PROPUESTA METODOLÓGICA PARA LA ADMINISTRACIÓN DEL RIESGO EN LAS INSTITUCIONES EDUCATIVAS PÚBLICAS DEL DEPARTAMENTO DEL ATLÁNTICO SOPORTADA EN LAS TIC

INGENIERA DALGYS ARENAS BUSTAMANTE

UNIVERSIDAD DE LA COSTA – CUC

MAESTRÍA EN GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

MODALIDAD INVESTIGATIVA

BARRANQUILLA

2020

PROPUESTA METODOLÓGICA PARA LA ADMINISTRACIÓN DEL RIESGO EN LAS INSTITUCIONES EDUCATIVAS PÚBLICAS DEL DEPARTAMENTO DEL ATLÁNTICO SOPORTADA EN LAS TIC

Ingeniera Dalgys Arenas Bustamante

Trabajo para optar al título de magíster en gestión de las tecnologías de la información

Mg. Fabio Enrique Mendoza Palechor Tutor

Mg. Zhoe Comas González Cotutor

UNIVERSIDAD DE LA COSTA – CUC

MAESTRÍA EN GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

MODALIDAD INVESTIGATIVA

BARRANQUILLA

2020

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

_____

Firma de jurado

_____

Firma de jurado

Barranquilla 2020

Agradecimientos

A Dios por siempre acompañarme.

A mi familia por apoyarme en este proceso.

A mis tutores: Ing. Gloria Jaramillo Rojas, Ing. Zhoe Comas González e Ing. Fabio Mendoza Palechor por las asesorías y el acompañamiento recibido.

A mis compañeros de maestría por toda su colaboración y apoyo.

A la Universidad de la Costa y el cuerpo docente por todos los conocimientos compartidos durante este tiempo.

Resumen

Las Instituciones Educativas -IE, al igual que cualquier organización en general, se encuentran expuestas a diferentes tipos de riesgos que si no se tratan o administran de manera adecuada pueden llegar a afectar su normal operación. Entre los riesgos que pueden encontrarse en las IE están los físicos, los de gestión, los de corrupción, y los de seguridad digital. De igual forma las IE no están exentas de ser afectadas por desastres naturales, por lo que deben estar en capacidad de formular planes de contingencia y ejecutar acciones de respuesta a emergencias con las que aseguren la continuidad de la prestación del servicio y garanticen el derecho a la educación. Por lo anterior, es de suma importancia que las IE estén en la capacidad de administrar los riesgos que se puedan materializar, sea cual sea su naturaleza, y establecer controles que garanticen el cumplimiento de sus objetivos institucionales. Por consiguiente, el presente trabajo de grado, propone la creación de una metodología basada en la guía para la administración del riesgo del Departamento Administrativo de la Función Pública - DAFP y en la guía 59 del Ministerio de Educación Nacional - MEN, con la finalidad de mitigar el impacto u ocurrencia de los riesgos que puedan afectar la normal operatividad de las IE. La metodología propuesta será operacionalizada por medio de una herramienta tecnológica que sistematizará y unificará la metodología de administración del riesgo, el diseño de controles y la atención a emergencias y desastres.

Palabras clave: administración del riesgo, control del riesgo, emergencias, instituciones educativas

Abstract

Educational Institutions -EI, as any other organization in the world, are exposed to different types of risks that must be treated or handled in a properly way, however this can affect their normal operation of the EI. Some of these risks could be the physical management, corruption, and digital security. For these reason the EI are not exempt to being affected by natural disasters, so they must be able to formulate contingency plans and execute emergency response actions that ensure the continuity of the service and guarantee the education rights to the students. In fact it is very important that the EI would be capable to manage the risks, before than they may to materialize, indistinct of their nature, and establish adequate controls to guarantee a total compliance of the goals and aims of the EI. Consequently, this Dissertation proposes to develop the creation of a methodology based in the risk management guide of the Administrative Department of the Public Function - DAFP and 59th guide of the Ministry of National Education. - MEN, in order to mitigate the impact or the probability of occurrence of the risks that may affect the normal operation of the IE. The proposed methodology will be developed through a technological tool that will systematize and will unify the risk management methodology, the design of the controls and the way to perform the attention to emergencies and disasters.

Keywords: risk management, risk control, emergencies, educational institutions

Contenido

Lista de tablas y figuras

Tablas

Figuras

Introducción

La administración del riesgo juega un papel importante en cualquier organización, ya que, de no realizar el tratamiento adecuado, puede llegar a materializarse, afectando negativamente a la entidad.

Las IE no están exentas a este escenario, por ello necesitan estar preparadas para administrar sus riesgos; esto es, estar en la capacidad de identificarlos, analizarlos y tratarlos, de manera que puedan reducirse y minimizar su impacto. Deben, además ser capaces de ejecutar acciones de respuesta ante las emergencias que se presenten en el entorno educativo.

El presente trabajo de investigación tiene como propósito definir una metodología para la administración del riesgo y el diseño de controles basada en la guía para la administración del riesgo del DAFP y en la guía 59 del MEN, soportada en una herramienta tecnológica que permita su implementación en las IE públicas del departamento del Atlántico. Se espera que, con la incorporación de las TIC, las instituciones sean capaces de administrar sus riesgos, diseñar controles, ejecutar acciones de respuesta a emergencias y a formular planes de contingencia que permitan la continuidad de la prestación del servicio, garantizando el derecho a la educación.

La metodología está basada en una serie de fases alineadas a unos objetivos específicos, alcanzables mediante la ejecución de un conjunto de actividades y resultados que definen la realización del proyecto.

El presente documento está organizado de la siguiente manera: en el primer capítulo se presenta el planteamiento del problema, en el segundo la justificación, luego, se define el alcance del proyecto a través del objetivo general y los objetivos específicos en el capítulo 3, en el cuarto capítulo se realiza el análisis de los referentes teóricos, en el quinto se presenta el estado del arte, obtenido a partir de la búsqueda de la temática que enmarca la investigación. El sexto capítulo

presenta la propuesta de investigación, que es la metodología para la administración de riesgos en las IE del departamento del Atlántico y la operacionalización de dicha metodología. Por su parte, el séptimo capítulo presenta los resultados de la evaluación de la metodología y de la herramienta tecnológica respecto a su validez para administrar el riesgo en las IE. Por último, en el octavo capítulo se realizan las conclusiones del trabajo de investigación.

1. Planteamiento del problema

Cualquier entidad, sea cual sea su naturaleza, está expuesta a riesgos, entendiéndose como riesgo el "efecto que produce la incertidumbre sobre los objetivos" (ICONTEC, 2011, 9). Por ello, es de vital importancia su administración para lograr minimizarlos y/o eliminarlos y así evitar impactos negativos que puedan afectar la normal operación de la entidad. Las IE se encuentran expuestas a diferentes tipos de riesgos y situaciones que pueden afectar la prestación del servicio y el logro de sus objetivos. Algunos de ellos son los de tipo físico, tales como los ocasionados por fenómenos naturales; los de gestión, relacionados con la operación de la IE; los de corrupción, con los que se desviarían los dineros públicos para beneficiar a terceros; y los de seguridad digital, con los que se afectaría la integridad, disponibilidad y confidencialidad de los activos de la institución.

El MEN, a través de la Guía 59[1], establece los lineamientos para la formulación de Planes Escolares de Gestión del Riesgo - PEGR. Sin embargo, estos lineamientos se centran en gestionar el riesgo escolar y en educar a la comunidad educativa, para que sean capaces de hacer frente a situaciones de emergencia, es decir, riesgos físicos que involucran peligros, o aquellos que afecten los espacios propicios para el desarrollo del aprendizaje.

Por otra parte, la guía para la administración del riesgo y el diseño de controles en entidades públicas, emitida por el DAFP, es un instrumento que permite administrar el riesgo en las entidades públicas, ofreciendo seguridad para lograr sus objetivos.

Con el fin de conocer el estado que presentan las IE del departamento del Atlántico frente a la administración de riesgos, se realizó una encuesta, en la que participaron cuarenta y tres (43) IE, cuyos resultados se muestran en el anexo 1, los cuales indican que a pesar de la

[1] Guía 59: Lineamientos para la formulación de Planes Escolares para la Gestión del Riesgo. MEN.

existencia de la Guía 59, la mayoría de las Instituciones no tienen diseñado ni ejecutado el PEGR; ni tampoco adoptan algún tipo de metodología que permita la administración de otros tipos de riesgos, por ejemplo, los de gestión, corrupción y de seguridad digital, lo que manifiesta la necesidad de implementar una metodología para que las IE fortalezcan su desempeño con respecto a la administración de riesgos, asegurando de esta forma el logro de los objetivos institucionales y de procesos.A la situación anterior se suma la falta de capacitación en las IE que permitan identificar los diferentes tipos de riesgos a las que están expuestas, los controles que pueden diseñar para reducirlos, y lograr operacionalizar los planes escolares de gestión del riesgo.

Se destaca que, para lograr la operacionalización de dichas metodologías, la tecnología se convierte en una gran aliada, ya que es una herramienta de solución, sobre todo a nivel empresarial. Algunas de sus ventajas son agilizar procesos, gestionar información, incrementar la seguridad, entre otras, que favorecen la productividad y competitividad. Es por esto que, al utilizar las TIC, además de operacionalizar la metodología en las IE, la secretaría de educación podrá contar con la información de administración del riesgo de forma sistematizada, actualizada y en línea.

De acuerdo con lo anterior, surge la siguiente pregunta de investigación: ¿Qué tipo de metodología soportada en las TIC, se debe definir para la administración del riesgo en las Instituciones Educativas públicas del Departamento del Atlántico?

2. Justificación

Teniendo en cuenta que en las IE del departamento del Atlántico no se adopta algún tipo de metodología que permita administrar los diferentes tipos de riesgos a los que pueden estar expuestas, se requiere diseñar una estrategia que apunte al fortalecimiento de este aspecto.

La presente propuesta de investigación pretende que las IE. adopten una metodología que les permita administrar sus riesgos, soportada en una herramienta tecnológica que facilite su operacionalización.

Esta metodología estará apoyada en la guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP y en la guía 59 del MEN, por lo que estará articulada con las directrices establecidas por el gobierno nacional, y a la vez estará contextualizada en el entorno de las IE, lo que permitirá que éstas sean capaces de administrar sus riesgos físicos, de gestión, de corrupción y de seguridad digital, además de ejecutar acciones de respuesta a emergencias y a formular planes de contingencia que les permitan continuar con la prestación del servicio, cuando éste pueda verse afectado.

Por otra parte, se contribuirá a la digitalización y al ahorro de papel, toda vez que la información será registrada en la herramienta web, que además permitirá mantener el contacto entre la secretaría de educación y las diferentes IE del departamento, con lo que se garantiza que ésta realice consultas y seguimiento a las diferentes actividades de control que se van desarrollando dentro de las instituciones.

Del mismo modo se apunta al cumplimiento del objetivo del componente TIC para el estado de la estrategia de gobierno digital, debido a que con esta propuesta se apunta al mejoramiento de las IE públicas y su vínculo con la secretaría su de educación, a través del uso de las TIC.

3. Objetivos

3.1 Objetivo general

- Definir una metodología para la administración del riesgo basada en la guía para la administración del riesgo del DAFP y la guía 59 del MEN, soportada en una herramienta tecnológica que permita su implementación en las instituciones educativas públicas del departamento del Atlántico.

3.2 Objetivos específicos

- Analizar referentes relacionados con la administración del riesgo y controles, contextualizados en las instituciones educativas y las tecnologías de la información y la comunicación (TIC).
- Integrar la guía 59 del MEN con la guía para la administración del riesgo y diseño de controles en entidades públicas del DAFP en el proceso de construcción de una metodología para las Instituciones Educativas públicas del departamento del Atlántico
- Desarrollar una herramienta tecnológica que permita operacionalizar la metodología para la administración del riesgo y diseño de controles en las Instituciones Educativas Públicas del Departamento del Atlántico.
- Evaluar la metodología y la funcionalidad de la herramienta tecnológica respecto a su validez para administrar el riesgo y diseñar controles en las Instituciones Educativas.

4. Marco teórico - conceptual

El objeto de estudio de la presente propuesta de investigación se encuentra sustentado por dos ejes temáticos, que son: la administración del riesgo, y el diseño de controles, contextualizados en el ámbito educativo y en la forma como las TIC facilitan la implementación de soluciones (Fuse et al., 2012) que permitan la gestión de estos dos ejes.

4.1 Administración del riesgo

Todas las empresas, sea cual sea su naturaleza, están expuestas a riesgos de todo tipo, que de materializarse podrían afectar la operación de ésta y ocasionar pérdidas. Es por esta razón que la gestión o administración del riesgo cobra importancia, ya que, de acuerdo con ICONTEC (2011) a través de ésta se pueden establecer actividades que permitan administrar y controlar una organización respecto a sus riesgos (p. 9).

Asimismo, el DAFP establece que “la administración del riesgo es el proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos” (DAFP, 2018b, p. 8). De igual forma, sugiere que se implemente una política de administración del riesgo, con la que se podrán definir los elementos básicos de actuación frente al control y la gestión de los diferentes riesgos que puedan presentarse.

Los autores (Fraser & Simkins, 2016) recomiendan que las empresas tengan una política general de administración del riesgo, en la que se deberán incluir las definiciones de los conceptos principales, tales como, "riesgo", para que se puedan usar las mismas definiciones en toda la empresa.

Del mismo modo, el DAFP (2018b), establece que la política de administración del riesgo además de incluir términos y definiciones relacionados con el tema, deberá incluir también como mínimo los siguientes aspectos: El objetivo, con el que se establece el marco de actuación para el

control y la gestión de los riesgos; el alcance, que permite establecer el ámbito de aplicación de los lineamientos; niveles de aceptación del riesgo o tolerancia al riesgo: define los niveles de aceptación de la entidad; niveles para calificar el impacto, que incluye la tabla de impactos institucional; tratamiento de riesgos, que establece el proceso para modificar el riesgo (pp. 15-16).

El proceso para la gestión del riesgo es definido en ICONTEC (2011), a través de una serie de actividades presentadas en la figura 1:

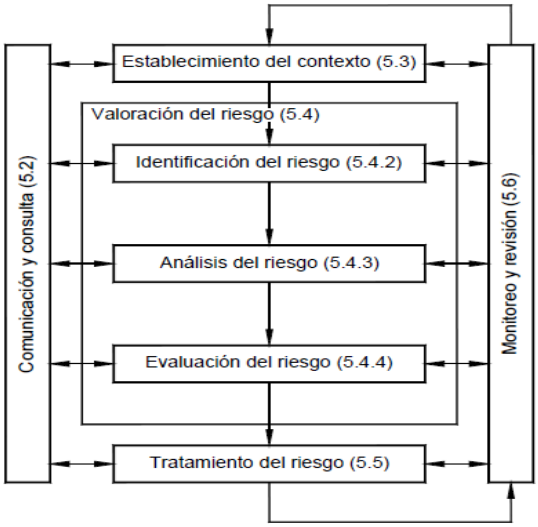


Figura 1 Proceso para la administración del riesgo. *Fuente:* ICONTEC, 2011, p. 22.

La anterior figura muestra cómo se da el proceso para la administración del riesgo, el cual inicia con el establecimiento del contexto, luego se realiza la identificación del riesgo, posteriormente se analiza y se evalúa el riesgo, y por último se aplica el tratamiento correspondiente que permita mitigar el riesgo. Las actividades de comunicación y consulta, y monitoreo y revisión se dan de forma transversal durante todo el proceso.

Mencionado lo anterior, es necesario aterrizar el concepto dentro de las IE. En este sentido, el MEN establece en su guía 59, que “la educación para la gestión del riesgo busca

disponer de estrategias para prevenir posibles riesgos que podrían afectar el buen funcionamiento de la institución y el bienestar de la comunidad educativa" (MEN,2015, p. 22).

