrollo del MSPI. (MinTIC, 2019)

- **Ministerio de las TIC - Identificación de riesgos:**

En el proceso de valoración de riesgos en seguridad de la información son de gran importancia los insumos, la clasificación de los objetos y las buenas prácticas al momento de realizar gestión de riesgos a los activos de información, los cuales se consideran con nivel de clasificación ALTA dependiendo de los criterios de clasificación; es decir que en los criterios de confidencialidad, integridad y disponibilidad tengan la calificación que se presenta en la figura 9:

Figura 9. Criterios de clasificación de riesgos

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Tabla 1. Criterios de Clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Fuente: MinTIC (2019).

- **Ministerio de las TIC - Identificación de las vulnerabilidades:**

Para identificar las vulnerabilidades en una organización se debe conocer la lista de amenazas comunes, la lista de inventario de activos y el listado de controles existentes.

Es necesario identificar las vulnerabilidades en las siguientes unidades de información, según la guía del MinTIC (2019):

- Organización.

- Procesos y procedimientos.

- Rutinas de gestión.

- Personal.

- Ambiente físico.

- Configuración del sistema de información.

- *Hardware, software* y equipos de comunicaciones.

- Dependencia de partes externas.

- **Ministerio de las TIC - Identificación de las consecuencias:**

Para identificar las consecuencias es necesario tener en cuenta:

- La lista de activos de información y su relación con cada proceso de la entidad.

- La lista de las amenazas y vulnerabilidades con respecto a los activos y su pertinencia.

- **Ministerio de las TIC - Evaluación del riesgo:**

> Esta se hace de manera cualitativa generando una comparación en la cual se presenta el análisis de la probabilidad de ocurrencia del riesgo versus el impacto del mismo, obteniendo al final la matriz denominada "Matriz de calificación, Evaluación y respuesta a los riesgos", con la cual la guía presenta la forma de calificar los riesgos con los niveles de impacto y probabilidad establecidos anteriormente, así como las zonas de riesgo presentando la posibles formas de tratamiento que se le puede dar a ese riesgo. (MinTIC, 2019)

Figura 10. Clasificación del riesgo

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo *Moderada:* Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo *Alta*: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo *Extrema*: Reducir el riesgo, Evitar, Compartir o Transferir

Fuente: MinTIC (2019).

- **Ministerio de las TIC - Valoración de controles para el tratamiento del riesgo:**

En la valoración de controles se pretende buscar una calificación en la matriz de riesgos, para luego ser medidos en cada etapa de identificación y análisis de riesgos. Asimismo, se pretenderá seleccionar los controles que permitan reducir los objetos de exposición del riesgo, de manera que se pueda realizar un reajuste y compararlo nuevamente con los criterios establecidos por la organización, y de este modo mitigar el riesgo en cada proceso para los temas de seguridad.

Al momento de clasificar y valorar los controles se deben tener en cuenta dos tipos de controles: preventivos y correctivos.

Preventivos: son los que actúan para eliminar las causas del riesgo y de esta forma prevenir su ocurrencia o materialización.

Correctivos: son todos aquellos que permiten el restablecimiento de las actividades, luego de detectar un evento no deseable. Esto ayuda a transformar las acciones que propiciaron las incidencias.

Por otro lado, se debe tener en cuenta la aprobación del plan de tratamiento de riesgos por parte de los directivos del área encargada, así como lograr la participación de las diferentes áreas incluidas en el proceso y, por supuesto, de la Dirección.

Para una mejor comprensión de las metodologías de gestión de riesgos del MinTIC, se ha elaborado la tabla 4.

Tabla 4. Resumen de las metodologías de Gestión de Riesgos del MinTIC

Para qué sirven las metodologías de gestión de riesgos del MinTIC	**Descripción de las metodologías de gestión de riesgos del MinTIC**	**Componentes de las metodologías de gestión de riesgos del MinTIC**
Ayuda a lograr un adecuado avance en todo el proceso de administración del riesgo. Ello significa que las organizaciones deben tener "compromiso de la alta y media dirección", al igual que el verdadero compromiso de los directivosm los cuales garantizan en gran medida el éxito de cualquier proceso emprendido, puesto que se necesita su aprobación y concurso en el momento de cualquier toma de decisiones. Asimismo, como se menciona en el MSPI, la necesidad de contar con la aprobación de la dirección en cada etapa es necesaria (MinTIC, 2019).	El MSPI es una herramienta que fue creada para establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las entidades.	Las organizaciones deben definir los siguintes componentes para garantizar que todos los activos relevantes se toman con la importancia requerida al momento de valorar el riesgo: ● Objetivos estratégicos de negocio, políticas y estrategias de la organización ● Procesos del negocio. ● Funciones y estructura de la organización. ● Los requisitos legales, reglamentarios y contractuales aplicables a la organización. ● La política de seguridad de la información de la organización. ● El enfoque global de la

		organización hacia la gestión del riesgo. ● Activos de información. ● Ubicación de la organización y sus características geográficas. ● Restricciones que afectan a la organización. ● Expectativas de las partes interesadas. ● Entorno sociocultural. ● Interfaces (Ej. Intercambio de información con otras entidades).
"Conformación de un equipo MECI o de un grupo interdisciplinario", con la idea de una integralidad en el tratamiento de los riesgos para poder tener una visión completa de la entidad y en la cual se pueda contar con el aporte de diferentes áreas analizando un mismo proceso, es esencial y ayuda a encaminar correctamente el MSPI. Es por esta razón que se deben incluir los riesgos de seguridad al momento de hacer el análisis para el MECI, o para el modelo de Gestión de Calidad (MinTIC, 2019)	Una amenaza dentro de una organización tiene la potestad de dañar activos, tales como la información, los procesos y los sistemas, etc. Los peligros pueden provenir de causas naturales o humanas y podrían ser accidentales o deliberadas, por lo cual es conveniente identificar todos los orígenes. Las amenazas deben identificar fallas comunes dentro de la organización y el tipo. Las causas podrían ser acciones no autorizadas, daño físico o fallas técnicas.	Con los controles se busca una calificación en la matriz de riesgos, para luego ser medidos en cada etapa de identificación y análisis de riesgos, y de este modo mitigar el riesgo en cada proceso para los temas de seguridad. En la clasificación y valoración de los controles se deben tener en cuenta dos tipos: preventivos y correctivos. **Preventivos:** son los que actúan para eliminar las causas del riesgo y de esta forma prevenir su ocurrencia o materialización. **Correctivos:** son todos aquellos que permiten el restablecimiento de las actividades, luego de detectar un evento no deseable. Esto ayuda a cambiar las acciones que propiciaron las incidencias.
"La capacitación en la metodología" es un punto más profundo, porque es	Para este apartado es indispensable recomendar criterios que se derivan	En este componente se debe tener en cuenta la especificidad en términos

claro que el equipo interdisciplinario debe capacitarse para poder analizar ahora los riesgos de seguridad; sin embargo, dicho equipo debe estar integrado por alguno de los integrantes del proyecto MSPI, para tener un contexto organizacional en todos los aspectos del desarrollo del MSPI (MinTIC, 2019).	de la periodicidad que existe dentro de las políticas, metas, objetivos de la entidad y de las partes interesadas. Para ello se deberían considerar los siguientes aspectos: ● Criterios del negocio. ● Aspectos legales y reglamentarios. ● Operaciones. ● Tecnología. ● Finanzas. ● Factores sociales y humanitarios.	del grado de daño o de los costos para la entidad, originados por un evento de seguridad de la información, considerando los siguientes aspectos (MinTIC, 2019):. ● Nivel de clasificación de los activos de información del proceso. ● Brechas en la seguridad de la información (ejemplo: pérdida de confidencialidad, integridad y disponibilidad de la información). ● Operaciones deterioradas. ● Pérdida del negocio y del valor financiero. ● Alteración de planes y fechas límites. ● Daños para la reputación. ● Incumplimiento de los requisitos legales.