La guía 59 se apoya en lo establecido en la ley 1523 de 2012 política de gestión del riesgo, la cual establece que:

> La gestión del riesgo 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. (Ley N°1523, 2012, art. 1).

De acuerdo con lo explicado anteriormente, la guía 59 se centra en los riesgos físicos a los que están expuestas las IE, y a la formulación de planes de respuesta a emergencias y desastres que permitan asegurar la continuidad del servicio educativo.

Sin embargo, las IE no solo se enfrentan a riesgos físicos, por lo que éstas deben estar en capacidad de gestionar los riesgos que pueden perjudicar su operación. En este sentido, (Fraser & Simkins, 2016), comentan que "a mediados de la década de 1990, varias publicaciones empezaron a recomendar a las empresas que la gestión de riesgos debería incluir todos los riesgos, no solo los que son más fáciles de cuantificar, y que los riesgos deberían gestionarse como una cartera en toda la empresa".

Es así como con esta solución no solo se gestionarían los riesgos físicos, tal como se menciona en la guía 59 sino también otro tipo de riesgos, tales como los de gestión, corrupción y seguridad digital, siguiendo lo establecido en la guía para la administración del riesgo y el diseño de controles en entidades públicas, sugerida por el DAFP.

4.2 Control

La ISO 31000, define el control como “una medida que modifica al riesgo” (ICONTEC, 2011, p. 14).

Teniendo en cuenta lo anterior, el DAFP (2018b) sugiere que para definir si un control logra mitigar adecuadamente un riesgo, se deberán tener en cuenta las variables mencionadas a continuación: responsable, periodicidad, propósito, cómo se realiza, qué pasa con las observaciones o desviaciones, y la evidencia (p. 49).

No es suficiente con que un control se diseñe correctamente, “el control debe ejecutarse por parte de los responsables tal como se diseñó. Porque un control que no se ejecute, o un control que se ejecute y esté mal diseñado, no va a contribuir a la mitigación del riesgo” (DAFP, 2018b, p. 59).

Una vez se realiza el análisis y la evaluación de los controles, se debe analizar el nivel de riesgo residual, es decir, aquel que permanece a pesar de haber tomado medidas de tratamiento. En este caso, se debe volver a realizar el análisis del riesgo y la revisión correspondiente a dicho tratamiento.

Una vez determinado el tratamiento a efectuar, se genera un reporte que contenga la información crucial del proceso de administración del riesgo, el cual será el reporte del plan de tratamiento de riesgos, en donde se destacan las actividades de control definidas para tratar los riesgos.

En consecuencia, establecer controles que permitan mitigar los riesgos favorecerá en gran medida a que las entidades logren alcanzar sus objetivos, de igual modo, las IE deberán implementar controles que garanticen minimizar la ocurrencia e impacto de riesgos de todo tipo, por ejemplo, los riesgos de corrupción, que posibilitan la desviación de los dineros públicos para favorecer a terceros.

En este sentido, (Gong & Subramaniam, 2018), comentan que un mayor nivel de uso de sistemas de control de gestión refleja una mayor propensión a la transparencia interna y la reparación, lo que promueve que los empleados desarrollen una comprensión abierta y oportuna de las operaciones de la escuela (por ejemplo, niveles de ingresos / costos), e investiguen desviaciones en los presupuestos y objetivos de ésta.

A continuación, se describen las dos guías metodológicas en las que se sustenta el desarrollo de la presente propuesta de investigación:

4.3 Guía para la administración del riesgo y el diseño de controles en entidades públicas

El DAFP, junto con otras entidades del estado tal como el Ministerio de Tecnologías de la Información y Comunicaciones – MinTIC, presentan la "Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital", y sus anexos, como un instrumento que le brinda a las entidades públicas del país, la oportunidad de administrar sus riesgos y diseñar controles, permitiendo el logro de sus objetivos institucionales. (DAFP,2018b, p. 6).

Esta metodología se encuentra articulada con el Modelo Integrado de Planeación y Gestión (MIPG) y está alineada con los mejores estándares internacionales como "COSO 2013, COSO ERM 2017 y el modelo de las tres líneas de defensa" (DAFP, 2018b, p. 6).

El modelo de las tres líneas de defensa "es un modelo de control que establece los roles y responsabilidades de todos los actores del riesgo y control en una entidad, este proporciona aseguramiento de la gestión y previene la materialización de los riesgos en todos sus ámbitos" (DAFP,2018b, p. 75).

Este modelo se enmarca de la siguiente forma:

- ✓ Línea estratégica: A cargo de la alta dirección, define el ámbito general para la gestión de riesgos.

- ✓ 1era línea de defensa: Encargada de implementar los procesos relacionados a la gestión de riesgos.
- ✓ 2da línea de defensa: Encargada de asegurar que los procesos ejecutados por la línea anterior, se diseñen y funcionen correctamente.
- ✓ 3era línea de defensa: Informa sobre la efectividad del sistema de control interno, supervisando las líneas anteriores.

La estructura de la metodología se muestra en la figura 2:

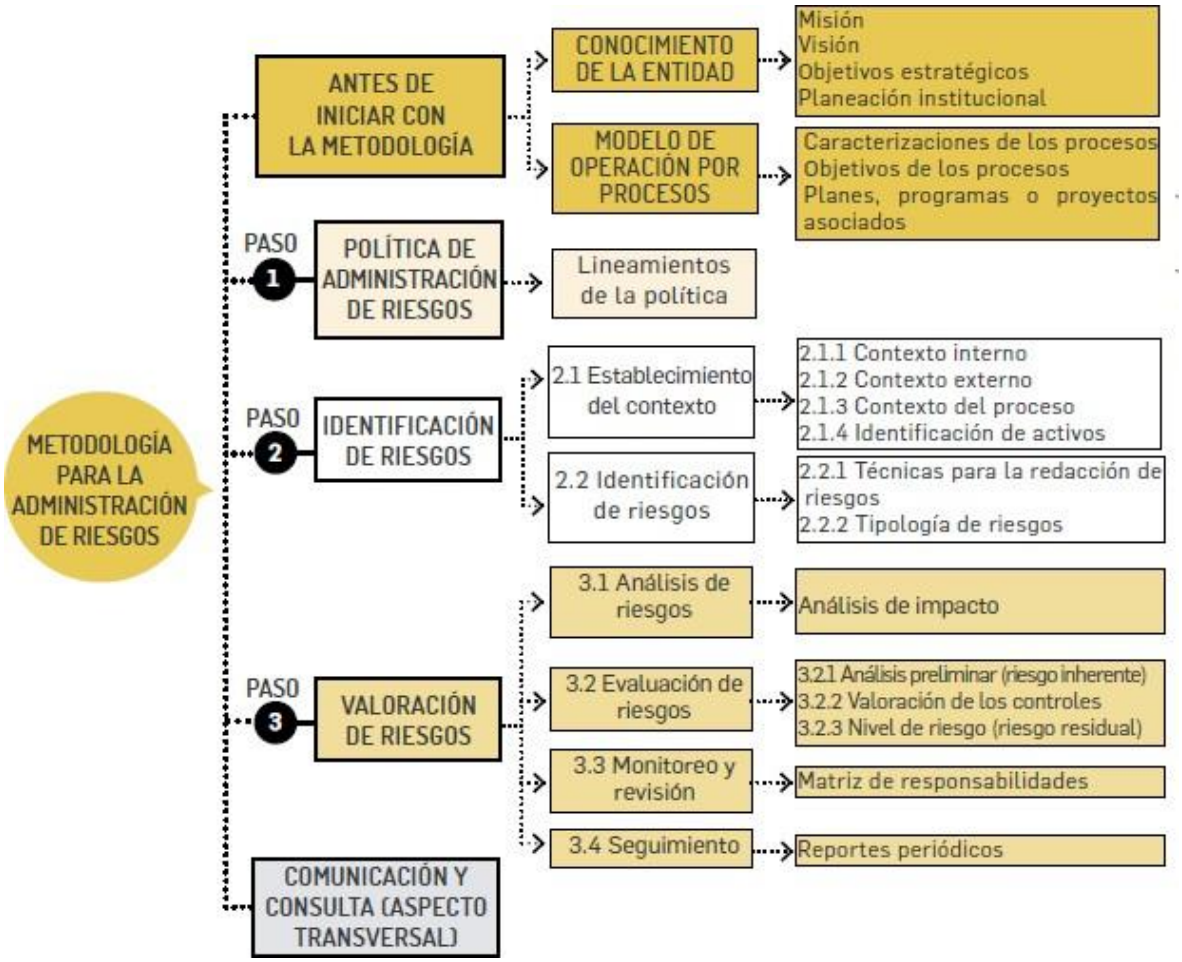


Figura 2 Metodología para la administración del riesgo. *Fuente:* DAFP,2018b, p. 13

Esta metodología necesita de un análisis inicial concerniente con el conocimiento de la entidad y el modelo de operación por procesos (caracterización de los procesos), seguido de tres pasos relacionados con la gestión del riesgo: establecimiento de la política, la identificación y

valoración de los riesgos, y por último precisar estrategias de comunicación que sean transversales en toda la organización.

4.4 Guía 59: Lineamientos para la Formulación de Planes Escolares para la Gestión del Riesgo

La guía 59 emitida por el MEN establece los lineamientos para la formulación de los PEGR, como una herramienta que permite que las IE sean capaces de leer y comprender su contexto, sus escenarios de riesgo, y desarrollar estrategias para su mitigación.

De igual forma, establece que la educación para la gestión del riesgo se materializa en dos aspectos: el primero, en el horizonte institucional, haciéndose transversal en el currículo escolar y en el PEI (Proyecto Educativo Institucional); y el segundo, en el diseño y ejecución del PEGR como herramienta de gestión de la comunidad educativa, que le permita conocer y reducir el riesgo, manejar las emergencias y/o desastres que pueden llegar a afectarla.

En cada IE es necesario definir un equipo de gestión del riesgo, que se apropie de los saberes relacionados al riesgo y al papel de la escuela como ente protector de los niños; este equipo puede estar conformado por personal directivo, administrativo, cuerpo docente, padres de familia, estudiantes y entidades externas.

Esta guía define que la gestión del riesgo en las IE implica contar con:

- Una comunidad educativa empoderada a través de procesos de formación para la prevención, reducción y la atención en situaciones de emergencia y post emergencia.
- Espacios sociales e institucionales fortalecidos, que faciliten la coordinación y articulación entre los diferentes actores para la actualización de los análisis de riesgos y la adopción de medidas de prevención, disminución, disuasión o superación del riesgo.

- Una capacidad resiliente y de recuperación de la comunidad afectada, que contribuye con la sostenibilidad de la IE.

Los PEGR son una herramienta de planeación participativa que comprende los enfoques, propósitos, líneas de acción, estrategias y metas para construir y/o fortalecer la educación para la gestión del riesgo (conocimiento y reducción del riesgo y manejo de desastres) en las comunidades educativas, como contribución a la garantía del derecho a la educación, derecho al ambiente sano y derechos de Niños, Niñas, Adolescentes y Jóvenes. (MEN,2015, p. 25).

De acuerdo con lo anterior, los dos ejes conceptuales (administración del riesgo y control) y las dos guías metodológicas descritas (Guía del DAFP y guía 59 del MEN), fundamentan el objeto de esta investigación, tanto desde el punto de vista de la metodología propuesta, como desde el enfoque de cómo las TIC soportan el desarrollo de soluciones que fortalezcan la operacionalización de dichas metodologías.

5. Estado del arte

En término de gestión eficiente de las escuelas, es importante precisar las posibles amenazas y cuellos de botella que pueden impedir el logro de metas y objetivos futuros o identificar cualquier tipo de riesgo que pueda presentarse, (Şahin & Faruk Ak, 2018).

Existe una estrecha relación entre crisis y riesgo, ya que ambas definiciones se centran en eventos que de llegar a materializarse pueden afectar el normal funcionamiento de la escuela.

Es así como, (Savelides, Mihiotis, & Koutsoukis, 2015), definen la crisis como un evento extraordinario que interrumpe el normal funcionamiento de la IE., específicamente la crisis srelacionada con emergencias, y cómo deben estar preparadas para hacer frente a ella, sin embargo, refieren que a pesar de la relativa frecuencia de crisis que ocurren en la educación, la literatura sobre cómo lidiar con ésta a nivel escolar es muy poca.

En este sentido, (Savelides et al., 2015) proponen a través de su documento, conocer las prácticas de gestión de crisis en la educación secundaria en Grecia que sirvan como guía para diseñar un sistema formal de gestión de crisis.

Adicionalmente, argumentan que las escuelas con una cultura de gestión del riesgo orientada al desempeño alentarán e involucrarán al personal para alinear sus actividades diarias con las metas de la escuela (Gong & Subramaniam, 2018), de igual modo expresan que es probable que una sólida cultura de gestión del riesgo orientada al desempeño fomente el logro de los objetivos financieros al tomar riesgos y oportunidades que apoyarán la obtención de recursos para la escuela y el ahorro de costos.

El riesgo no es estático, y éste depende de las condiciones y vulnerabilidad del contexto (McEntire, 2012) así como de las respuestas de comportamiento de las personas que enfrentan dichos riesgos (Lewis, 2019), es por esto que las IE deben desarrollar un plan estratégico que les permita responder a cualquier riesgo que se pueda presentar (Pattanajureepan et al., 2013), tanto dentro como fuera de ellas (Encyclopedia, 2019).

Teniendo en cuenta que en las IE se pueden presentar diferentes tipos de riesgos (Moyo, Abdullah, & Nienaber, 2013) mencionan los riesgos de seguridad digital y manifiestan que la importancia de la seguridad de la información en las escuelas secundarias está aumentando debido al mayor uso y dependencia de los sistemas de información, resaltando su principal objetivo que es el de preservar la confidencialidad, integridad y disponibilidad de los activos.mo

En este sentido, la seguridad de la información requiere una variedad de habilidades y conocimientos que rara vez se encuentran en organizaciones de pequeña escala como las escuelas secundarias, por esto (Moyo et al., 2013) proponen que se deben establecer mecanismos apropiados de gestión de riesgos de seguridad de la información para salvaguardar

sus sistemas de información, por lo tanto se hace necesario que las escuelas sean guiadas o asistidas para realizar ejercicios de administración de riesgos.

Con respecto a los riesgos físicos, a nivel nacional, las IE diseñan sus PEGR siguiendo lo establecido en la guía 59 del MEN y en la ley 1523 de 2012, ésta última suministra tres pasos para la gestión del riesgo: conocimiento del riesgo, reducción del riesgo y manejo de los desastres; tal es el caso de (Pérez, Sáenz & Gómez, 2016), quienes en su documento plantean una metodología para la implementación del PEGR en una IE de la ciudad de San José de Cúcuta, Colombia.

Dado que las IE involucran cada vez más a las TIC (Yasuda, 2010), se hace necesario utilizar este tipo de herramientas para operacionalizar metodologías que permitan administrar los riesgos que pueden afectar el logro de los objetivos propuestos.

Al realizar la revisión de la literatura en el presente estado del arte, se pudo evidenciar que en los trabajos existentes no se aborda el ámbito de estrategias TIC para gestionar riesgos en las IE. Sin embargo, en Colombia y Costa Rica, se encuentran propuestas que involucran a las TIC para gestionar riesgos escolares.

En los casos mencionados se hace uso de las TIC como herramienta de apoyo, ya que es un mecanismo que proporciona precisión y confianza tanto a las escuelas como a los responsables de la toma de decisiones, facilitando procesos rápidos y oportunos para comprender los niveles de riesgo (Ruiz, 2015).

En Colombia, la alcaldía de Bogotá, a través del Instituto Distrital de Gestión de Riesgos y Cambio Climático – IDIGER, definió las pautas para el diseño de los Planes Escolares de Gestión de Riesgos y Cambio Climático - PEGR-CC.