Fuente: elaboración propia.

Norma ISO/IEC 27000

> ISO/IEC 27000 es conocida como una de serie de procesos, la cual se desarrolla y es publicada por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) para facilitar un marco reconocido de forma mundial a las prácticas de gestión de la seguridad de la información. (ISO/IEC 27000).

A continuación, se realizará para este trabajo de grado una lista de las normas que hacen referencia a la seguridad de la información y se explicará brevemente de qué trata cada una de ellas.

1. ISO/IEC 27002 - En un código de buenas prácticas para la gestión de seguridad de la información.

2. ISO/IEC 27003 - Son directrices para la implementación de un SGSI.

3. ISO/IEC 27004 - Son métricas para la gestión de seguridad de la información.

4. ISO/IEC 27005 - Trata la gestión de riesgos en seguridad de la información.

5. ISO/IEC 27006:2007 - Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información.

6. ISO/IEC 27007 - Es una guía para auditar el SGSI.

7. ISO/IEC 27799:2008 - Es una guía para implementar ISO/IEC 27002 en la industria de la salud.

8. ISO/IEC 27035:2011 - Técnicas de seguridad - Gestión de incidentes de seguridad: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades. Estas normas fueron tomadas de (ISO 27001:2013).

ISO 27001:2013 define el SGSI como:

> Un (sistema de gestión para la seguridad de la información). Y se compone de una serie de procesos para implementar, mantener y mejorar de forma continua la seguridad de la información tomando como base los riesgos que afectan a la seguridad de la información en una empresa u organización. (ISO 27001:2013)

La norma resalta las buenas prácticas que se deben aplicar dentro de las organizaciones.

- **¿Por qué usar un modelo de la serie ISO/IEC 27000?**

Para garantizar la seguridad de la información en las organizaciones. Con el continuo progresivo y adelanto de las tecnologías de la información, es necesario que las entidades protejan sus activos de datos críticos, y de esta forma avalar la confianza continua de los clientes, y los socios.

Las organizaciones que incluyen sus prácticas de seguridad de la información con un estándar de la serie ISO 27000 pueden:

● Asegurar sus activos críticos.

● Administrar los riesgos de forma mucho más efectiva.

● Mejorar y mantener la confianza del cliente.

● Demostrar conformidad con las mejores prácticas internacionales.

● Evitar daños de marca, pérdida de ganancias o posibles multas regulatorias.

● Desarrollar su postura de seguridad de la información junto con los desarrollos tecnológicos. (ISO/IEC 27000).

La norma ISO 27000 tiene un amplio reconocimiento en las organizaciones, por lo que no importa el tamaño de la empresa o el sector donde se mueve. Dado que las tecnologías crecen constantemente, es necesario llevar a cabo nuevos modelos y de esta manera poder abordar cambios continuos en el área de seguridad de la información.

- **Criticidad del riesgo, norma ISO 27000:**

Se deben evaluar las consecuencias potenciales para evidenciar el tipo de riesgo: riesgo aceptable o riesgo residual.

Riesgo aceptable: se recomienda reducir su posibilidad de ocurrencia y minimizar las consecuencias a niveles que la organización pueda asumir, en los aspectos económico, logístico, de imagen, de credibilidad, etc.

• **Riesgo residual:** son las posibilidades de que ocurra un incidente, pese a verse implantado con eficacia las medidas evaluadoras y correctoras para mitigar el riesgo en el en SGSI.

• **La implementación de controles, norma ISO 27000.**

Con el objetivo de que cada riesgo identificado previamente quede cubierto y pueda ser auditable, la norma ISO 27001 establece en su última versión (ISO/IEC 27001:2013):

• Políticas de seguridad de la información.

• Controles operacionales.

• **Formas de afrontar el riesgo, norma ISO 27000:**

Una organización puede enfrentar un riesgo de tres formas diferentes: eliminarlo, mitigarlo o trasladarlo.

Eliminación: es el peligro que afecta a la continuidad de la organización; esta posibilidad procura que haya cero amenazas y evita que se vuelva a producir algún evento dentro de la entidad.

Mitigación: según la norma ISO/IEC 27001:2013, “no es posible llegar a la eliminación total del riesgo, ya sea porque es imposible técnicamente o bien porque la empresa decida que no es un riesgo suficientemente crítico. En estos casos, la organización puede aceptar el riesgo, ser consciente de que la amenaza para la información existe y dedicarse a monitorearlo con el fin de controlarlo”.

Traslado: este riesgo está relacionado con la contratación de algún tipo de seguro que compense las consecuencias económicas de una pérdida o deterioro de la información.

- **El modelo COBIT:**

Control Objectives for Information and related Technology (COBIT) es el marco aceptado internacionalmente sobre buenas prácticas para el control de la información, TI y los riesgos que conllevan. COBIT se usa para implementar el gobierno de TI y mejorar los controles de TI. De igual manera, contiene objetivos de control, directrices de aseguramiento, mediciones de desempeño y resultados, factores críticos de éxito y modelos de madurez.

- **Dónde se aplica el modelo COBIT:**

Se aplica a los sistemas de información de toda la empresa, que abarcan los computadores personales y las redes, los cuales se administran por medio de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

- **La estructura del modelo COBIT:**

Es el conjunto de lineamientos y estándares internacionales conocidos como COBIT, que define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro *dominios* principales, a saber:

- Planificación y organización.

- Adquisición e implantación.

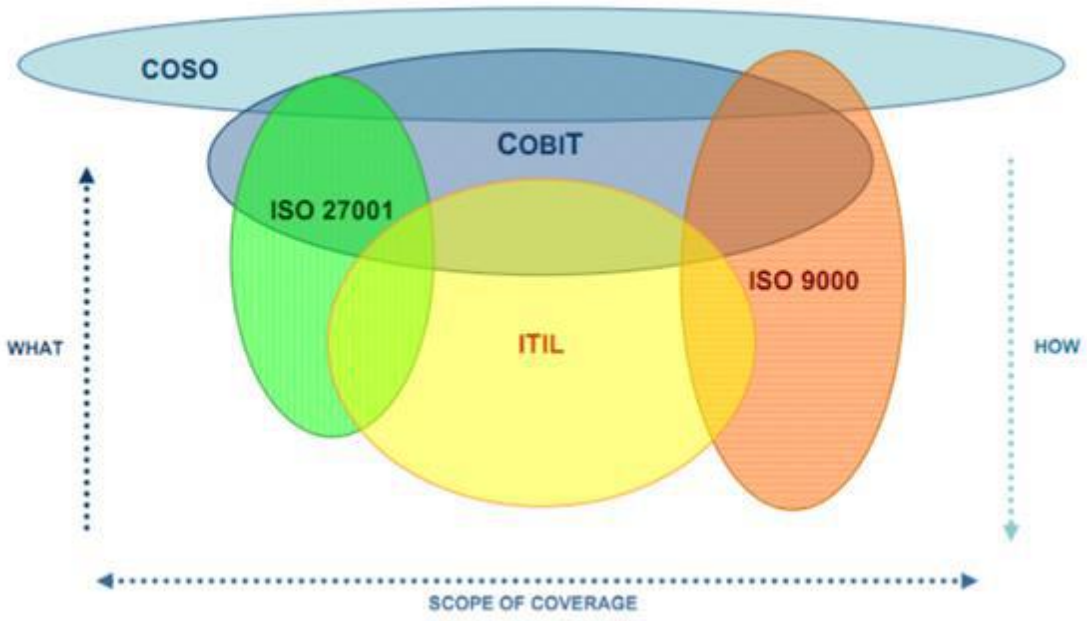
- Soporte y servicios.