El PEGR-CC es un instrumento que orienta e integra los procesos estratégicos

de la gestión de riesgos y el cambio climático cuyo fin es conocer los riesgos a los que se encuentra expuesta la población en el contexto escolar, planear las medidas para reducir los riesgos identificados, así como los efectos del cambio climático, responder ante una emergencia en caso de que se presente y garantizar la continuidad del servicio educativo. (Instituto Distrital de Gestión de Riesgos y cambio climático, 2015, p. 4).

Igualmente, se creó la herramienta web denominada Sistema Único de Registro Escolar - SURE, a través de la cual se cuenta con información en línea sobre el estado de los PEGR de estas IE.

Por su parte, en Costa Rica, se diseñó un prototipo de un sistema para gestionar la información relacionada con el análisis integral de riesgos y los planes para reducir el riesgo en las escuelas (Sistema GIRE). El objetivo de la plataforma es administrar la información relacionada con el análisis integral de riesgos y los planes para reducir el riesgo escolar a través de un sistema que permita la generación de conciencia situacional por parte del gobierno y la comunidad educativa, permitiéndoles tomar decisiones para convertirse en comunidades educativas resilientes (Paton & Johnston, 2004).

Sin embargo, estos sistemas solo manejan la información relacionada a los PEGR, es decir que se centra en la gestión de riesgos físicos y la atención a emergencias (Pattanajureepan et al., 2013), y no a la gestión de diferentes tipos de riesgos que se pueden presentar en las IE, tales como los riesgos de gestión, de corrupción y de seguridad digital.

6. Metodología

Una vez revisado el planteamiento del problema, el marco teórico y el estado del arte de la presente investigación, se procede a presentar la metodología propuesta, se describen sus diferentes pasos, así como la herramienta web que permitirá su operacionalización.

6.1 Metodología para la administración del riesgo

Para el desarrollo de la presente metodología, se propone la integración de la guía 59 del MEN, con la guía para la administración del riesgo y diseño de controles del DAFP, como se explicó en el capítulo 1, la primera establece la administración de riesgos físicos y la respuesta a emergencias, mientras que la segunda define la administración de riesgos de gestión, corrupción y seguridad digital.

Al realizar el análisis de las actividades que conforman estas metodologías, se pudo evidenciar que tienen aspectos comunes, especialmente los relacionados con el tratamiento del riesgo. De igual forma, se pudo analizar que la guía del DAFP se complementa con la guía 59 del MEN, ya que ésta última incluye además de los pasos para la administración de riesgos físicos, los pasos a seguir para la respuesta a emergencias.

Teniendo en cuenta que la guía del DAFP está diseñada para su implementación en las entidades públicas del país, y que las IE públicas hacen parte de este grupo, pero con condicionales y características particulares, es posible unificar las actividades descritas en cada una de las metodologías mencionadas anteriormente, iniciando con las actividades propias de la administración del riesgo, y concluyendo con las actividades relacionadas a la respuesta a emergencias.

Siguiendo lo establecido en la guía del DAFP, con respecto al modelo de las tres líneas de defensa, en el ámbito de las IE, se definen las siguientes líneas:

- Primera línea de defensa: su objetivo es asegurar la gestión, mediante la ejecución efectiva de controles internos, sobre una base del día a día. Estará a cargo de los jefes de proceso, o las personas responsables de ejecutar los procesos. Ejemplo: rector, consejo académico, docente orientador, etc.

- Segunda línea de defensa: Esta línea de defensa estará representada por el CARAE (Comité de Administración del Riesgo y Atención a Emergencias) y su objetivo es el de asegurar que la primera línea esté diseñada y opere de manera efectiva con respecto a la administración de riesgos. En cada IE es necesario definir un CARAE, el cual estará conformado como mínimo por: rector (Líder del comité); coordinador; líder del PRAE, se escoge del grupo de docentes dinamizadores de los Proyectos Ambientales Escolares; líder del Grupo de logística, se escoge un representante del personal administrativo, de seguridad, mantenimiento, almacén, o servicios generales; líder del consejo académico, se escoge un líder del consejo académico, grupo conformado por un docente representante de cada área; líder del área de Tecnología e Informática, se escoge un líder del grupo de docentes del área de tecnología e informática; líder de brigada, se escoge un líder del grupo de respuesta a emergencias, conformado por las tres brigadas necesarias para la respuesta a emergencias: primeros auxilios, contra incendios y evacuación; líder de padres de familia, se escoge un líder del grupo conformado por los representantes de padres de familia; líder de Estudiantes, personero; se puede contar con la representación de los organismos de socorro locales, tales como defensa civil, bomberos, cruz roja, etc. (Opcional).

- Tercera línea de defensa: Su objetivo es proporcionar aseguramiento independiente sobre la eficacia de la administración de riesgos. La representa la secretaría de educación.

Teniendo en cuenta estos aspectos comunes y complementarios, la metodología propuesta solicita iniciar con el análisis de las IE, incluyendo su contexto, seguida de tres pasos para administrar el riesgo y por tres pasos adicionales para ejecutar la respuesta a emergencias, además de la definición de estrategias de comunicación, consulta y seguimientos transversales a toda la entidad. (Ver figura 1).

De esta forma las IE públicas del departamento del Atlántico estarían cumpliendo con lo que normativamente se exige tanto desde el gobierno nacional como desde el MEN, asegurando que estén en la capacidad de administrar cualquier tipo de riesgo y puedan responder a emergencias.

A continuación, la figura 1 muestra la estructura completa de la metodología propuesta:

Figura 3 Estructura de la metodología. *Fuente:* elaboración propia.

6.1.1 Paso 1. Presentación institucional

Se inicia con la presentación de la IE y su entorno. Este paso está conformado por dos aspectos claves, la identificación de la institución y la identificación de la sede. En la figura 2 se muestra la estructura de este primer paso de la metodología:

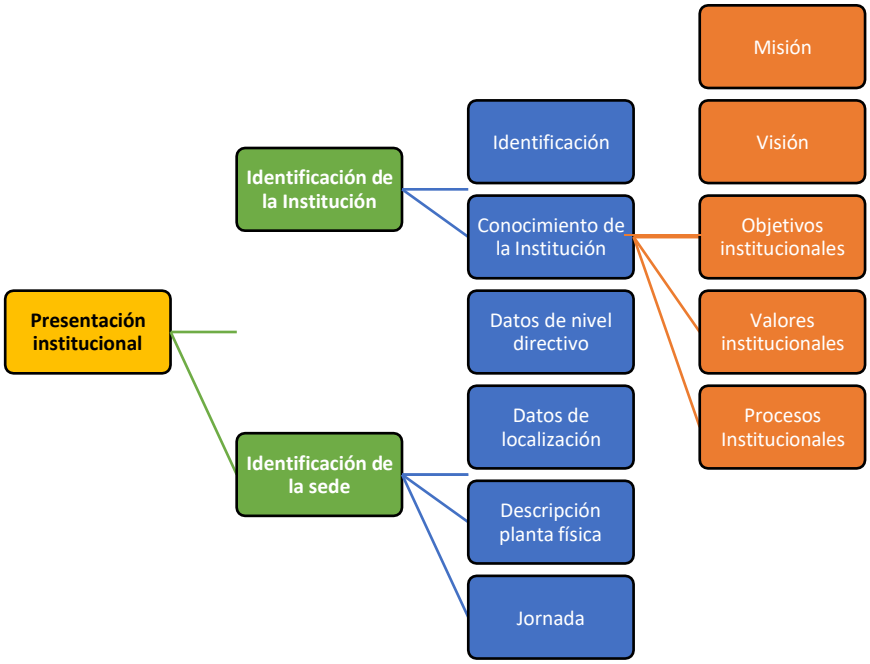


Figura 4 Presentación institucional. *Fuente:* elaboración propia

La sección identificación de la institución se desglosa de la siguiente manera:

- ✓ Identificación: nombre de la IE, código DANE, rector, número de sedes.
- ✓ Conocimiento de la institución: misión, visión, objetivos y valores institucionales.
- ✓ Procesos institucionales: identifican el conjunto de actividades interrelacionadas que agregan valor a la IE, alineadas con el Plan de Mejoramiento Institucional (PMI). Siguiendo lineamientos establecidos por el MEN en la guía 34: Guía para el mejoramiento institucional. Estos procesos corresponderán a cada una de las áreas de la gestión institucional: gestión directiva, gestión académica, gestión administrativa y financiera y gestión de la

comunidad. (MEN,2008). La figura 3 muestra los procesos por cada área de gestión.

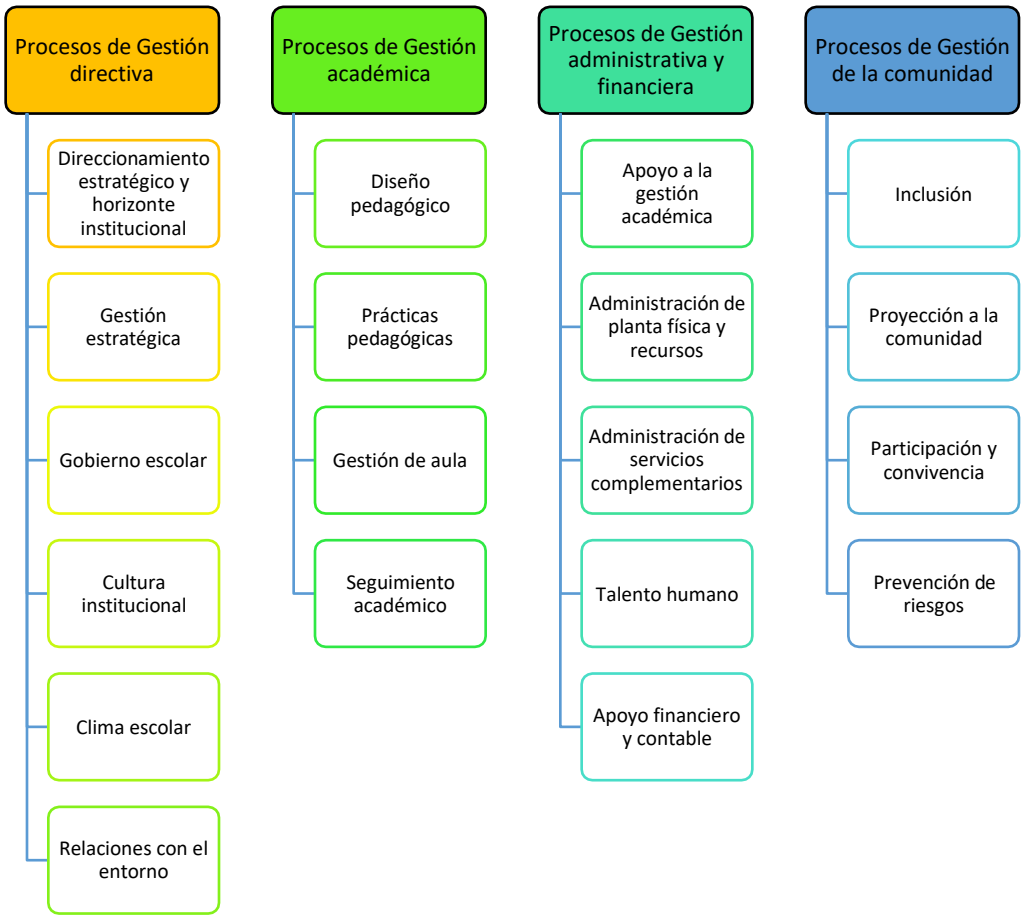


Figura 5 Procesos de las áreas de gestión institucional. *Fuente:* elaboración propia

La sección información de la sede se desglosa de la siguiente manera:

- ✓ Identificación: Código DANE, Coordinador(es), identificación del CARAE.
- ✓ Datos de nivel directivo: Cargo, nombre, correo, teléfono
- ✓ Datos de localización: municipio, barrio, dirección, teléfono, correo electrónico
- ✓ Vecinos inmediatos: Norte: -Sur: -Este: -Oeste:
- ✓ Descripción planta física: año de construcción, total, área construida (m2), total, área libre (m2), licencia de construcción, concepto uso de la construcción, concepto higiénico-sanitario, permiso ambiental, concepto bomberos, cantidad

edificios y/o

bloques: (1,2, 3…), edificio #, cantidad de pisos, tipo de salón (Almacenes, auditorio, baños, biblioteca, bodegas, cafetería, canchas y/o polideportivo, cocina, comedor, enfermería, gimnasio, laboratorios, oficinas, parqueaderos, punto de primeros auxilios, sala de informática, sala de profesores, salones, salón de arte, garitas (vigilancia) – Cantidad

- ✓ Jornada de la sede: única, mañana, tarde, noche

Al finalizar el primer paso de la metodología se obtiene toda la información referente a la identificación de la IE y sus procesos, destacando la conformación del CARAE (segunda línea de defensa), comité encargado de coordinar las acciones establecidas en la presente metodología.

6.1.2 Paso 2. Política de administración del riesgo

Para el DAFP (2018b) la política de administración del riesgo es:

> La declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo (NTC ISO31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos. (p. 14).

En este sentido, la política de administración del riesgo debe ser establecida por el equipo directivo y debe incluir como mínimo los siguientes ítems:

- ✓ **Términos y definiciones:** A modo de glosario se listan términos afines con la administración del riesgo para que toda la comunidad educativa entienda su contenido y aplicación. **Objetivo:** Se debe establecer cuál es el fin de la política, con el que se busca gestionar los riesgos que se pueden presentar en la IE, a un

nivel que sea aceptado por ésta.

- ✓ **Alcance:** Se establece el ámbito de la política. Debe cubrir todos los procesos de la institución, de igual forma se sugiere incluir a todas las sedes.
- ✓ **Niveles de aceptación del riesgo:** "Es la decisión informada de tomar un riesgo particular" (DAFP,2018b, p. 14). Teniendo en cuenta que hay 4 niveles de riesgo: *bajo, moderado, alto y extremo,* la IE debe determinar el nivel de aceptación de cada uno, es decir, debe indicar cuáles son aceptables y cuáles inaceptables.
- ✓ **Niveles para calificar el impacto:** Se debe tener en cuenta que existen cinco niveles para calificar el impacto del riesgo, los cuales son: insignificante, menor, moderado, mayor y catastrófico.
- ✓ **Tratamiento del riesgo:** Es el proceso que permite la modificación del riesgo, la IE debe decidir el tratamiento a aplicar a cada uno, teniendo como opción: aceptarlo, evitarlo, compartirlo o reducirlo. Es de resaltar que los riesgos de corrupción se pueden presentar en todos los procesos, por lo que no se deben aceptar y deben siempre poder tratarse (DAFP,2018b, p. 68)

En el anexo 2 se muestra un ejemplo de política de administración del riesgo para una IE.

6.1.3 Paso 3. Identificación del riesgo

El CARAE deberá realizar el análisis de los objetivos tanto institucionales como de procesos, para reconocer riesgos que puedan llegar a afectar su cumplimiento. Se debe tener en cuenta que los objetivos de proceso deben contribuir al cumplimiento de los objetivos institucionales, los que a su vez deberán estar alineados con la misión y la visión de la IE.

Este paso de la metodología se desarrolla en dos fases, la primera es la de la caracterización del contexto de la IE, a través de la cual se definen los parámetros tanto internos como externos, los parámetros del contexto del proceso y de los activos de seguridad digital, que deben considerarse para administrar el riesgo. La segunda fase es la de identificación del riesgo, por medio de la cual se define el tipo de riesgo, su descripción, principales causas y consecuencias.

El equipo de trabajo podrá hacer uso de herramientas y técnicas para caracterizar el contexto y valorar el riesgo, tales como: lluvia de ideas, entrevistas estructuradas o semiestructuradas, análisis de escenario, análisis de causa y efecto, etc.

6.1.3.1 Caracterización del contexto

Para realizar la caracterización del contexto se definen los parámetros internos y externos, los parámetros de proceso y se identifican los activos de seguridad digital[2].

Es posible determinar las causas de los riesgos a partir de los factores que se definan en esta caracterización.

I. Caracterización del contexto externo

Se identifican las particularidades del entorno en el que se encuentra la institución, tales como: políticos, legales y reglamentarios: en este aspecto se mencionan aspectos relacionados a políticas educativas, leyes, decretos, políticas públicas, etc. Económicos y financieros: estrato socioeconómico de la población, desempleo. Sociales y culturales (demografía): acceso a servicios públicos, recreación, deporte, salud, seguridad, etc.

[2] Explicado en la página 42

Tecnológicos: disponibilidad de sistemas de información, avances tecnológicos. Ambientales: en este aspecto se debe determinar si el entorno escolar puede verse afectado por fenómenos de origen natural, tales como atmosféricos, hidrológicos y geológicos.

II. Caracterización del contexto interno

Se identifican las particularidades del entorno interno con el que cuenta la IE. A continuación, se describen estas características:

- ✓ Estructura física: En este aspecto se describe el estado físico general de la IE, relacionado con:

  Cimientos de las edificaciones, muros estructurales, techos y cubiertas, sismo resistencia, escaleras y accesos, puertas y muros cortafuegos, salidas de emergencia, rutas de evacuación, señalización de vías de evacuación y equipos contra incendios, suministro de energía, suministro de agua, recolección de basura, gas natural, sistemas de detección de incendios, parqueaderos, disponibilidad de tanque de reserva, camillas, botiquines, extintores, sistema de alarma, planta de emergencia, sistema de vigilancia, otros. (Instituto Distrital de Gestión de Riesgos y cambio climático, 2015, p. 19).

- ✓ Estructura organizacional: En este aspecto se plasma el organigrama institucional.

- ✓ Financieros: Este ítem está relacionado con todo el aspecto financiero de la IE, especialmente relacionado con el presupuesto de funcionamiento y la existencia de rubros para mitigar los riesgos: presupuesto y recursos para implementar la administración de riesgos, mecanismos para gestión externa de recursos,

presupuesto para respuesta a emergencia, pólizas: para la IE, muebles, enseres y equipos

- ✓ Comunidad educativa: Este aspecto está relacionado con la población que conforma a la IE, en aspectos relacionados con:
  - Población
    - Tipo de población: menores de tres años, educación pre-escolar, básica primaria, básica secundaria, docentes, docente orientador, administrativos, cafeterías-restaurantes, servicios generales, portero, seguridad privada (vigilancia)
    - Cantidad de población
    - Número de personas con discapacidad: sensorial, cognitiva, física
  - Factores educativos: Este aspecto está relacionado con la apropiación de la IE con respecto a la administración del riesgo, se deben analizar entre otros:
    - Intervención de acudientes y padres de familia en proyectos
    - Incorporación curricular de la administración del riesgo en los planes de estudio, proyectos de aula, transversales, etc.: En la actividad de diseño curricular, se plantea la transversalización de la gestión del riesgo en todos los escenarios escolares, de manera interdisciplinaria y mediante la selección y organización de contenidos (saberes, no temas) conceptuales, actitudinales y procedimentales que permitan transformar las realidades adversas a la formación de ciudadanía crítica y de cultura de

derechos. (MEN,2015)

- Implementación de herramientas pedagógicas para la administración del riesgo
- Apropiación de temas relacionados con la administración del riesgo por parte de docentes, directivos docentes y estudiantes.
- Comité de Administración del Riesgo y Atención a Emergencias (CARAE): Con respecto al comité, se debe analizar si:
    - El CARAE está conformado
    - El CARAE está funcionando
    - Las brigadas de emergencia están conformadas
    - Las brigadas de emergencia están funcionando
    - Existen herramientas que permiten verificar el estado de los equipos y dotaciones de emergencia
- Comunicación interna: Este aspecto está relacionado con los canales de comunicación que utiliza la IE y su efectividad para que el flujo de información circule por todos los procesos y miembros de la comunidad educativa. Por ejemplo: página web, periódico institucional, correo electrónico, circulares, etc.

III. Contexto del proceso

Se identifican las particularidades del proceso y sus interrelaciones. Es recomendable utilizar las caracterizaciones de los procesos como herramienta para analizar el contexto de éstos, incluyendo aspectos como: nombre del proceso, objetivo, alcance, responsable, entrada del proceso, actividades clave, salida del proceso, cliente

del proceso, recursos, requisitos del proceso (normatividad), indicadores asociados. En el anexo 3 se puede ver un ejemplo de caracterización de procesos.

IV. Identificación de activos de seguridad digital

"Un activo es cualquier elemento que tenga valor para la organización" (Ministerio de Tecnologías de la Información y las Comunicaciones, 2018, p. 11). En el contexto de seguridad digital, los activos son denominados activos de información, ya que están relacionados con cualquier elemento referente al tratamiento de la información (equipos, bases de datos, sistemas de información…) que tenga valor para la organización.

En este sentido, cuando se mencione el término activos en la presente investigación se estará haciendo alusión a los activos de información.

Para identificar los activos de seguridad digital de la IE, se siguen los pasos mostrados en la figura 4:

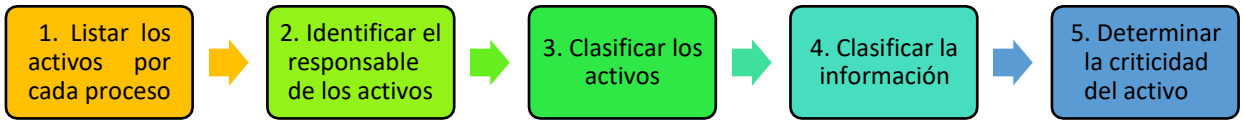


Figura 6 Identificar y valorar activos seguridad digital. Adaptado de "Lineamientos Para La Gestión De Riesgos De Seguridad Digital En Entidades Públicas". *Fuente:* MinTIC, 2018, p. 12.

Listar los activos por cada proceso:

Se definen los activos de cada proceso, incluyendo, nombre del proceso y una breve descripción. (Ver Tabla 1).

Tabla 1

Lista de activos

Proceso		Activo	Descripción
Seguimiento académico	1.	Sistema de notas	Software que permite la consulta y registro de notas de los estudiantes

Administración de planta física y recursos	2. Facturas de compra de productos y/o servicios	Soportes de compras institucionales
	3. Base de datos de inventario	Almacena la información correspondiente al inventario de la I. E

Nota: Adaptado de "Lineamientos Para La Gestión De Riesgos De Seguridad Digital En Entidades Públicas", por MinTIC, 2018, p. 12.

Identificar el responsable de los activos

A cada activo identificado se le deberá asignar un responsable, que vele y garantice la protección de dicho activo. (Ver Tabla 2).

Tabla 2

Responsable de activos

Activo	Descripción	Responsable del activo
Sistema de notas	Software que permite la consulta y registro de notas de los estudiantes	Coordinador
Facturas de compra de productos y/o servicios	Soportes de compras institucionales	Rector
Base de datos de inventario	Almacena la información correspondiente al inventario de la I. E	Secretaria – Aux. administrativo

Nota: Tomado de "Lineamientos Para La Gestión De Riesgos De Seguridad Digital En Entidades Públicas", por MinTIC, 2018, p. 13.

Clasificar *los activos*

Los activos deberán clasificarse de acuerdo a su naturaleza, por ejemplo: hardware, software, información entre otros. Para el caso de las IE los activos pueden ser clasificados como se muestra en la Tabla 3:

Tabla 3

Clasificación de activos

Tipo de activo	Descripción

Información	Información almacenada en formato físico o en formato digital. Se puede distinguir como información: contratos, documentos institucionales (PMI, PEI, manual de convivencia, planes de área, reportes, etc.), estados financieros, archivos ofimáticos, bases de datos con información relevante para algún proceso de la institución.
Software	Activo informático lógico como programas, herramientas ofimáticas (Word, Excel, PowerPoint, Access), sistema de información institucional (sistema de notas)
Hardware	Equipos físicos de cómputo (portátiles, Tablet, computadores de escritorio, servidores)
Recurso humano	Personas que por su valor para el proceso son considerados activos de información, por ejemplo: un asesor experto.
Instalaciones	Espacio físico que permite salvaguardar la información.
Otros	Otro tipo de activos, que no se encuentre listado anteriormente.

Nota: Adaptado de "Lineamientos Para La Gestión De Riesgos De Seguridad Digital En Entidades Públicas", por MinTIC, 2018, pp. 12-13.

La Tabla 4 muestra un ejemplo de clasificación de activos:

Tabla 4

Ejemplo clasificación de activos

Activo	Tipo de activo
Sistema de notas	Software
Facturas de compras institucionales	Información
Formatos de remisión de estudiantes	Información

Fuente: *elaboración propia*

Clasificar la información

Una vez clasificados los activos, se procede a realizar la clasificación de la información de dichos activos, para esto, se puede tener en cuenta lo establecido en las leyes 1712 de 2014 y 1581 de 2012.

- ✓ **Ley de transparencia 1712 de 2014**

"El objeto de la ley de transparencia es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información" (Ley 1712, 2014, art. 1).

Para determinar si la información es publicable o no, se deberá tener en cuenta la clasificación que propone la presente ley:

Información pública: Es la información que maneja un sujeto obligado (toda entidad pública).

Información pública clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley.

Información pública reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley. (Ley 1712, 2014, art. 6).

- ✓ **Ley 1581 de 2012: protección de datos personales**

Esta ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, teniendo como ámbito de aplicación los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada. Esta ley define el dato personal como cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581, 2012, art. 1-3).

A su vez, el dato personal se clasifica en:

Dato público: Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

Dato semiprivado: Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

Dato privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

> Dato sensible: Son aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.
>
> Se prohíbe el tratamiento de datos sensibles a menos que el titular haya dado su autorización explícita a dicho tratamiento. (Ley 1581, 2012, art. 3).

Teniendo en cuenta que en las IE se realiza el tratamiento de datos personales de estudiantes, padres de familia, empleados, y personas interesadas en adquirir servicios educativos, se deberá tener presente a la hora de identificar los activos de seguridad digital si éstos contienen o no datos personales. Por ejemplo, las IE pueden obtener datos personales de los estudiantes por medio de diferentes fuentes, tales como: formulario de inscripción, hoja de matrícula, registro de entrevistas a padres y estudiantes, observador del estudiante, ficha médica, formatos de remisión y atención psicológica o a docente orientador, evaluaciones o libro de valoraciones. Es importante resaltar que, para el tratamiento de datos personales de menores de edad, se debe contar con la autorización expresa de sus representantes legales y/o tutores.

De acuerdo con las leyes mencionadas anteriormente, en este paso de la identificación de los activos de seguridad digital, se deberá determinar qué tipo de información contiene cada uno de los activos, para ser tenido en cuenta a la hora de determinar la criticidad del mismo.

En la Tabla 5 se muestra un ejemplo de clasificación de la información:

Tabla 5

Clasificación de la información

Activo	Tipo de activo	Ley de transparencia (1712 de 2014)	Ley de protección de datos personales (1581 de 2012)
Formatos de remisión de estudiantes	Información	Información pública reservada	Dato sensible
Sistema de notas	Software	Información pública clasificada	Dato semiprivado
Base de datos de inventario	Información	Información pública	Dato público

Nota: Adaptado de "Lineamientos Para La Gestión De Riesgos De Seguridad Digital En Entidades Públicas", por MinTIC, 2018, pp. 14-15.

Determinar la criticidad del activo (Valoración del activo)

En este paso se determina el valor general del activo, es decir, se evalúa la criticidad de los activos, de tal forma que se pueda establecer su nivel de importancia, para tenerlo en cuenta a la hora de analizar el riesgo y poder valorarlo adecuadamente.

Una vez identificado el tipo de información de cada activo, la IE, deberá definir las escalas de criticidad: alta, media y baja, para valorar los activos en cuanto a su confidencialidad, integridad y disponibilidad y así poder identificar su criticidad.

- ✓ ***Clasificación de acuerdo con la confidencialidad***

"La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. Se definen tres niveles alineados con los tipos de información declarados en la ley 1712 del 2014" (MinTIC, 2016,

p. 16), mostrados en la Tabla 6.

Tabla 6

Esquema de clasificación por confidencialidad

Confidencialidad	
Información pública reservada (Alta)	Información disponible solo para un proceso de la IE y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
Información pública clasificada (Media)	Información disponible para todos los procesos de la IE y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de ésta. Esta información es propia de la IE o de terceros y puede ser utilizada por todos los funcionarios de la IE para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
Información pública (Baja)	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la IE, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
No clasificada	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información pública reservada.

Nota: Adaptado de "Guía para la Gestión y Clasificación de Activos de Información", por MinTIC, 2016, p. 16.

- ✓ ***Clasificación de acuerdo con la integridad***

"La integridad se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción" (MinTIC, 2016, p. 17). Se definen tres niveles de clasificación, mostrados en la Tabla 7.

Tabla 7

Esquema de clasificación por integridad

Integridad	
Alta	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económico, retrasar sus funciones, o generar pérdidas de imagen severas de la IE.
Media	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económico, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la IE.
Baja	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la IE o entes externos.
No clasificada	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad alta.

Nota: Adaptado de "Guía para la Gestión y Clasificación de Activos de Información", por MinTIC, 2016, p. 17.

- ✓ ***Clasificación de acuerdo con la disponibilidad***

"La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera ésta. Se definen tres niveles de clasificación" (MinTIC, 2016, p. 17). (Ver tabla 8).

Tabla 8

Esquema de clasificación por disponibilidad

	Disponibilidad
Alta	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económico, retrasar sus funciones, o generar pérdidas de imagen severas a la entidad o entes externos.
Media	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económico, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad o entes externos.
Baja	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
No clasificada	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad Alta.

Nota: Tomado de "Guía para la Gestión y Clasificación de Activos de Información", por MinTIC, 2016, pp. 17-18.

Una vez realizada la clasificación de los activos por su confidencialidad, integridad y disponibilidad, se determina la criticidad del activo (valor general del activo), definiendo las escalas de criticidad: alta, media y baja, para valorar dicho activo. (Ver Tabla 9)

Tabla 9

Niveles de clasificación

Nivel	Descripción

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.

Nota: Tomado de "Guía para la Gestión y Clasificación de Activos de Información", por MinTIC, 2016, p. 7.

En la tabla 10 se muestra un ejemplo de nivel de criticidad de activos:

Tabla 10

Ejemplo nivel de criticidad de activos

Activo	Tipo de activo	Criticidad respecto a su confidencialidad	Criticidad respecto a integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
Formatos de remisión de estudiantes	Información	ALTA	MEDIA	MEDIA	MEDIA
Sistema de notas	Software	MEDIA	MEDIA	BAJA	MEDIA
Base de datos de inventario	Información	BAJA	BAJA	BAJA	BAJA

Nota: Adaptado de "Lineamientos Para La Gestión De Riesgos De Seguridad Digital En Entidades Públicas", por MinTIC, 2018, p. 16.

6.1.3.2 Identificación del riesgo

Con base en la fase anterior (Caracterización del contexto: externo, interno, de proceso e identificación de activos de seguridad digital), se determinan las causas del riesgo, que permitirán su posterior identificación, "el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos" (DAFP, 2018b, p. 22).

La presente propuesta de investigación se enmarca en la tipología de riesgos mostrada en la figura 5, es decir que en esta fase de la metodología las IE podrán identificar riesgos de tipo físico, de gestión, de corrupción y de seguridad digital.