- Monitoreo.

Los objetivos de control cubren los aspectos de información y facilitan que la reproducción y procesamiento de la información cumpla con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. Asimismo, se deben tener en cuenta los recursos que proporciona la TI, tales como datos, sistemas de aplicación, tecnología (plataformas), instalaciones y el recurso humano.

La figura 11 visualiza la relación entre el COBIT y las otras normas que atañen al Sistema de Gestión de Riesgos.

Figura 11. Relación del COBIT con otras normas



Fuente: Vargas y Castro (s. f.).

Para finalizar, se realiza un cuadro comparativo describiendo lo más importante de la norma ISO/IEC 27000 (tabla 5).

Tabla 5. Resumen de la norma ISO/IEC 27000

Para qué sirve la norma ISO/IEC 27000	**Descripción de la norma ISO/IEC 27000**	**Componentes de la norma ISO/IEC 27000**
El pilar de la serie ISO 27000 es ISO 27001:2013, que establece todos los requisitos contra los cuales se puede auditar y certificar el Sistema de Gestión de Seguridad de la Información. Todos los otros estándares ISO 27000 son código de prácticas no interactivos, que	Se creó garantizar la seguridad de la información en las organizaciones. Con el progresivo avance de las tecnologías de la información, es necesario que las entidades protejan sus activos de información críticos, y de esta forma avalar la confianza continua de los clientes y los socios.	Las organizaciones que incluyen sus prácticas de seguridad de la información con un estándar de la serie ISO 27000 pueden: ● Asegurar sus activos críticos. ● Administrar los riesgos de forma mucho más efectiva.

proporcionan pautas de mejores prácticas que las empresas pueden seguir en todo o en parte y que admiten ISO 27001 (ISO/IEC 27000).		● Mejorar y mantener la confianza del cliente. ● Demostrar conformidad con las mejores prácticas internacionales. ● Evitar daños de marca, pérdida de ganancias o posibles multas regulatorias. ● Desarrollar su postura de seguridad de la información junto con los desarrollos tecnológicos.
ISO 27001 propone un marco de gestión de la seguridad de toda la información de la empresa, incluso si es información perteneciente al propio conocimiento y experiencia de las personas. No debemos centrar la atención solamente en los sistemas informáticos, por mucho que tengan hoy en día una importancia más que relevante en el tratamiento de la información, ya que podríamos estar dejando sin proteger información que puede ser esencial para la actividad de la empresa.	La norma ISO 27000 tiene un amplio reconocimiento en las organizaciones, por lo cual no importa el tamaño de la empresa ni el sector donde se mueve. Dado que las tecnologías crecen constantemente, es necesario llevar a cabo nuevos modelos y de esta manera abordar cambios continuos en el área de seguridad de la información.	A continuación, se mencionan las normas más relevantes y que ayudan al Sistema de Gestión de Riesgos. 1. ISO/IEC 27002 - Es un código de buenas prácticas para la gestión de seguridad de la información. 2. ISO/IEC 27003 - Son directrices para la implementación de un SGSI. 3. ISO/IEC 27004 - Son métricas para la gestión de seguridad de la información. 4. ISO/IEC 27005 - Trata la gestión de riesgos en seguridad de la información. 5. ISO/IEC 27006:2007 - Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información.

		6. ISO/IEC 27007 - Es una guía para auditar el SGSI. 7. ISO/IEC 27799:2008 - Es una guía para implementar ISO/IEC 27002 en la industria de la salud. 8. ISO/IEC 27035:2011 - Técnicas de seguridad - Gestión de incidentes de seguridad: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades.
"ISO/IEC 27000 es conocida como una de serie de procesos, la cual se desarrolla y es publicada por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) para facilitar un marco reconocido de forma mundial a las prácticas de gestión de la seguridad de la información". (ISO/IEC 27000).	Con el objetivo de que cada riesgo identificado previamente quede cubierto y pueda ser auditable, la norma ISO 27001 establece en su última versión (ISO/IEC 27001:2013):	• Políticas de seguridad de la información. • Controles operacionales.

Fuente: elaboración propia.

Finalmente, se concluye que tanto las normas como las metodologías son importantes al momento de implementar un Sistema de Gestión de Riesgos en una organización. Para ello, es fundamental que desde la gerencia se creen las buenas prácticas y de esa forma involucrar a todo el personal activo de la empresa y hacer conciencia sobre la importancia de cada una de estas reglas. A su vez, es necesario llevar a cabo planes de contingencia y mejoras en la continuidad del negocio, las cuales no deben quedar solo plasmadas en un documento, sino hacerlas posibles y llegar al objetivo propuesto desde el génesis de la entidad.

A continuación, la tabla 6 es un cuadro comparativo de las normas y metodologías nombradas anteriormente:

Tabla 6. Tabla comparativa de metodologías de riesgo

Preguntas	**Norma ISO 31000: 2009**	**Metodología del COSO de riesgo**	**Metodología de gestión de riesgo del MinTIC**	**Norma ISO/IEC 27000**
Tienen controles de riesgo	X	X	X	X
Manejan análisis de riesgo	X	X	X	X
Es aplicable para todas las organizaciones (pública y privada)	X	X	X	X
Garantiza una certificación				X
Optimiza los controles y métodos de seguimiento y monitoreo	X	X	X	X
Evalúa los controles internos	X	X	X	X
Utiliza planes correctivos y preventivos	X	X	X	X
Garantiza la seguridad de la información	X	X	X	X
Es auditable	X	X	X	X
Tiene periodicidad	X	X	X	X
Hace parte de la gestión documental	X	X	X	X

Fuente: elaboración propia.

En el siguiente apartado se mostrarán las ventajas, desventajas, oportunidades, características en común y diferencias significativas, basadas en el diseño de la guía.

- **Ventajas:** al implementar las normas y metodologías nombradas anteriormente se logrará mejorar la eficiencia operativa y asimismo la gobernabilidad interna de las entidades, creando un mejor rendimiento y sostenibilidad. Por otro lado, se posibilitará la priorización de los objetivos, logrando implementar controles adecuados para su correcta gestión, con lo cual se controlará y manejará el Sistema de Gestión de Riesgos de forma adecuada en las organizaciones.

- **Desventajas:** dentro de las normas y las metodologías cabe resaltar que no todo funciona de manera adecuada; sin embargo, introducir o modificar un sistema de gestión del riesgo (SGR), lleva mucho tiempo e implica gastar un dinero que la organización debe asumir. Por otro parte, los requisitos pueden parecer difíciles de interpretar, ya que existen nuevos conceptos. Es importante resaltar que el control interno no debería tener ningún error, no obstante, puede tenerlos dados los errores humanos que ocurren debido a la desinformación o confusión durante el intercambio de los funcionarios.

- **Oportunidades:** las normas y las metodologías deberían enfocarse más a los sistemas de gestión de riesgo, o siquiera a un determinado grupo de empresa, y de esta forma lograr calcular los riesgos de información y el contenido de los datos.

- **Características en común:** dentro de este ítem cabe mencionar que todas las normas tienen un análisis FODA y todas tienen una matriz de riesgo, lo cual facilita a la organización llevar un control interno para cada área, ayudando a implementar planes correctivos y preventivos en una eventual catástrofe.

• **Diferencias significativas:** la guía de MinTIC solo aplica para Colombia, debido a que cada país tiene su guía diseñada. También se podría decir que no todas las normas y metodologías son certificables, pero sirven de referencia para otros modelos de Sistema Gestión de Riesgos.

Finalmente, se podría decir que todas las normas y metodologías nombradas anteriormente aplican en la realización de la guía que se está realizando para el objeto de estudio del CNMH, ya que hacen parte de los SGR, y el presente trabajo de grado está enfocado en este diseño.

Matriz de riesgos de la información

En este apartado se abordará una de las herramientas para la efectiva gestión de riesgos en información, ya que permite el registro de las actividades de identificación, análisis, valoración y tratamiento de los riesgos, y con ello se garantiza una adecuada gestión y supervisión de riesgos que se enmarcan en un modelo de gobierno de información.

Con la matriz de riesgos de información, la gestión del riesgo también implica la construcción de procedimientos, instructivos, manuales y demás documentos donde se pueda establecer un alcance, contexto y los criterios para la identificación, análisis, evaluación y tratamiento de los riesgos, de acuerdo con la unidad de información y la metodología que adopte, así como el seguimiento y revisión, registro e informe, comunicación y consulta de los riesgos informacionales identificados. Albanese (2012) plantea que la matriz de riesgos tiene cierto grado de dificultad:

> Su elaboración requiere dedicación y amplio conocimiento del negocio y de la normativa vigente, entre otros aspectos. Esto posibilitará la definición de factores clave para confeccionar un esquema matricial. (p. 209)

Así pues, a continuación, se establecerán los campos que debe tener una matriz de riesgos, basados en las metodologías abordadas anteriormente.

Clasificación interna para el riesgo

La identificación del riesgo requiere, en primer lugar, de un ejercicio para determinar el contexto en el que se va a identificar; es decir, el tipo de unidad de información y las dependencias, direcciones o el proceso afectado con el responsable de su gestión. A su vez, se debe identificar el sistema de gestión con el que se relaciona, la norma que impacta y el factor o fuente del riesgo (tabla 7). A continuación, se describe cada campo:

Dependencia, dirección o proceso: esto depende del organigrama de la unidad de información, siempre identificando de lo macro a lo micro la jerarquía que se tenga.

Responsable: dependencia, dirección, proceso o proyecto de la unidad en el que se identifica el riesgo y es su propietario.

Cargo responsable: cargo del líder o proyecto responsable.

Sistema: sistema de gestión al cual se puede asociar el riesgo (en caso de que haya más de un sistema asociado, se debe elegir aquel que tenga mayor relevancia para la unidad).

Norma que impacta: ley, circular, resolución, decreto o cualquier otra norma con la que se relacione el riesgo y ayude a su gestión (debe indicarse si el riesgo se asocia a más de una norma).

Factor/Fuente de riesgo: indica la parte interesada, el proceso, la ubicación geográfica o cualquier otra fuente que sea la generadora del riesgo.

Tabla 7. Clasificación interna del riesgo

CLASIFICACION INTERNA PARA EL RIESGO						
No.	**DEPENDENCIA O DIRECCIÓN**	**PROCESO RESPONSABLE**	**CARGO RESPONSABLE**	**SISTEMA**	**NORMA QUE IMPACTA**	**FACTOR DE RIESGO**
1	Dirección de Archivo de Derechos Humanos	Proceso de Procesamiento técnico	Coordinadores y Directores	Ambiental Calidad Corrupción y Sobornos Gestión Documental SARLAFT Seguridad de la Información SG-SST Todos	ISO OHSAS SGT-SST Ley 1266 de 2008 Ley 1424 de 2010 Ley 1448 de 2011 Ley 1581 de 2012 Ley 1712 de 2014	Areas geográficas Auditorias internas Victimas Comunidad DOFA Entes externos de control Estrategia Evento materializado Externos Gobierno Infraestructura Partes interesadas Personas PQR's Procesos / SGI Proveedores y contratistas Requisitos legales Servicios y productos Tecnología Trabajadores / Recurso Humano Trabajadores y su familia
2	Dirección de Archivo de Derechos Humanos	Proceso de Custodia				
3	Dirección de Archivo de Derechos Humanos	Proceso de Consulta				

Fuente: elaboración propia.

Descripción del riesgo

Consiste en identificar un evento que puede presentarse o que ya se ha materializado de acuerdo a unas condiciones, generando una causa y una consecuencia (tabla 8). Para esto es importante contar con información pertinente y actualizada de fuentes macroentorno y microentorno de la entidad.

La identificación del riesgo (figura 12) se realiza de manera sistemática, iterativa, colaborativa y permanente, mediante la aplicación de una o varias de las siguientes técnicas: lluvia de ideas, entrevistas, encuestas, juicio de expertos, DOFA, PESTEL (análisis de los factores político, económico, sociocultural, tecnológico, ecológico y legal), entre otros. Puede realizarse a nivel estratégico, táctico u operativo, y a nivel de unidad (global) de los procesos.

La identificación del riesgo requiere documentar:

- **El evento:** descripción de la situación que se presentó brevemente, se presenta o puede presentarse y si esta afecta los objetivos estratégicos de la unidad, planteando la siguiente pregunta: ¿Qué puede o podría ocurrir?

- **Causa:** circunstancia que lleva o puede llevar a la ocurrencia del evento de riesgo y está relacionada con el factor/fuente de riesgo. ¿Por qué sucede o puede suceder esto?

En su descripción en el campo es importante evitar negación.

- **Consecuencia:** se debe documentar el impacto que tiene o puede tener el evento identificado en caso de llevarse a cabo. Este impacto puede afectar a nivel económico, reputacional, legal, ambiental, la continuidad y las personas.

Figura 12. Identificación del riesgo

Fuente: elaboración propia.