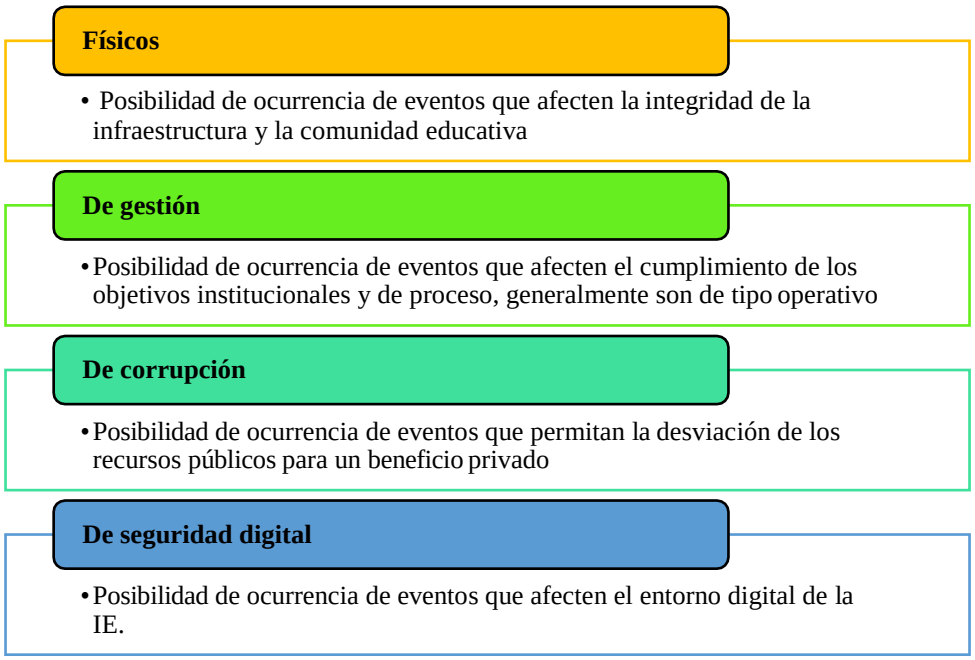


Figura 7 Tipología de riesgos. *Fuente:* elaboración propia

Para la identificación del riesgo, el DAFP sugiere tener en cuenta las siguientes preguntas: "¿Qué puede suceder?, ¿Cómo puede suceder?, ¿Cuándo puede suceder?, ¿Qué consecuencias tendría su materialización?" (DAFP, 2018b, p. 22).

El riesgo debe estar escrito de manera clara y precisa, se sugiere redactar los riesgos teniendo en cuenta el objetivo del proceso analizado, evitando iniciar con palabras negativas tales como "no…", "ausencia de…", "insuficiente…", en lugar de esto, se debe tratar de redactar el evento o riesgo como si ya estuviera sucediendo, ejemplo: "usuarios atendidos en forma deficiente", "obra ejecutada que incumple estándares de calidad", "programas institucionales operados de manera ineficiente", "posibilidad de ocurrencia de inundación", etc. Un ejemplo de un riesgo de gestión sería: "Compras institucionales ejecutadas de forma inadecuada".

Se sugiere realizar la descripción de los riesgos utilizando tablas, tal como las mostradas a continuación. Para identificar las causas y consecuencias se deben seguir

los pasos descritos en la sección 6.1.4.1 del presente documento (Análisis de riesgos).

La Tabla 11 muestra un ejemplo de descripción de un riesgo de tipo físico: “posibilidad de ocurrencia de un conato de incendio”

Tabla 11

Ejemplo riesgo físico

Riesgo	Descripción	Tipo	Causas	Consecuencias
Posibilidad de ocurrencia de un conato de incendio	Debido al inadecuado mantenimiento de las instalaciones eléctricas, la ausencia de la brigada, el equipamiento contra incendios, y la necesidad de capacitación para la respuesta a emergencias, se puede generar un riesgo físico que conlleve a la posibilidad de ocurrencia de un conato de incendio	FISICO	Inadecuado o inexistente mantenimiento a las instalaciones eléctricas Ausencia de equipamiento contra incendios Ausencia de brigada contra incendios Necesidad de capacitación para la respuesta a emergencias	interrupción del servicio educativo daños en las instalaciones peligro para la comunidad educativa

Nota: Adaptado de “Guía para la administración del riesgo y el diseño de controles en *entidades públicas”*, por DAFP,2018, p. 30.

Para el caso de los riesgos físicos, adicional a la descripción del riesgo, se recomienda realizar una representación visual del escenario del riesgo de la IE (puede ser el plano del establecimiento educativo y su entorno), mediante el cual se analizan las causas y consecuencias del riesgo. Esta representación puede diseñarse de diferentes formas, por ejemplo: un croquis, una maqueta, un mapa (MEN,2015, p. 43).

En el caso de los riesgos de gestión (se refieren a los riesgos de tipo operativo), se sugiere diligenciar la Tabla 12:

Tabla 12

Ejemplo riesgo de gestión

Riesgo	Descripción	Tipo	Causas	Consecuencias
Proceso de matrícula de estudiantes ejecutado de forma inadecuada	Situaciones como la falta de controles para la realización de matrículas, la falta de capacitación en el proceso de matrículas y uso de plataforma (SIMAT), documentación de estudiantes incompleta, pueden generar un riesgo operativo en el proceso de matriculas	OPERATIVO	Ausencia de controles en el procedimiento de matrícula Insuficiente capacitación en el procedimiento de matrículas y uso de plataforma (SIMAT) Inadecuada verificación del cumplimiento de requisitos de los estudiantes	Demandas y acciones jurídicas Pérdida de imagen institucional Investigaciones disciplinarias

Nota: Adaptado de "Guía para la administración del riesgo y el diseño de controles en entidades públicas", por DAFP,2018, p. 30.

Con respecto a los riesgos de corrupción, es preciso mencionar que éstos se definen a partir de los siguientes componentes: 1. Acción u omisión, 2. Uso del poder, 3.

Desviación de la gestión de lo público, 4. Beneficio privado (DAFP, 2018b, p. 23).

En este sentido, para identificar si un riesgo es o no de corrupción, se puede utilizar la matriz sugerida por el DAFP, plasmada en la tabla 13, la cual define que, si el riesgo aplica a todos y cada uno de estos componentes, se trata de un riesgo de corrupción, es decir, si se marca con una x cada una de las casillas de la tabla, el riesgo descrito se identificará como de corrupción.

Tabla 13

Matriz definición de riesgo de corrupción

Matriz: definición de riesgo de corrupción				
Descripción del riesgo	Acción u omisión	Uso del poder	Desviar la gestión de lo público	Beneficio privado

Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato de compra	X	X	X	X

Nota: Tomado de "Guía para la administración del riesgo y el diseño de controles en entidades públicas", por DAFP,2018, p. 24.

Se mencionan algunas actividades susceptibles de riesgos de corrupción, cada IE podrá tener en cuenta otros que considere pertinente:

Concentración de autoridad o exceso de poder; ausencia de canales de comunicación; inversiones de dineros públicos en entidades de dudosa solidez financiera a cambio de beneficios indebidos para servidores públicos encargados de su administración; estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación (estableciendo necesidades inexistentes o aspectos que benefician a una firma en particular); ausencia de sistemas de información; cobros asociados a trámites; tráfico de influencias: (amiguismo, persona influyente). (DAFP,2018b, p.32)

La tabla 14 muestra un ejemplo de un riesgo de corrupción

Tabla 14

Ejemplo riesgo de corrupción

Riesgo	Descripción	Tipo	Causas	Consecuencias

Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato de compra	Debilidades en la etapa de planeación del contrato, poca efectividad del consejo directivo, excesiva discrecionalidad, la falta de conocimiento y/o experiencia del rector	CORRUPCIÓN	Debilidades en la etapa de planeación, que facilitan la inclusión de requisitos orientados a beneficiar a un proponente Carencia de controles y verificación por parte del consejo directivo en el procedimiento de contratación Falta de conocimiento y/o experiencia para celebrar contratos por parte del rector Excesiva discrecionalidad	Pérdida de la imagen institucional Demandas Pérdida de confianza en lo público Investigaciones penales, disciplinarias y fiscales Obras inconclusas Mala calidad de las obras Enriquecimiento ilícito de servidores públicos

Nota: Adaptado de "Guía para la administración del riesgo y el diseño de controles en entidades públicas", por DAFP,2018, p. 31.

Con respecto a los riesgos de seguridad digital:

Éstos se basan en la afectación de tres criterios en un activo o grupo de activos dentro del proceso: integridad, confidencialidad y disponibilidad. En este sentido, se podrán identificar los siguientes tres tipos de riesgos: pérdida de la confidencialidad, pérdida de la integridad y pérdida de la disponibilidad. (DAFP,2018b, pp. 34-35).

Se deben agrupar por tipo los activos o el grupo de activos específicos del proceso, y luego para cada riesgo de seguridad digital se deberán identificar posibles amenazas y vulnerabilidades que pueden facilitar su aparición.

En la tabla 15 se muestra un ejemplo de la descripción de un riesgo de seguridad digital:

Tabla 15

Descripción riesgo de seguridad digital

Riesgo	Activo	Descripción del riesgo	Amenaza	Tipo	Causas/ vulnerabilidades	Consecuencias
Pérdida de la integridad	Sistema de notas	El uso de contraseñas sin protección, la falta de entramiento en el manejo del sistema de notas, la ausencia de conciencia en seguridad digital y políticas de uso aceptable, pueden facilitar una modificación no autorizada, lo cual ocasionaría la pérdida de la integridad del sistema de notas.	Modificación no autorizada	Seguridad digital	Contraseñas sin protección Entrenamiento insuficiente Falta de conciencia en seguridad digital Ausencia de políticas de uso aceptable	Pérdida de confianza en la gestión académica detrimento de la imagen institucional demandas

Nota: Adaptado de "Guía para la administración del riesgo y el diseño de controles en entidades públicas", por DAFP,2018, p. 34.

A continuación, se dan las indicaciones para poder identificar las amenazas y las vulnerabilidades del activo, a manera de ejemplo, en la Tabla 16 se listan las siguientes amenazas que pueden afectar a los activos y materializarse en riesgos, indicando si se dan de forma deliberada (D), por la acción humana de forma accidental (A), y ambientales (AM).

Tabla 16

Ejemplo de amenazas comunes

Tipo de amenaza	Amenaza	Origen
Daño físico	Fuego	D, A, AM
	Daño por agua	
Eventos naturales	Fenómenos climáticos	AM
	Inundación	
Pérdida de los servicios esenciales	Pérdida de suministro de energía	D, A, AM
	Falla en el sistema de suministro de agua o aire acondicionado	D, A

Perturbación debida a la radiación	Radiación electromagnética	D, A, AM
	Radiación térmica	D, A, AM
Compromiso de la información	Hurto de equipos, medios o documentos	D
	Divulgación	D, A
	Manipulación con software	D, A
Fallas técnicas	Mal funcionamiento del equipo o del software	A
	Saturación del sistema de información	D, A
Acciones no autorizadas	Uso no autorizado del equipo	D
	Uso de software falso o copiado	D, A
	Procesamiento ilegal de los datos	D
Compromiso de las funciones	Error en el uso o abuso de derechos	D, A
	Falsificación de derechos	D

Nota: Tomado de "Norma técnica colombiana NTC-ISO/IEC 27005", por ICONTEC, 2009, p. 56.

Es recomendable tener en cuenta las fuentes de amenazas dirigidas por el hombre, en la tabla 17 se muestran ejemplos de este tipo:

Tabla 17

Ejemplos de amenazas dirigidas por el hombre

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso ilegal	Reto, ego, dinero	Piratería, Ingeniería social, intrusión, acceso forzado al sistema
Criminal de la computación	Destrucción de información, divulgación ilegal de información, alteración no autorizada de datos	Suplantación de identidad, intrusión en el sistema, acto fraudulento
Terrorismo	Chantaje, destrucción	Ataques contra el sistema, penetración en el sistema, manipulación del sistema
Espionaje industrial (inteligencia, empresas, otros intereses gubernamentales)	Ventaja competitiva Espionaje económico	Hurto de información, penetración en el sistema, ingeniería social
Intrusos (empleados con entrenamiento deficiente, descontentos, deshonestos o despedidos)	Curiosidad, errores y omisiones no intencionales Ganancia monetaria	Chantaje, uso inadecuado del computador, fraude y hurto, sabotaje y/o acceso no autorizado al sistema

Nota: Tomado de "Norma técnica Colombiana NTC-ISO/IEC 27005", por ICONTEC, 2009, p. 57.

De igual forma, se deben identificar las vulnerabilidades que pueden facilitar la

materialización de riesgos de tipo de seguridad digital. Se debe tener presente que “la sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad” (MinTIC, 2018, p. 22).

En la tabla 18 se presentan ejemplos de amenazas y vulnerabilidades de los activos:

Tabla 18

Ejemplo de amenazas y vulnerabilidades

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Información	Falta de controles de acceso a la información	Hurto de información
	Ausencia de soportes de remisiones de casos de estudiantes	Incumplimiento de la norma
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
Hardware	Almacenamiento sin protección	Hurto de equipos, medios o documentos
	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
	Ausencia de “terminación de la sesión” cuando se abandona la estación de trabajo	Abuso de derechos
Software		

	Interf	az de usuario compleja	Error en el uso Ausencia de
		mecanismos de identificación y autentificación, como la autentificación de usuario Contraseñas sin protección	Falsificación de derechos
Red		Conexión deficiente de los cables	Falla del equipo de telecomunicaciones
		Conexiones de red pública sin protección	Uso no autorizado del equipo Uso incorrecto de software y hardware Error en el uso
	Personal	Entrenamiento insuficiente y/o falta de conciencia acerca de la seguridad	Error en el uso
		Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
		Ubicación en un área susceptible de inundación	Inundación
	Instalaciones	Red energética inestable	Pérdida del suministro de energía
		Ausencia de protección física de la edificación, puertas y ventanas	Hurto de equipo

Nota: Adaptado de "Lineamientos Para La Gestión De Riesgos De Seguridad Digital En Entidades Públicas", por MinTIC, 2018, p. 22.

Al finalizar este paso de la metodología, la IE obtendrá la caracterización de su contexto (interno, externo, de los procesos y de activos de seguridad digital), destacando la importancia que tiene la apropiación de la administración del riesgo por medio de su incorporación curricular en los planes de estudio, proyectos de aula, transversales, etc. De igual forma, en este paso se obtiene la identificación de los diferentes riesgos, resaltando la importancia de representar el escenario o mapa de riesgo en los riesgos físicos, el cual facilitará el desarrollo de los pasos 5, 6 y 7 de la presente metodología (respuesta a emergencias).

6.1.4 Paso 4. Valoración de riesgos

En este paso de la metodología se realiza el análisis de los riesgos y su evaluación, de tal forma que se determine qué tan probable es que ocurra el riesgo y su nivel de impacto, para así poder obtener el riesgo inherente (zona de riesgo inicial), y luego confrontar los resultados de dicho análisis con los controles definidos por la IE, para poder establecer el riesgo residual (zona de riesgo final).

De acuerdo con lo anterior, la valoración de riesgos se desarrolla en dos fases, la primera es la del análisis de riesgos, y la segunda la de evaluación de riesgos, para finalmente realizar el reporte del plan de tratamiento de riesgos.

6.1.4.1 Análisis de riesgos

Esta fase se realiza siguiendo los pasos listados a continuación:

I. Análisis de causas

Para conocer las causas que dan origen a los riesgos, se deben tener en cuenta las actividades críticas dentro del grupo de actividades que apuntan al logro de los objetivos.

Una vez realizada la caracterización del contexto, se obtienen las diferentes causas que pueden originar la materialización de riesgos, estas causas se deben priorizar para determinar las causas raíz, cada IE determinará la herramienta más apropiada para priorizar dichas causas.