Tabla 8. Descripción del riesgo

DESCRIPCION DEL RIESGO			
EVENTO	**CAUSA**	**CONSECUENCIA**	**CLASE DE RIESGO**
• La continuidad de las operaciones informáticas no se garantiza • Indisponibilidad de aplicativos únicos o de terceros • Ataque contra la información • Fuga de la información por espionaje industrial • Generar información o presentar informes inconsistentes (errados, falsos o incompletos) a los entes de control internos y/o externos • Indisponibilidad de los Correos electrónicos • Acceso no permitido, destrucción o alteración de información	• El plan de contingencia de información no se encuentra documentado, implementado, mantenido ni en proceso de mejora continua • Inexistencia de lineamientos documentados para el almacenamiento y protección de la documentación física y electrónica • Los acuerdos de servicio con el proveedor no se establecen • Elegir un proveedor que no cuente con servidores redundantes en caso que se presenten fallas • Los contratos de mantenimiento y soporte con el proveedor no se establecen ante casos de fallas en la comunicación con el aplicativo, entre otros • Inexistencia de lineamientos ante la extracción y suministro de información sensible o estratégica por parte del personal • Vulnerabilidades en los sistemas informáticos	• Afectación de la seguridad de la información (Pérdida de trazabilidad) • Afectación económica • Afectación legal y Reputacional • Afectación tecnológica • Daño del formato • Favorecimiento de actividades delictivas o de incumplimiento • Fuga de información • Perdida de continuidad en las operaciones • Perdida de información • Perdida de integridad de los datos • Personas sin autorización ingresan a información crítica • Se afecta la Confidencialidad de la información Afectación de la seguridad de la información (Captura, Procesamiento, Disponibilidad, integridad o confidencialidad)	Ambiental Continuidad Cumplimiento Gestión de la información Económico Estratégico Financiación del Terrorismo Lavado de Activos Operativo Personas Reputacional Seguridad de la Información Terrorismo TIC

Fuente: elaboración propia.

Valoración del riesgo inherente

La valoración del riesgo inherente consiste en comparar los resultados del análisis o clasificación del riesgo sin controles con los criterios establecidos para determinar la probabilidad de ocurrencia y su impacto (tabla 9).

La probabilidad de ocurrencia está asociada a la frecuencia con que se presentó o se puede presentar un evento de riesgo. Esta probabilidad debe calificarse como casi cierto, probable, posible, ocasional o raro, según la escala de lineamientos de la NTC ISO 31000.

El impacto se determina como el efecto del evento de riesgo frente a los siguientes factores: personas, económico, reputacional, legal, ambiental, gestión documental y continuidad. Se califica como crítico, mayor, moderado, menor o bajo.

El nivel de riesgo indica el nivel de severidad del riesgo inherente (que no tiene en cuenta los controles existentes). Es el resultado de multiplicar la calificación asignada a la probabilidad con la calificación asignada al impacto:

Nivel de riesgo = Probabilidad x Impacto

Así pues, el nivel de riesgo resultante se calcula de forma automática y puede ser: Riesgo Extremo, Riesgo Alto, Riesgo Moderado y Riesgo Bajo.

Tabla 9. Evaluación del riesgo inherente

EVALUACIÓN DEL RIESGO INHERENTE		
PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
Casi Cierto Probable Posible Ocasional Raro	Crítico Mayor Moderado Menor Bajo	Riesgo Extremo Riesgo Alto Riesgo Moderado Riesgo Bajo

Fuente: elaboración propia.

Controles

Los controles internos son la mejor forma de tratamiento de los riesgos y son actividades que buscan disminuir (mitigar) la probabilidad de ocurrencia del evento de riesgo en cualquier tipo de escenario que sea planteado. Estas actividades se aplican para los riesgos inherentes (tabla 10).

Los controles se indican de la siguiente manera:

Descripción: actividad o acción que actualmente se realiza para solucionar o tratar la causa del evento de riesgo inherente; se sugiere describir la actividad con un verbo en infinitivo: verificar, comparar, conciliar, revisar, reportar, entre otros.

Responsable del control: cargo(s) responsable(s) de la ejecución del control redactado.

Documentado en: el control debe tener una gestión de conocimiento, es decir, se documenta en una política, un manual, un procedimiento, un instructivo o documento que se encuentre vigente en un sistema documental de la unidad.

Evaluación: se determina la efectividad del control frente a la causa que origina el evento de riesgo inherente.

Para evaluar el control, se definen cuatro variables para la forma en que opera, su oportunidad en aplicación, su seguimiento y su estado. El resultado es la combinación de estas variables. El control puede clasificarse en las siguientes categorías: fuerte, moderado o débil.

Tabla 10. Controles

CONTROLES			
DESCRIPCION	RESPONSABLE DEL CONTROL	DOCUMENTADO EN	EVALUACION
Contratos Datos Documento Especifico Formato Instructivo Manual Matriz de Riesgos No documentado Política Póliza	Coordinadores y Directores	Contratos Datos Documento Especifico Formato Instructivo Manual Matriz de Riesgos No documentado Política Póliza	Casi cierto Probable Posible Ocasional Raro

Fuente: elaboración propia.

Nivel del riesgo residual

El riesgo residual es el resultado de aplicar la evaluación del control al nivel de riesgo inherente. El control evaluado afecta la probabilidad de ocurrencia del evento de riesgo inherente, es decir, valor del control x valor de la probabilidad, cuyo resultado se multiplica por el valor del impacto (tabla 11). Es una operación matemática que se realiza de forma automática en la matriz.

Al evaluar el control sobre el riesgo inherente se puede disminuir la criticidad del riesgo. Asimismo, el resultado de la evaluación del riesgo residual puede conducir a que no se tome ninguna acción adicional o considerar opciones para su tratamiento. Por eso, un análisis detenido

del nivel de riesgo residual ayuda a comprender mejor el riesgo y mantener los controles existentes o reconsiderar complementarlos.

Tabla 11. Riesgo residual

Fuente: elaboración propia.

Tratamiento del riesgo

El tratamiento de los riesgos se realiza bajo indicadores determinados (tabla 12). Por ejemplo, cuando el nivel de riesgo residual sea “Riesgo Bajo”, no será necesario establecer una opción de tratamiento, pero si el nivel es diferente de “Riesgo Bajo”, será necesario efectuar tratamiento

adicional y esta actividad deberá documentarse en un procedimiento o en un sistema de gestión de calidad que tenga la unidad.

El tratamiento del riesgo se puede definir como la acción o actividad que se va a implementar para mitigar el nivel de riesgo residual. En el campo se indicará una de las siguientes opciones: evitar, reducir, compartir y asumir/aceptar.

En el campo de descripción se redacta de forma detallada la actividad o la acción que se va a realizar para mitigar el nivel de riesgo residual.

En el campo documentado, la actividad para el tratamiento se documenta en una política, un manual, un procedimiento o un instructivo.

En el cargo responsable se indica el(los) cargo(s) responsable(s) de la ejecución de la actividad de tratamiento descrita.

Finalmente, en la fecha de ejecución y periodicidad de ejecución se indica el día, mes y año que se tiene proyectado iniciar la ejecución de la actividad de tratamiento descrita y se establece una frecuencia para su ejecución: diaria, semanal, mensual, bimestral, trimestral, semestral, anual o cada vez que se requiera.

Tabla 12. Tratamiento del riesgo

TRATAMIENTO DEL RIESGO					
TRATAMIENTO DEL RIESGO	**DESCRIPCION**	**DOCUMENTADO EN**	**CARGO RESPONSABLE**	**FECHA DE EJECUCIÓN**	**PERIODICIDAD DE EJECUCIÓN**
Evitar el riesgo Reducir el riesgo Compartir el riesgo Asumir / aceptar el riesgo	• Evaluar del acceso de personal • Verificar su nivel de seguridad • Asegurar el cumplimiento del plan anual de capacitación • Implementar buenas prácticas • Establecer contratos de mantenimiento y acuerdos de servicio • Seguir planes de acción y cierre de brechas resultantes de las auditorias • Establecer perfiles de segmentación • Implementar metodologías de seguridad • Ejecutar Plan de Contingencia	Contratos Datos Documento Especifico Formato Instructivo Manual Matriz de Riesgos No documentado Política Póliza	Coordinadores y Directores	Fecha del Tratamiento	Diario Semanal Quincenal Mensual Bimestral Trimestral Semestral Anual Cada vez que se requiera

Fuente: elaboración propia.

Metodología de análisis de riesgo en el marco de la gobernanza de información

Identificación de la Información que maneja la unidad de información

Identificar la información o cualquier elemento relacionado con su tratamiento, en cualquier medio, sea digital o análogo, y su valoración en términos de acceso, confidencialidad y criticidad. Estos objetos de información se registran en la matriz de riesgos de información.

- **Instrumento de análisis de información basado en riesgos: Matriz de riesgos de información:**

Para identificar los objetos de información, los insumos son: las entradas y salidas en los flujos de información, inventarios documentales o colecciones, tablas de retención documental, sistemas de información u otros.

Clasificación de la información

Se clasifica la información teniendo como principio la confidencialidad, y según su restricción de acceso se identificará la clase a la que pertenece el objeto de información, sea esta información pública, semipública, reservada o sensible.

Calificación de la información

Los criterios para calificar los objetos de información se realizan por medio de las entrevistas a funcionarios de las direcciones, procesos, dependencias o como esté estructurada la unidad de información. Esta calificación tiene como variables la captura, el procesamiento, las entradas, las salidas, la confidencialidad, la integridad y la disponibilidad de la información, las cuales tienen rangos de valoración cuantitativa representados en la matriz, definidos y sujetos al impacto que puede perder cada uno de estos criterios.

El propietario o encargado del objeto define la criticidad, asignando los valores correspondientes. Cada uno tiene cuatro niveles de calificación de 0 a 3, siendo 3 el nivel más alto y 0 el más bajo. A partir de allí se pueden identificar los riesgos inherentes y determinar los riesgos residuales, y basado en esto atar los controles.

Valoración de la información

La calificación de cada uno de los criterios se obtiene de la sumatoria para valorar el objeto de información. Dependiendo de su resultado, se asigna el nivel de criticidad para la organización en términos de la captura, el procesamiento, las entradas, las salidas, la confidencialidad, la integridad y la disponibilidad de la información, a fin de proteger los objetos de información, tener el control y determinar los tipos de riesgos.

- **Rangos de valoración:**

• Muy baja: Valores de clasificación de 0 y 1

• Baja: Valores de clasificación de 2 y 3

• Media: Valores de clasificación de 4 y 5

• Alta: Valores de clasificación de 6 y 7

• Muy Alta: Valores de clasificación de 8 y 9

Periodicidad de la revisión de la matriz de riesgo de la información

Se realiza la verificación para determinar si un objeto de información sigue o no siendo parte del inventario, o si la valoración asignada en el inventario y clasificación de los objetos de información deben ser modificados.

Para ser revisados y validados los objetos en cualquier momento, el propietario de la información deberá ser autorizado y conocer la información específicamente, y así poder añadir, actualizar o eliminar los objetos.

Las razones por las cuales debería realizarse una revisión o validación son:

• Actualizaciones al proceso al que pertenecen los objetos.

• Adición de actividades al proceso.

• Inclusión de nuevos registros de calidad, nuevos procesos y procedimientos.

• Inclusión de nuevos objetos.

• Eliminación de una dirección, proceso, dependencia o como esté estructurada la unidad de información o cargo en la entidad, que tenía asignado el rol de propietario o custodio (cambios organizacionales).

• Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados.

• Cambios físicos de la ubicación de los objetos de información.

Sin embargo, para la revisión o actualización del inventario de objetivos de información se establecerá como periodicidad mínima una vez al año.

Este documento presenta una guía para realizar inventario y clasificación de los objetos de información, que son manejados por las unidades de información a través de los procesos, con el

fin de determinar qué objetos de información tiene la unidad, para poder determinar su clasificación y valoración frente a los criterios de captura, procesamiento, entradas, salidas, confidencialidad, integridad y disponibilidad de la información.

De esta manera y con base en lo establecido en la norma técnica NTC ISO/IEC 27001:2013 en el dominio Gestión de Activos y de acuerdo con la Ley 1712 de 2014, la Ley 1581 de 2012 y la NTC ISO 31000:2018, se definieron los siguientes tipos de objetos:

Información análoga, Información digital, Información electrónica, Información análoga/Información digital y/o Electrónica, *Software*, *Hardware*, Servicios y usuarios.

Conclusiones

Tal como se pudo comprobar, la identificación de los flujos de información en la unidad es la parte inicial para la gestión de riesgos de información, ya que es el primer insumo para establecer los objetos de información, sus entradas, procesos y salidas, y de esta forma analizar los posibles riesgos que estos pueden llegar a presentar.

Tras el análisis de las metodologías y normas para la gestión de riesgos, podemos deducir que estas ofrecen lineamientos generales que se adaptan a las diferentes organizaciones para realizar la gestión de riesgos de forma general, hasta llegar a consolidar un sistema de forma específica, por medio de una metodología propia de la entidad basada en sus necesidades y cumplimientos normativos que le apliquen.

Cuando se elabora una matriz de riesgos y en este caso enfocada en la información como objeto, conocer la unidad de información es fundamental para mapear los posibles riesgos que se pueden materializar por medio de los eventos, con lo cual se puede llegar a mitigarlos y controlarlos.

Asimismo, fue muy acertado para el estudio entrevistar a los dueños de la información, quienes interactúan a diario con los datos, pues ellos son fuentes primarias que van estructurando la matriz, hasta llegar a tener la herramienta totalmente gestionada, teniendo siempre como base que la gestión de riesgos no es estática sino dinámica, y depende de muchos factores que hacen que todo cambie.

Actualmente, la gestión de riesgos se aborda desde una mirada holística para todas las organizaciones, pero diseñar una guía enfocada en la gestión de riesgos de información hace que la identificación de los riesgos y sus componentes sea más específica y aborde como tal la

información, sin dejar atrás los medios tecnológicos. Ello genera un valor estratégico en la entidad, que se considera un activo intangible que debe ser protegido, ya que hace parte de la gestión del conocimiento y lo que constituye la unidad de la corporación.

Durante la investigación realizada en este trabajo de grado, tomando como objeto el CNMH y su DADH, se puedo evidenciar que la información y los datos que componen la organización son parte de la gestión de riesgos y, a su vez, la acompañan con la seguridad de la información dos factores de riesgo que se valoran y controlan por separado. Cabe resaltar que al fortalecer la gestión del riesgo de información se genera una gobernanza de la información, pudiendo así identificar sus objetos de información y otorgándole a cada uno un valor para salvaguardarlo. Por supuesto, esto se da por medio de la colaboración de los colaboradores como equipo y su apropiación del conocimiento de la entidad, ya que finalmente son los que manejan y custodian la información.

Dentro del análisis expuesto para los riesgos de información, se definió que conocer qué tipo de entidad, corporación o unidad es la que se está analizando nos muestra las necesidades que esta tiene frente al manejo de su información. Asimismo, que consideran ellos como información los tipos de información frente al soporte que tiene, el tipo de contenido y su función en la unidad, para darle un valor y clasificación a la información, donde uno de los insumos es la gestión documental que tiene la unidad, lo cual establece los inicios de una gobernanza de su información y la posterior adaptación de una mejor metodología de riesgo que satisfaga su apetito de riesgo y tolerancia.