Se pueden utilizar herramientas que permitan realizar el análisis de causas, tales como: matriz DOFA, 5 porqué o 3 porqué, espina de pescado, lluvia de ideas, análisis que pasa si, entre otras.

A modo de ejemplo se muestra la herramienta matriz de priorización, la cual se

diligencia a través de los siguientes pasos:

1. Liste las causas identificadas 2. Cada uno de los integrantes del proceso deberá numerar las causas de menor a mayor importancia donde 1 es la menos importante y el número más alto (en el ejemplo del siguiente cuadro 5) es la más importante 3. En un cuadro, transcriba las calificaciones de cada miembro del equipo en las columnas 4. Totalice las calificaciones de cada causa y determine el promedio (divida por el número de miembros del equipo que participaron) 5. Las causas que obtengan los mayores puntajes son las causas raíz 6. Establezca las actividades de control que requiera para cada causa. (DAFP, 2018a, p. 6).

La Tabla 19 muestra un ejemplo de la matriz de priorización del proceso apoyo a la gestión académica, cuyo riesgo es “Proceso de matrícula de estudiantes ejecutado de forma inadecuada”:

Tabla 19

Matriz de priorización

No.	Causas	P1	P2	P3	P4	P5	Total	Promedio
1	Ausencia de controles en el procedimiento de matrícula	5	5	4	5	4	23	4,6
2	Registro incorrecto en SIMAT (Sistema Integrado de Matrícula)	3	4	4	4	3	18	3,6
3	Cálculo incorrecto de la cobertura institucional	3	3	3	4	4	17	3,4
4	Insuficiente capacitación en el procedimiento de matrículas y uso de plataforma (SIMAT)	5	4	5	4	4	22	4,4
5	Inadecuada planeación de la continuidad de los alumnos matriculados (reserva de cupo)	4	3	3	3	4	17	3,4
6	Inadecuada verificación del cumplimiento de requisitos de los estudiantes	4	5	5	4	5	23	4,6

P1=participante 1, P2= participante 2……

Nota: Adaptado de "Anexo 5 Análisis y priorización de causas", por MinTIC, 2018, p. 7.

Como causas raíz se obtienen la de mayor puntuación, resaltadas en la tabla anterior: la ausencia de controles en el procedimiento de matrícula, la insuficiente capacitación en el procedimiento de matrículas y uso de plataforma (SIMAT), y la inadecuada verificación del cumplimiento de requisitos de los estudiantes.

II. Determinar probabilidad

Para determinar la probabilidad de ocurrencia del riesgo se tiene en cuenta la frecuencia o factibilidad.

La frecuencia se obtiene analizando la cantidad de veces que se presentan situaciones o eventos asociados al riesgo en un período determinado de tiempo, mientras que con el criterio de factibilidad se analizan los sucesos que no se han presentado, pero que posiblemente pueden presentarse. Cada IE deberá establecer las pautas para determinar la probabilidad de ocurrencia del riesgo.

Si en la IE se han materializado eventos o se tienen datos históricos de situaciones asociadas al riesgo, se deberá establecer la relación entre el nivel de probabilidad y la frecuencia de ocurrencia del evento, para esto deberán diligenciar los datos, tal como se muestra en la Tabla 20:

Tabla 20

Criterios para determinar la probabilidad

Nivel	Descriptor	Descripción	Frecuencia
5	Casi seguro	Se espera que el evento ocurre en la mayoría de las circunstancias	Más de 1 vez al año
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez al año
3	Posible	El evento podrá ocurrir en cualquier momento	Al menos 1 vez en los últimos dos años
2	Improbable	El evento puede ocurrir en cualquier momento	Al menos 1 vez en los últimos 5 años
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años

Nota: Adaptado de "Guía para la administración del riesgo y el diseño de controles en entidades públicas", por DAFP,2018, p. 39.

Si, por el contrario, en la IE no se cuenta con un registro sobre la cantidad de situaciones que se han presentado en un lapso de tiempo, cada una de las personas que conforma el CARAE deberá de forma individual, calificar la probabilidad de acuerdo con la factibilidad, para esto pueden utilizar una matriz de priorización de probabilidad, tal como la explicada en la tabla 21.

En la siguiente tabla, se listarán los riesgos relacionados al proceso, y cada participante dará una calificación de 1 a 5, en donde 1 será el menor nivel de probabilidad de ocurrencia, y 5 corresponderá a la mayor probabilidad de ocurrencia.

Tabla 21

Ejemplo matriz de priorización de probabilidad en el proceso clima escolar

No.	Riesgo	P1	P2	P3	P4	P5	Total	Promedio
1	Posibilidad de ocurrencia de un conato de incendio	3	3	2	3	3	14	3 Posible
2	Programa de inducción y de acogida a estudiantes nuevos ejecutado de manera inadecuada	5	5	4	5	5	24	5 Casi seguro
3	Aguas residuales tratadas de manera ineficiente	4	5	3	4	4	20	4 Probable

P1=participante 1, P2= participante 2……

Fuente: propia de autor

III. Determinar consecuencias o nivel de impacto

El riesgo se puede calificar según su nivel de impacto, clasificándose en alguno de los siguientes: insignificante, menor, moderado, mayor y catastrófico. Se sugiere que cada IE ajuste los criterios teniendo en cuenta su realidad.

La Tabla 22 muestra un ejemplo de criterios para calificar el impacto de los riesgos físicos.

Tabla 22

Criterios para calificar el impacto - Riesgos físicos

Impacto	Descriptor
Catastrófico	Los efectos del evento afectan entre el 76% y el 100% de la IE. Generación de muertes y/o pérdidas de grandes montos de dinero.
Mayor	Los efectos del evento afectan entre el 51% y el 75% de la IE. Generación de alguno heridos y/o pérdidas económicas considerables
Moderado	Los efectos del evento afectan entre el 26% y el 50% de la IE. Generación de lesiones personales de no mucha gravedad y/o pérdidas económicas
Menor	Los efectos del evento afectan entre el 1% y el 25% de la IE. Generación de lesiones personales muy leves y/o pequeñas pérdidas económicas
Insignificante	Los efectos del evento no afectan la infraestructura de la IE. No se generan heridos ni pérdidas económicas de consideración.

Nota: Adaptado de "Guía para la administración del riesgo y el diseño de controles en entidades públicas", por DAFP,2018, p. 40.

La Tabla 23 muestra un ejemplo de criterios para calificar el impacto de los riesgos de gestión.

Tabla 23

Criterios para calificar el impacto - Riesgos de gestión

Impacto	Descriptor
Catastrófico	Interrupción de las operaciones de la IE por más de diez (10) días Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. Pérdida de información crítica para la IE que no se puede recuperar Imagen institucional afectada en el orden regional o nacional por actos o hechos de corrupción comprobadas.
Mayor	Interrupción de las operaciones de la IE por más de cinco (5) días Sanción por parte del ente territorial Pérdida de información crítica para la IE que puede ser recuperada de forma parcial o incompleta Imagen institucional afectada en el orden regional o nacional por incumplimiento en la prestación del servicio a la comunidad educativa
Moderado	Interrupción de las operaciones de la IE por más de dos (2) días Reclamaciones o quejas de la comunidad educativa que podrían implicar una denuncia o demanda ante el ente territorial Inoportunidad en la información, ocasionando retrasos en la atención de la comunidad educativa Imagen institucional afectada en el orden regional o nacional por retrasos en la prestación del servicio a la comunidad educativa
Menor	Interrupción de las operaciones de la IE por algunas horas Reclamaciones o quejas de la comunidad educativa que implican investigaciones internas disciplinarias Imagen institucional afectada en el orden local por retrasos en la prestación del servicio a la comunidad educativa
Insignificante	No hay interrupción de las operaciones de la IE No se generan sanciones por parte de Ningún ente No se afecta la imagen institucional de forma significativa

Nota: Adaptado de "Guía para la administración del riesgo y el diseño de controles en entidades públicas", por DAFP,2018, p. 40.

"Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles "moderado", "mayor" y "catastrófico", dado que estos riesgos siempre serán significativos" (DAFP,2018b, p. 47). Ver tabla 24.

Tabla 24

Criterios para calificar el impacto - Riesgos de corrupción

No.	Pregunta: Si el riesgo de corrupción se materializa podría…	Respuesta SI	 NO
1	¿Afectar al grupo de funcionarios del proceso?		

2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?
3	¿Afectar el cumplimiento de misión de la entidad?
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?
6	¿Generar pérdida de recursos económicos?
7	¿Afectar la generación de los productos o la prestación de servicios?
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?
9	¿Generar pérdida de información de la entidad?
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?
11	¿Dar lugar a procesos sancionatorios?
12	¿Dar lugar a procesos disciplinarios?
13	¿Dar lugar a procesos fiscales?
14	¿Dar lugar a procesos penales?
15	¿Generar pérdida de credibilidad del sector?
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?
17	¿Afectar la imagen regional?
18	¿Afectar la imagen nacional?
19	¿Generar daño ambiental?

Responder afirmativamente de UNA a CINCO preguntas genera un impacto moderado Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor
Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico

Moderado: Genera medianas consecuencias para la IE

Mayor: Genera altas consecuencias para la IE

Catastrófico: Genera consecuencias desastrosas para la IE

Nota: Adaptado de "Guía para la administración del riesgo y el diseño de controles en entidades públicas", por DAFP,2018, p. 46.

Por su parte, la Tabla 25 muestra un ejemplo de criterios para calificar el impacto de los riesgos de seguridad digital.

Tabla 25

Criterios para calificar el impacto - Riesgos de seguridad digital

Impacto	Descriptor
Catastrófico	Afectación muy grave de la integridad, disponibilidad y confidencialidad de la información
Mayor	Afectación grave de la integridad, disponibilidad y confidencialidad de la información
Moderado	Afectación moderada de la integridad, disponibilidad y confidencialidad de la información

Menor	Afectación leve de la integridad, disponibilidad y confidencialidad de la información
Insignificante	Sin afectación de la integridad, disponibilidad y confidencialidad de la información

Nota: Adaptado de "Guía para la administración del riesgo y el diseño de controles en entidades públicas", por DAFP,2018, p. 42.

IV. Estimar el nivel de riesgo inicial – Inherente

Una vez obtenida la probabilidad y el impacto del riesgo se procede a determinar el riesgo inicial o inherente, utilizando la matriz de calificación del riesgo. Ver figura 6.

En la Tabla 26 se muestra un ejemplo de estimación de riesgo inherente de seguridad digital, analizando el riesgo "pérdida de la integridad". Para comenzar, se toma la probabilidad que se obtuvo en la matriz de priorización de probabilidad, tabla 21, y posteriormente se obtiene el impacto (por ser un riesgo de seguridad digital se consulta la tabla 25), para determinar el nivel del riesgo.

Tabla 26

Probabilidad e impacto riesgo de seguridad digital

Riesgo	Activo	Amenaza	Causas/ vulnerabilidades	Probabilidad	Impacto
Pérdida de la integridad	Sistema de notas	Modificación no autorizada	Contraseñas sin protección Entrenamiento insuficiente Falta de conciencia en seguridad digital Ausencia de políticas de uso aceptable	Probable	Moderado

Nota: Adaptado de "Guía para la administración del riesgo y el diseño de controles en entidades públicas", por DAFP,2018, p. 44.

Se ubica en la matriz de calificación de riesgo o mapa de calor, la calificación de probabilidad e impacto, en las filas se ubicará el valor de la probabilidad y en las columnas el del impacto, el punto de intersección corresponderá al nivel del riesgo.

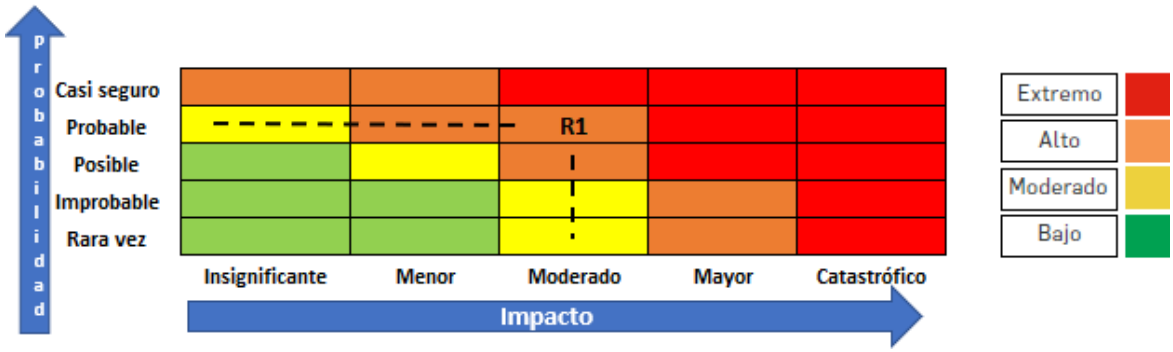


Figura 8 Matriz de calificación de riesgo - Mapa de calor. Adaptado de "Guía para la administración del riesgo y el diseño de controles en entidades públicas". *Fuente:* DAFP,2018, p. 45.

En este caso, el riesgo de pérdida de la integridad (R1) se ubica en el nivel alto, lo que indica que es probable que exista pérdida de integridad de la información del sistema de notas debido a una modificación no autorizada, generando un impacto moderado en la IE, toda vez que la información del sistema perdería su veracidad y confiabilidad.

Se debe tener presente que, aunque en los riesgos de corrupción el mapa de calor empleado es el mismo, se deberán omitir las columnas de los niveles de impacto insignificante y

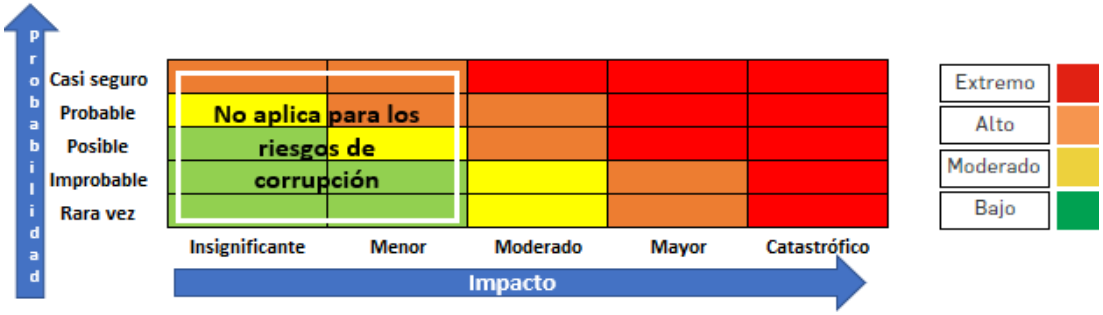


Figura 9 Mapa de calor riesgos de corrupción. Adaptado de "Guía para la administración del riesgo y el diseño de controles en entidades públicas". *Fuente:* DAFP,2018, p. 47

menor, debido a que en este tipo de riesgos solo se tienen en cuenta los impactos de nivel moderado, mayor y catastrófico, para la probabilidad se utilizan los mismos cinco niveles que aplican a los demás riesgos. (Ver figura 7).

6.1.4.2 Evaluación de riesgos

Con el nivel de riesgo inherente identificado y sus causas, se procede a identificar los controles que permiten mitigar la ocurrencia del riesgo (valoración de controles). Para cada causa debe existir un control, siendo posible que un control sea lo suficientemente efectivo para apuntar a varias causas. Luego se determina el nivel de riesgo residual (después de los controles) y por último se establece el tratamiento o respuesta dada al riesgo. (Ver figura 8).