Finalmente, en el desarrollo de la investigación se lograron los objetivos de identificar los flujos de información, con ayuda de los colaboradores del CNMH, por medio de las herramientas propuestas (la entrevista y el inventario básico). De este modo, se seleccionaron las metodologías

y normas que cubrían las necesidades informacionales para la gestión de riesgos, que fueron proyectadas en una matriz de riesgos, dando alcance para la identificaron de unos riesgos generales de información y los escenarios que la unidad maneja. Ello nos ayudó a generar un producto guía para el desarrollo de una metodología propia para el análisis de riesgos, en un marco de gobernanza de información, que puede convertirse en un referente para otras unidades de información.

Recomendaciones

- Tener en cuenta que la gestión de riesgos de información no estática, sino dinámica, debido al constante cambio en la información, la forma como esta se consume y sus diferentes públicos objetivos, donde se deben contemplar la mayor cantidad de eventos posibles que se pueden materializar, para así plantear los riesgos y sus controles.
- Se recomienda una periodicidad anual en la revisión, actualización, inclusión y eliminación de los riesgos mapeados en la matriz, ya que así se pueden identificar cambios significativos.
- Las metodologías y normas se deben analizar desde las necesidades de protección de la unidad y estas se pueden combinar, cubriendo dichas necesidades con miras a las buenas prácticas y los cumplimientos normativos.

Referencias

Aja, L. (2002). Gestión de información, gestión del conocimiento y gestión de la calidad en las organizaciones. *Acimed, 10*(5), 36-41. http://eprints.rclis.org/5135/1/gestion.pdf

Albanese, D. E. (2012). Análisis y evaluación de riesgos: aplicación de una matriz de riesgo en el marco de un plan de prevención contra el lavado de activos. *Revista Base, 9*(3), 206-215. https://www.redalyc.org/pdf/3372/337228651001.pdf

Areitio, B. (2008). *Seguridad de la información, redes, informática y sistemas de información*. Cengage Learning Paraninfo.

Baque, J. V. (2013). *Diseño de un manual de control interno y flujograma de procesos aplicado al Departamento de Auditoría Interna de Camaronera Lebama S. A.* [Tesis de grado], Universidad Laica Vicente Rocafuerte de Guayaquil. http://repositorio.ulvr.edu.ec/bitstream/44000/202/1/T-ULVR-0188.pdf

Bautista, M. (2014). *Marco de referencia para la formulación de un plan de continuidad de negocio para TI, un caso de estudio*. Corporación Centro Nacional de Control de Energía (Cenace).

Cárdenas, D. X., Wilches, A. M, Peñate, Y., & Lozada, D. (2018). La gestión documental en la Universidad de Guayaquil: situación actual y retos futuros. *Revista Espacios*, *39*(43), 10. http://www.revistaespacios.com/a18v39n43/18394310.html

Centro Nacional de Memoria Histórica (CNMH). (2017a). *Política pública de archivos de derechos humanos, memoria histórica y conflicto armado*. CNMH.

http://www.centrodememoriahistorica.gov.co/descargas/politica-publica-archivo-ddhh.pdf

Centro Nacional de Memoria Histórica (CNMH). (2017b). *Protocolo de gestión documental*. https://centrodememoriahistorica.gov.co/protocolo-de-gestion-documental

Cerrillo, A. (2005). *La gobernanza hoy: 10 textos de referencia*. Instituto Nacional de Administración Pública de Madrid. https://www.ucipfg.com/Repositorio/MGTS/MGTS15/MGTSV15-06/semana1/obligatorio/Lagobernanzahoy-INAP.pdf

Chiavenato, I. (2009). *Administración de recursos humanos. El capital humano de las organizaciones*. McGraw-Hill. https://www.sijufor.org/uploads/1/2/0/5/120589378/administracion_de_recursos_humanos_-_chiavenato.pdf

Congreso de Colombia. (2008, 3 de diciembre). Ley 1266 de 2008. *Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones*. DO: 47.219.

Congreso de Colombia. (2012, 17 de octubre). Ley 1581 de 2012. *Por la cual se dictan disposiciones generales para la protección de datos personales*. DO: 48.587.

Congreso de Colombia. (2014, 6 de marzo). Ley 1712 de 2014. *Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones*. DO: 49.084.

Corona, J. L., & Maldonado, J. M. (2018). Investigación Cualitativa: Enfoque Emic-Etic. *Revista Cubana de Investigaciones Biomédicas*, *37*(4).

Daltabiut, E., Hernández, L., Mallén, G., & Vázquez, J. (2009). *La seguridad de la información*. Limusa Noriega Editores.

De Abreu, F., Gastaud, A. C., & Kumar, K. (2017). Modelo estrutural de governança da informação para bancos. *RAE: Revista de Administração de Empresas*, *57*(1), 79-95. https://doi-org.ezproxy.javeriana.edu.co/10.1590/S0034-759020170107

Deloitte. (2015). COSO Marco de referencia para la implementación, gestión y control de un adecuado Sistema de Control Interno. https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/COSO-Sesion1.pdf

Ealde Business School. (2020, 23 de julio). ¿Qué es el marco COSO de Gestión de Riesgos y cómo surge? https://www.ealde.es/marco-coso-riesgos/

Eito-Brun, R., & Calleja-Aliaga, C. (2020). La gestión documental en los modelos de gobernanza TIC: presencia y visibilidad de la normativa internacional en el modelo de referencia COBIT. *Revista Española de Documentación Científica*, *43*(3), e272. https://doi.org/10.3989/redc.2020.3.1666Instituto Colombiano de Normas Técnicas y

Certificación (Icontec). (2013a). Norma NTC/ISO 27001:2013. *Requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI)*.

Estupiñán, R. (2006). *Control interno y fraudes. Análisis de Informe COSO I, II y III con base en los ciclos transaccionales*. Ecoe.

Gallego, J., & Juncà, M. (2009). *Fonts d'informació I*. http://hdl.handle.net/10609/242

García-Morales, E. (2012). Gobernanza de la información. *Anuario ThinkEPI*, *6*, 100-103 https://core.ac.uk/download/pdf/296528653.pdf

García-Morales, E. (2013). Gestión del ciclo de vida de datos y documentos: acercando posiciones. *Anuario ThinkEPI*, *7*, 98-100. http://www.thinkepi.net/gestion-ciclo-vida-datos-documentos-acercando-posiciones

González, I., Cruzata, C. M., & Medina, V. (2017). Una contribución a la gestión de la información de ciencia, tecnología e innovación. *Revista Vivat Academia*, *140*(20), 55-63. http://www.vivatacademia.net/index.php/vivat/article/view/1022

Guerrero-Aguiar, M., Medina-León, A., & Nogueira-Rivera, D. (2020). Procedimiento de gestión de riesgos como apoyo a la toma de decisiones. *Ingeniería Industrial*, *41*(1), e4101. https://www.redalyc.org/journal/3604/360464918007/html/

Hernández-Sampieri, R. (s. f.). *Recolección de datos cuantitativos*. https://bit.ly/3ktLOPX

Instituto Colombiano de Normas Técnicas y Certificación (Icontec). (2013b). Norma NTC/ISO 27002:2013. *Técnicas de Seguridad. Código de práctica para controles de seguridad de la información*.