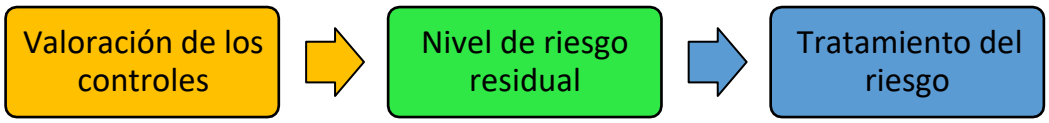


Figura 10 Evaluación de riesgos. Fuente: elaboración propia

I. Valoración de los controles

Para realizar la valoración de los controles, primero se debe entender cómo se diseña un control, de tal manera que permita la mitigación del riesgo (DAFP,2018b, p. 49).

A continuación, se explican cada uno de los pasos que se deben seguir para poder realizar el diseño y la valoración del control:

Paso 1. Responsable: Definir el encargado de realizar la actividad de control, sea una persona (establecer el cargo) o un sistema. Ejemplo: rector, coordinador, secretaria, SIMAT, sistema de notas, etc.

Paso 2. Periodicidad: Establecer la frecuencia de ejecución (diario, semanal, quincenal, etc.). Ejemplo: La secretaria: diariamente, el docente orientador: semanalmente, consejo académico: trimestralmente.

En el caso de los controles que no tienen una periodicidad específica, se debe manifestar cada cuánto se realiza. Ejemplo: que cada vez que se desarrolla la actividad se ejecuta el control. Ejemplo: Cada vez que se realiza una compra institucional se ejecuta el control. El SIMAT, cada

vez que se realiza una matrícula.

Paso 3. Propósito: Expresar cuál es la intención del control, es decir, para qué se diseña, indicando si es preventivo o detectivo, se debe redactar en infinitivo, ejemplo: validar, comprobar, revisar, etc.

Ejemplo: Comprobar que los datos que proporciona el proveedor corresponden con los requerimientos de la compra.

Paso 4. Cómo se realiza: Se debe explicar el procedimiento que se sigue para ejecutar el control. Ejemplo: para validar si un estudiante cumple con todos los requisitos para legalizar la matrícula, se debería utilizar una lista de chequeo que permita confirmar que se cumple con todos los requisitos.

Paso 5. Qué pasa con las observaciones o desviaciones: Se debe realizar seguimiento a las novedades que surjan durante la ejecución del control, indicando que se hace con ellas. Ejemplo: En caso de encontrar información faltante a la hora de realizar la matrícula, se requerirá al padre de familia y/o acudiente completar la documentación para poder seguir con el proceso.

Paso 6. Evidencia: Ejecutado el control, debe existir una evidencia.

A continuación, se muestra un ejemplo de un control para el riesgo “proceso de matrícula de estudiantes ejecutado de forma inadecuada”, el cual se identifica como control

1. Este control cumple con todos los criterios explicados anteriormente, ejemplo: cada vez que se realiza un proceso de matrícula, la secretaria valida por medio de una lista de chequeo que la documentación recibida por parte del acudiente y/o padre de familia corresponde con los requerimientos definidos por la institución. Si llegase a faltar información al momento de realizar la matrícula, se requerirá al padre de familia y/o acudiente completar la documentación para poder seguir con el proceso. Evidencia: Lista de chequeo diligenciada, hoja de matrícula diligenciada y firmada. Registro de estudiante en SIMAT.

Para realizar la valoración de los controles, se debe tener en cuenta que para la adecuada mitigación de los riesgos no basta con que un control esté bien diseñado, éste debe ejecutarse por parte de los responsables tal como se diseñó. Un control que no se ejecute, o un control que se ejecute y esté mal diseñado, no va a contribuir a la mitigación del riesgo (DAFP,2018b, p. 59).

Es recomendable diligenciar las tablas mostradas a continuación para valorar el diseño de los controles.

Se inicia con la tabla 27, la que permite realizar el análisis y la evaluación del diseño del control.

Tabla 27

Análisis y evaluación del diseño del control

Criterio de evaluación	Aspecto a evaluar en el diseño del control	Opciones de respuesta	
1. Responsable	¿Existe un responsable asignado a la ejecución del control?	Asignado	No asignado
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado	Inadecuado
2. Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna	Inoportuna
3. Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, Ej.: verificar, validar, cotejar, comparar, revisar, etc.?	Prevenir o detectar	No es un control

4. Cómo se realiza la actividad de control	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	Confiable	No confiable
5. Qué pasa con las observaciones o desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven Oportunamente	No se investigan y resuelven oportunamente
6. Evidencia de la ejecución del control	¿Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión?	Completa	Incompleta / no existe

Nota: Tomado de "Guía para la administración del riesgo y el diseño de controles en entidades públicas", por DAFP,2018, p. 60.

Luego, la Tabla 28 establece el peso de cada variable en el diseño del control.

Tabla 28

Peso de cada variable en el diseño del control

Criterio de evaluación	Opción de respuesta al criterio de evaluación	Peso en la evaluación del diseño del control
1.1 Asignación del responsable	Asignado	15
	No asignado	0
1.2 Segregación y autoridad del responsable	Adecuado	15
	Inadecuado	0
2. Periodicidad	Oportuna	15
	Inoportuna	0
3. Propósito	Prevenir	15
	Detectar	10
	No es un control	0
4. Cómo se realiza la actividad de control	Confiable	15
	No confiable	0
5. Qué pasa con las observaciones o desviaciones	Se investigan y resuelven oportunamente	15
	No se investigan y resuelven oportunamente	0
6. Evidencia de la ejecución del control	Completa	15
	Incompleta	10
	No existe	0

Nota: Tomado de "Guía para la administración del riesgo y el diseño de controles en entidades públicas", por DAFP,2018, p. 61.

Por último, la Tabla 29 muestra la calificación del diseño del control.

Tabla 29

Resultados de la evaluación del diseño del control

Rango de calificación del diseño	Resultado – Peso en la evaluación del diseño del control
Fuerte	Calificación entre 96 y 100
Moderado	Calificación entre 86 y 95
Débil	Calificación entre 0 y 85

Nota: Tomado de "Guía para la administración del riesgo y el diseño de controles en entidades públicas", por DAFP,2018, p. 62.

Para que un control se evalúe como bien diseñado, deben cumplirse todas las variables, en este sentido, "si el diseño de los controles está por debajo de 96, se debe establecer un plan de acción que permita tener un control o controles bien diseñados" (DAFP, 2018b, p.62).

Tomando como ejemplo el control 1, se evidencia que cumple con todos los criterios establecidos en la tabla 27, obteniendo como resultado una calificación de 100, lo que indica que el diseño del control es fuerte.

De igual manera se deberá evaluar si el control se ejecuta tal como fue diseñado, indicando si su ejecución es fuerte, moderado o débil. (Ver tabla 30).

Tabla 30

Resultados de la evaluación de la ejecución del control

Rango de calificación de la ejecución	Resultado: Peso de la ejecución del control
Fuerte	El control se ejecuta de manera consistente por parte del responsable
Moderado	El control se ejecuta algunas veces por parte del responsable
Débil	El control no se ejecuta por parte del responsable

Nota: Tomado de "Guía para la administración del riesgo y el diseño de controles en entidades públicas", por DAFP,2018, p. 62.

Al evaluar la ejecución del control 1, se obtiene como resultado de la evaluación una calificación fuerte, ya que el responsable, en este caso, la secretaria, lo ejecuta correctamente.

Análisis y evaluación de los controles

Debido a que la calificación del riesgo se efectúa al riesgo y no a cada causa, hay que consolidar el conjunto de los controles asociados a las causas, para evaluar si estos de manera individual y en conjunto ayudan al tratamiento de los riesgos, considerando tanto el diseño, ejecución individual y promedio de los controles. (DAFP, 2018b, p.63).

La valoración del control se realiza teniendo en cuenta su solidez (diseño y ejecución), un control es sólido si está bien diseñado y ejecutado.

Teniendo en cuenta que tanto la variable de diseño como la variable de ejecución del control son de importancia para tratar los riesgos, cada control obtendrá su solidez de acuerdo a la variable que tenga menor calificación. (Ver tabla 31).

Tabla 31

Solidez individual de cada control

Peso del diseño de cada control	Peso de la ejecución de cada control	Solidez individual de cada control Fuerte: 100 Moderado: 50 Débil: 0	Debe establecer acciones para fortalecer el control: Si/No
Fuerte: calificación entre 96 y 100	Fuerte (siempre se ejecuta)	Fuerte + fuerte = fuerte	No
	Moderado (Algunas veces se ejecuta)	Fuerte + moderado = moderado	Sí
	Débil (No se ejecuta)	Fuerte + débil = débil	Sí
Moderado: calificación entre 86 y 95	Fuerte (siempre se ejecuta)	Moderado + fuerte= moderado	Sí
	Moderado (Algunas veces se ejecuta)	Moderado + moderado = moderado	Sí
	Débil (No se ejecuta)	Moderado + débil = débil	Sí
Débil: calificación entre 0 y 85	Fuerte (siempre se ejecuta)	Débil + fuerte = débil	Sí
	Moderado (Algunas veces se ejecuta)	Débil + moderado = débil	Si
	Débil (No se ejecuta)	Débil + débil = débil	Sí

Nota: Tomado de "Guía para la administración del riesgo y el diseño de controles en entidades públicas", por DAFP,2018, p. 63.

Siguiendo con el ejemplo del control 1, éste tiene una calificación de 100 tanto en el diseño como en su ejecución, por lo tanto, la solidez individual dará como resultado una valoración fuerte (100), no necesitando en este caso ninguna acción para fortalecerlo.

A modo de ejemplo, digamos que se tienen dos controles más para mitigar el riesgo: El control 2, tiene una calificación moderada en su diseño, y fuerte en su ejecución, lo que da como resultado una solidez individual moderada (50).

Por su parte el control 3, tiene una calificación de fuerte en su diseño y de moderado en su ejecución, dando como resultado una solidez individual moderada (50).

Solidez del conjunto de controles

Debido a que un riesgo puede tener varias causas y cada causa puede tener asociados varios controles, se hace necesario que, una vez obtenida la solidez individual de cada control, se califique la solidez del conjunto de controles asociados al riesgo. (Ver figura 9).

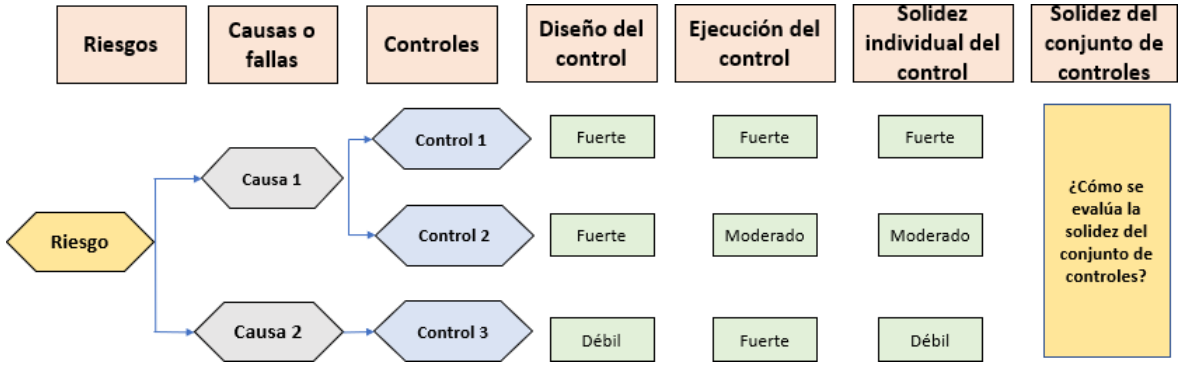


Figura 11 Solidez del conjunto de controles. *Tomado de "Guía para la administración del riesgo y el diseño de controles en entidades públicas". Fuente: DAFP,2018, p. 64.*

"La solidez del conjunto de controles se obtiene calculando el promedio aritmético simple de los controles por cada riesgo" (DAFP, 2018b, p.64). La Tabla 32 muestra la calificación de la solidez del conjunto de controles.

Tabla 32

Solidez del conjunto de controles

Calificación de la solidez del conjunto de controles	
Fuerte	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100.
Moderado	El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre 50 y 99.
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50.

Nota: Tomado de "Guía para la administración del riesgo y el diseño de controles en entidades públicas", por DAFP,2018, p. 64.

Siguiendo el ejemplo con los controles 1, 2 y 3, mencionados anteriormente, para obtener la solidez del conjunto de controles, se calcula el promedio aritmético de los mismos, el control 1

tiene una solidez individual de 100, por su parte los controles 2 y 3 tienen una solidez individual de 50 cada uno, al sumarlos y ponderarlos da como resultado una calificación de 67, es decir que la solidez del conjunto de controles es moderada.

II. Nivel de riesgo -Riesgo residual

Después de analizar el riesgo y evaluar los controles, se elabora el mapa de riesgo residual (ver figura 11).

Para explicar esta sección, se toma como ejemplo el riesgo R1 (Pérdida de integridad), tal como se explicó en la figura 6, es probable que exista pérdida de integridad de la información del sistema de notas debido a una modificación no autorizada, lo que genera que el riesgo inherente sea alto. (ver figura 10).

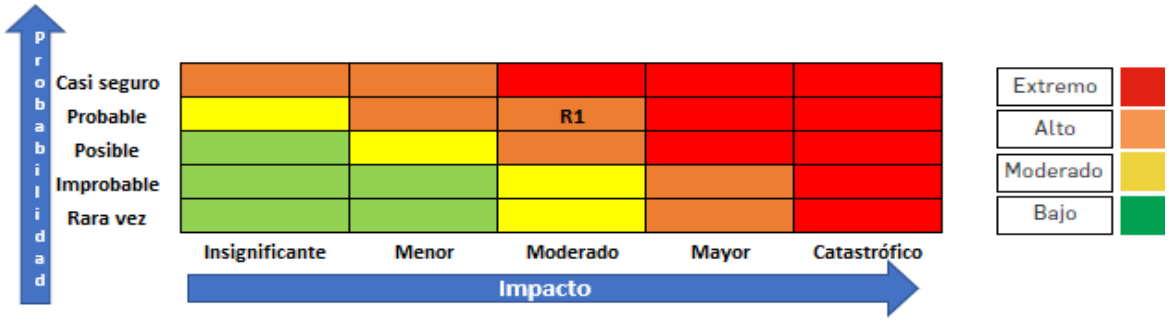


Figura 12 Ejemplo de mapa de riesgo inherente (Antes de controles). Tomado de "Guía para la administración del riesgo y el diseño de controles en entidades públicas". *Fuente:* DAFP,2018, p. 67.

Los controles que disminuyen la probabilidad de ocurrencia del riesgo también disminuyen de forma indirecta el impacto, ya que, de no existir controles para disminuir la probabilidad de ocurrencia del riesgo, el impacto por el número de eventos que se llegarían a materializar sería mayor (DAFP, 2018b, p.65).

A continuación, en la tabla 33 se muestra el desplazamiento que puede tener un riesgo inherente en su probabilidad o impacto para calcular el riesgo residual:

Tabla 33

Posibles desplazamientos de la probabilidad y del impacto

Solidez del conjunto de los controles	Controles ayudan a disminuir la probabilidad	Controles ayudan a disminuir impacto	# Columnas en la matriz de riesgo que se desplaza en el eje de la probabilidad	# Columnas en la matriz de riesgo que se desplaza en el eje de impacto
Fuerte	Directamente	Directamente	2	2
Fuerte	Directamente	Indirectamente	2	1
Fuerte	Directamente	No disminuye	2	0
Fuerte	No disminuye	Directamente	0	2
Moderado	Directamente	Directamente	1	1
Moderado	Directamente	Indirectamente	1	0
Moderado	Directamente	No disminuye	1	0
Moderado	No disminuye	Directamente	0	1

Nota: Tomado de "Guía para la administración del riesgo y el diseño de controles en entidades públicas". Fuente: DAFP,2018, p. 66.