Instituto Distrital de Gestión de Riesgos y Cambio Climático (Idiger). (2018). *Política de Gobierno de Datos, Documento TIC Versión 1*. https://www.idiger.gov.co/documents/20182/325216/Pol%C3%ADtica+de+Gobierno+de+Datos.pdf/9f471d05-f8b8-41b5-bed9-91950da1e83d

International Organization for Standardization (ISO). (2005). ISO 27001. https://normaiso27001.es/referencias-normativas-iso-27000/

International Organization for Standardization (ISO). (2009). *Norma ISO 31000: el valor de la gestión de riesgos en las organizaciones*. Isotools Excellence. https://www.isotools.org/pdfs-pro/ebook-iso-31000-gestion-riesgos-organizaciones.pdf

International Organization for Standardization (ISO). (2012). ISO 22301 Sistemas de gestión de continuidad de negocio.

Kuhn, T. (1995). *La estructura de las revoluciones científicas* (Trad. A. Contín). Fondo de Cultura Económica.

Martelo, R. J., Madera, J. E., & Betín, A. D. (2015). Software para gestión documental, un componente modular del Sistema de Gestión de Seguridad de la Información (SGSI). *Revista Información Tecnológica*, *26*(2), 129-134. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642015000200015

Martínez, C. (2012). La ciencia de la información como plataforma para potenciar el estudio de los flujos de la información en las organizaciones. *Revista e-Ciencias de la Información*, *2*(1), 1-14. https://www.redalyc.org/artículo.oa?id=476848735002

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2018). *Guía de gestión de riesgos. Seguridad y privacidad de la información. Guía Nº 7*. https://mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2019). *G.INF.06 Guía Técnica de Información - Gobierno del dato*. https://www.mintic.gov.co/arquitecturati/630/articles-9258_recurso_pdf.pdf

Opendatasoft. (2018, 18 de junio). *¿Qué es la gobernanza de los datos?* https://www.opendatasoft.com/es/blog/2018/06/28/que-es-la-gobernanza-de-los-datos

Oriol, J. (2003). El concepto y el análisis de la gobernabilidad. *Revista Instituciones y Desarrollo*, *14-15*, 239-269. https://www.ses.unam.mx/docencia/2007II/Lecturas/Mod3_Oriol.pdf

Paternina, R. A. (2018). *Estudio de vulnerabilidades en el proceso de cadena de custodia de evidencias en delitos informáticos en la ciudad de Cartagena* [Tesis de especialización], Universidad Nacional Abierta y a Distancia (UNAD). https://repository.unad.edu.co/handle/10596/28400

Policía Nacional. (2020). *Tendencias cibercrimen Colombia 2019-2020*. https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

Portafolio. (2021, 23 de febrero). Colombia perdió 509.370 micronegocios por la crisis. https://www.portafolio.co/negocios/colombia-perdio-509-370-micro-por-la-crisis-segun-dane-549417

Pérez, S. S., Cruz, D., & Piedra, V. M. (2015). El Enterprise Risk Management (ERM) para la evaluación de riesgos estratégicos en microempresas comerciales hidalguenses. *Acta Universitaria*, *24*, 95-104. http://www.actauniversitaria.ugto.mx/index.php/acta/article/view/713

Pomim, M. L. (2009). Ambientes y flujos de información en contextos empresariales. *Revista Ibersid*, 3, 55-60. https://www.ibersid.eu/ojs/index.php/ibersid/article/view/3722/3483

Ponjuán, G, & Torres, D. (2020). La otra cara de la información: la desinformación y la información imprecisa como retos para la gestión de la información institucional. *Revista Cubana de Información en Ciencias de la Salud*, *31*(2), e1575. https://www.redalyc.org/jatsRepo/3776/377665620003/html/

Rodríguez, N. P., & Sánchez, M. (2017). *Plan de mejoramiento Departamento de Droguería Almacenes La 14 S. A., orientado a la gestión de inventarios, operador logístico Comfandi de la ciudad* [Tesis de grado], Fundación Universitaria Católica Lumen Gentium.

https://repository.unicatolica.edu.co/bitstream/handle/20.500.12237/445/FUCLG0016610.pdf?sequence=1&isAllowed=y

Rivero, S., Díaz, M., López-Huertas, M. J., & Rodriguez, R. J. (2017). *Instrumento para la medición de la ciencia y la tecnología en la gestión de la información institucional: caso de estudio*. http://sedici.unlp.edu.ar/handle/10915/63378

Sabino, C. (1992). *El proceso de investigación*. Panapo. http://paginas.ufm.edu/sabino/ingles/book/proceso_investigacion.pdf

Servicio Geológico Colombiano. (2017). *Políticas de gestión de la información geocientífica, Código: DG-GGC-10 Versión 2*. https://www2.sgc.gov.co/sgc/mapas/Documents/PDF%20POL%C3%8DTICAS/politicas-gestion-informacion-dgi0.pdf

Soler-Gonzalez, R., Varela-Lorenzo, P., Oñate-Andino, A., & Naranjo-Silva, E. (2018). La gestión de riesgo: el ausente recurrente de la administración de empresas // Risk management: the recurrent absence of business administration. *Ciencia Unemi*, *11*(26), 51-62. https://doi.org/10.29076/issn.2528-7737vol11iss26.2018pp51-62p

Talend. (s. f.). *¿Qué es la gobernanza de datos? ¿La necesito?* https://www.talend.com/es/resources/what-is-data-governance/

Temesio, S. (2019). La gobernanza de la información en las organizaciones. *Páginas a&b*, *3*(11), 34-54. https://doi.org/10.21747/21836671/pag11a4

Tobar, J. E., Tobar, G. W., & Santos, R. C. (2018). Seguridad de la información y matriz de riesgo enfocado en el plan estratégico: caso Laboratorios Luque S. A. *Revista Contribuciones a las Ciencias Sociales* [en línea]. http://www.eumed.net/rev/cccss/2018/01/matriz-riesgo-laboratoriosluquesa.html

Torres, M., Paz, K., & Salazar, F. (s. f.). *Métodos de recolección de datos para una investigación*. https://fgsalazar.net/LANDIVAR/ING-PRIMERO/boletin03/URL_03_BAS01.pdf

Universidad Eafit (s. f.). *COBIT: Modelo para auditoría y control de sistemas de información*. https://www.eafit.edu. co/escuelas/administracion/consultorio-contable/Documents/A%20COBIT.pdf

Valenzuela, L. A., Collantes, Z. M., & Durand, E. E. (2020). Sobre la gobernanza digital, política digital y educación. *Revista Eleuthera*, *22*(2), 88-103. http://www.scielo.org.co/scielo.php?pid=S2011-45322020000200088&script=sci_abstract&tlng=es

Vargas, A. C., & Castro, A. (s. f.). *Sistemas de gestión de seguridad de la información*. http://archivo.ucr.ac.cr/docum/ISOEIC27000.pdf

Whittingham, M. V. (2010). ¿Qué es la gobernanza y para qué sirve? *Revista Análisis Internacional*, *2*, 219-235. https://revistas.utadeo.edu.co/index.php/RAI/article/view/24/26

Anexos

A. Banco de preguntas

B. Entrevista

C. Infografía

D. Matriz de riesgos de información