En cuanto a los desplazamientos, se debe tener en cuenta que, si la solidez del conjunto de los controles es débil, este no disminuirá ningún cuadrante de impacto o probabilidad asociado al riesgo y con respecto a los riesgos de corrupción únicamente hay disminución de probabilidad, es decir, para el impacto no opera el desplazamiento. (DAFP, 2018b, p. 66).

De acuerdo con lo anterior, y siguiendo el ejemplo del riesgo R1 (Pérdida de integridad),si en la IE hay controles bien diseñados y ejecutados que disminuyen directamente la probabilidad, al seguir lo establecido en la tabla 33, se disminuirían dos posiciones en la probabilidad, pasando de probable a improbable, y una posición de impacto, pasando de moderado a menor, lo que indica que con los controles establecidos es improbable que exista pérdida de integridad de la información del sistema de notas debido a una modificación no autorizada. (Ver figura 11).

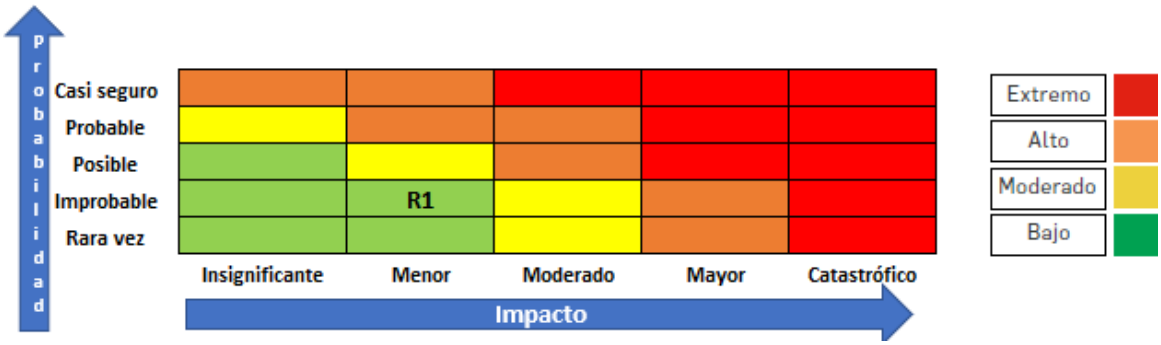


Figura 13 Ejemplo de mapa de riesgo residual (Después de controles). Tomado de "Guía para la administración del riesgo y el diseño de controles en entidades públicas", por DAFP,2018, p. 66.

- ✓ **Tratamiento del riesgo**

Si una vez valorado el riesgo, éste sigue superando el nivel de aceptación establecido por la IE, se dará una respuesta o tratamiento, el cual incluye las siguientes opciones:

- ✓ **Aceptar el riesgo**

Si el nivel de riesgo cumple con los criterios de aceptación de riesgo no es necesario poner controles y puede ser aceptado, Se debe tener en cuenta que, para los casos de riesgos de corrupción, éstos no pueden ser aceptados. (DAFP, 2018b, p. 69).

- ✓ **Evitar el riesgo**

Es criterio de la IE decidir abandonar las actividades que pueden llegar a originar el riesgo. Es decir que después de aplicar esta medida de tratamiento, no habría riesgo, debido a que se cancelan las actividades que lo originan. (DAFP, 2018b, p. 70).

- ✓ **Compartir el riesgo**

Si para la IE es difícil tratar el riesgo, puede compartirlo con otra entidad que pueda gestionarlo de forma efectiva, por ejemplo, a través de seguros, o con la tercerización. (DAFP, 2018b, p. 71).

- ✓ **Reducir el riesgo**

Mediante esta opción de tratamiento se busca que el riesgo residual pueda ser reevaluado

como algo aceptable para la IE, para esto se adoptan medidas que permitan reducir la probabilidad y/o el impacto del riesgo a través de la implementación de actividades de control. (DAFP,2018b, p. 72).

Estas actividades de control permiten prevenir y detectar la ocurrencia de los riesgos, a partir de acciones que se ejecutan, tales como políticas o procedimientos. En este sentido, se deben seleccionar actividades de control preventivas y detectivas que por sí solas ayuden a mitigar o tratar la causa del riesgo, siendo ejecutadas como parte del día a día de las operaciones. (DAFP,2018b, p. 73).

Un ejemplo de un control preventivo sería “la revisión al cumplimiento de los requisitos contractuales en el proceso de selección de un proveedor para una compra institucional”, y como ejemplo de un control detectivo sería “la realización de reinducciones para actualizar al personal con respecto a los cambios en el proceso de matrícula”.

Con respecto al tratamiento de los riesgos de seguridad digital, se sugiere emplear como insumo los controles presentados en el anexo 4 del presente documento, el cual se basa en la norma ISO/IEC 27001:2013 en su anexo A (MinTIC 2018), Sin embargo, la IE puede implementar nuevos controles de seguridad que no estén incluidos dentro del Anexo, siempre y cuando sean efectivos y eficaces para tratar el riesgo.

6.1.4.3 Reporte del plan de tratamiento de riesgos

Después de definir el tratamiento que se le dará a cada riesgo, se debe elaborar un reporte que permita consolidar los aspectos clave de la administración del riesgo.

Este reporte se consolida en un formato, mostrado en la tabla 34, el cual debe contener los siguientes ítems: riesgo identificado; la clase de riesgo: físico, de gestión, corrupción o seguridad digital; las causas raíz; probabilidad e impacto; l nivel del riesgo residual; la opción de

tratamiento; el soporte de cada actividad de control; el responsable de la actividad de control; el tiempo o periodicidad de ejecución de la actividad de control; después de todas las actividades de control, se debe indicar la acción de contingencia que se implementaría de forma inmediata si el riesgo se llegara a materializar (al igual que con las actividades de control, se debe relacionar el soporte, el responsable y el tiempo de ejecución); por último, se formulan los indicadores clave de riesgo, con los que se hace seguimiento al cumplimiento e impacto de las actividades de control, es decir, a su eficacia y efectividad.

La Tabla 34 muestra un ejemplo de formato de mapa y plan de tratamiento de riesgos:

Tabla 34

Formato de mapa y plan de tratamiento de riesgos

No.	Riesgo	Clasificación	Causas	Probabilidad	Impacto	Riesgo	Opción manejo	Actividad de control	Soporte	Responsable	Tiempo	Indicador
			Ausencia de controles en el procedimiento de matrícula				Reducir	Verificación y actualización de procedimiento	Procedimiento actualizado	Asistente	1er trimestre 2019	
			Insuficiente capacitación en el procedimiento de matrículas y uso de plataforma (SIMAT)				Reducir	Difusión y capacitación de procedimiento	Acta de capacitación	Rector	Del 01/02/2019 al 28/02/2019	Eficacia: Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100

1	Proceso de matrícula de estudiantes ejecutado de forma inadecuada	Operativo	Inadecuada verificación del cumplimiento de requisitos de los estudiantes	Improbable	Moderado	Moderado	Reducir	Diseño de instrumento de verificación de requisitos	Instrumento de verificación (Check list)	Asistente	Del 01/02/2019 al 05/02/2019	Efectividad: del plan de manejo de riesgos= ((# de casos de riesgo en el periodo actual - # de casos de riesgo en el periodo anterior) / # de casos de riesgo presentados periodo anterior) x 100
							Acción de contingencia	Revisar de forma inmediata el caso y solicitar la documentación requerida para completar el proceso de matrícula. Realizar las correcciones pertinentes en la plataforma	Novedad registrada en acta	Asistente administrativo	1 semana una vez el riesgo se materialice	

Nota: Adaptado de "Guía para la administración del riesgo y el diseño de controles en entidades públicas", por DAFP,2018, p. 83.

Al finalizar este paso de la metodología se obtendrán los diferentes mapas de riesgo (físicos, de gestión, corrupción y seguridad digital) con los que la IE podrá tener una visión general de sus riesgos y los planes de tratamiento de cada uno. A su vez la secretaría de educación podrá hacer el seguimiento correspondiente a la administración del riesgo en cada IE.

6.1.5 Paso 5. Preparación para la respuesta a emergencias

Según la política nacional de gestión del riesgo de desastres la emergencia es la situación caracterizada por la alteración o interrupción intensa y grave de las condiciones normales de funcionamiento u operación de una comunidad, causada por un evento adverso o por la inminencia del mismo, que obliga a una reacción inmediata y que requiere la respuesta de las instituciones del Estado, los medios de comunicación y de la comunidad en general. (Ley 1523,

2012, art. 4).

A partir de este punto de la metodología se definen, todas las acciones relacionadas con la respuesta a emergencias (plan de contingencia), iniciando con la preparación, siguiendo con la ejecución y finalizando con la preparación para la recuperación de la IE.

En esta primera parte, se incluyen todas las actividades preliminares que permitan mejorar la respuesta de la IE en caso de manifestarse una emergencia o desastre. Esta acción se lleva a cabo siguiendo los pasos descritos a continuación:

6.1.5.1 Organización para la respuesta a emergencias

La IE debe realizar determinadas acciones que le permitan organizarse y estar preparada para responder en caso de una emergencia, para esto deberá inicialmente reconocer y establecer los diferentes servicios de respuesta tanto internos como externos, para luego organizarse de tal manera que se asignen responsables a cada uno de estos servicios. Se sugiere tener en cuenta los servicios establecidos en la Tabla 35:

Tabla 35

Definición de servicios internos de respuesta a emergencias

Definición de servicios internos de respuesta a emergencias		
No.	Servicios de respuesta a emergencias	Descripción
1	Coordinación de la respuesta escolar a emergencias	Garantizar que la respuesta a la emergencia se ejecute de manera segura y eficiente, mientras hacen presencia los organismos de socorro y durante las actividades que estos desarrollen. Que todos los demás servicios de respuesta se lleven a cabo de manera efectiva y ordenada de acuerdo con el evento y daños presentados.
2	Extinción de incendios	Extinción de conatos de incendio
3	Primeros auxilios	Asistencia primaria en salud a los miembros de la comunidad educativa afectada, física o psicológicamente, con el fin de proteger su vida y evitar complicaciones mayores mientras se obtiene ayuda médica especializada.

4	Evacuación	Desplazamiento ordenado de la comunidad educativa hacia sitios seguros
5	Control de tránsito vehicular	Despejar las vías para garantizar el desplazamiento de la comunidad educativa hacia los puntos de encuentro externos a la IE y el acceso a la IE o acercamiento de los vehículos de respuesta a emergencias como carro de bomberos, ambulancias y patrullas de policía.
6	Servicios sanitarios	Asegurar las condiciones de higiene de la IE para atender sus necesidades fisiológicas
7	Manejo de servicios públicos	Garantizar la prestación del servicio de agua, energía, comunicaciones y transporte en caso de que resulten afectados, incluye también la suspensión de éstos, en caso de que puedan representar una amenaza para la comunidad o las edificaciones
8	Traslado al hospital	Desplazamiento de miembros de la comunidad educativa afectados por un evento con el fin de que reciban atención médica especializada.
9	Búsqueda y rescate	Hallazgo y recuperación a salvo de personas perdidas y/o atrapadas por colapso de estructuras o elementos pesados, o en áreas de difícil acceso
	Manejo de materiales peligrosos	Reconocer, identificar y controlar cuando sea posible la presencia de materiales peligrosos para la salud, el medio ambiente o las edificaciones
11	Otros	

Nota: Tomado de "Guía Plan Escolar para la Gestión del Riesgo", por Sistema Nacional para la Prevención y Atención de Desastres,2010, p. 55.

Se debe precisar que, de acuerdo con las características de la emergencia presentada, la IE deberá prestar uno u otros servicios y si la situación es muy compleja tendrá que efectuar todos los definidos en la tabla anterior. Por lo tanto, la IE podrá establecer otros servicios de respuesta en la medida que se requieran.

En el caso de situaciones de emergencia que superen la capacidad de respuesta de la IE, se deberá acudir a servicios de respuesta de entidades externas que existan en el municipio, los cuales deben ser identificados con anterioridad, por ejemplo, cuerpo de bomberos, policía, centro de salud, defensa civil, etc. (Sistema Nacional para la Prevención y Atención de Desastres, 2010, p. 58).

Se debe tener presente que los servicios de respuesta a emergencias al interior de la IE, deben ser coordinados y ejecutados por directivos, administrativos y docentes, los estudiantes participan, pero no pueden ser los responsables directos de ningún servicio de respuesta, dadas las implicaciones legales que se ocasionarían si los estudiantes sufren algún tipo de daño debido a su ejecución. (Sistema Nacional para la Prevención y Atención de Desastres, 2010, p. 56).

Los responsables de cada servicio deberán conformar brigadas, en la Tabla 36, se presenta un modelo de organización:

Tabla 36

Organización para la respuesta a emergencias

Organización para la respuesta a emergencias			
Organización	Funciones	Nombre de responsables	Suplentes
Coordinador de la respuesta escolar a emergencias	Obtener y analizar información sobre el evento. Informar a sus brigadas las condiciones del evento. Activar la respuesta a emergencias. Coordinar y optimizar los recursos humanos y técnicos para atender la emergencia. Servir de conexión con entidades operativas. Informar a la comunidad educativa sobre el estado de la emergencia. Apoyar al rector(a) en la toma de decisiones. Consolidar los reportes de las brigadas de la escuela.		
Brigadas de evacuación	Planear y ejecutar simulacros de evacuación por cursos y general. Llevar a cabo labores de señalización. Difundir el plan de evacuación. Activar la alarma de evacuación. Conducir la evacuación de los alumnos a los puntos de encuentro. Conteo final en coordinación con los directores de cada curso. Elaboración de reporte de evaluación sobre participación, tiempos de desplazamiento, orden.		
Brigadas de primeros auxilios	Atender los casos específicos de primeros auxilios básicos. Definir un lugar para proveer la atención primaria a los afectados. Identificar los centros asistenciales cercanos a la IE Mantener actualizado un directorio de entidades de ayuda. Mantener vigente el kit de emergencias de la IE Elaborar reporte de atención.		

Brigadas contra incendios	Atender conatos de incendio, para lo cual deberán haber sido capacitados. Detectar y prevenir incendios dentro de las instalaciones de la IE Revisar el estado y ubicación de los extintores o sistemas contra incendio. Hacer inventario de recursos necesarios para atender incendios. Identificar puntos de abastecimiento de agua. Comunicar a los bomberos siempre en caso de incendio.
Brigadas control tráfico vehicular	Identificar los puntos críticos para el despeje de vías. Controlar la movilidad vehicular para evitar que ponga en riesgo a la comunidad educativa y/o garantizar la evacuación hacia puntos de encuentro externos a la IE.
Brigadas servicios sanitarios	Identificar focos de contaminación del agua y/o del aire. Implementar medidas de saneamiento básico. Coordinar la prestación del servicio de agua y energía siempre y cuando no representen un riesgo.
Otras brigadas	Las que se requieran según las condiciones de emergencia.

Nota: Tomado de "Guía Plan Escolar para la Gestión del Riesgo", por Sistema Nacional para la Prevención y Atención de Desastres,2010, p. 57.

6.1.5.2 Capacitación

Esta acción permite que las personas desarrollen conocimientos y habilidades específicas que les permitan cumplir de la mejor manera los servicios de respuesta a emergencias definidas para la IE. Por lo tanto, es recomendable que los responsables y brigadistas definidos en el modelo organizacional se capaciten en los servicios requeridos. (Sistema Nacional para la Prevención y Atención de Desastres, 2010, p. 60).

Se sugiere definir las necesidades de capacitación, a partir de un diagnóstico de las personas capacitadas y con base en esto programar las actividades de capacitación a que haya lugar. Para esto se puede diligenciar un formato como el mostrado en la tabla 37:

Tabla 37

Necesidad de capacitación para la respuesta

Necesidad de capacitación para la respuesta

Servicio de respuesta	Número de personas capacitadas	Número de personas a capacitar	Oferente de capacitación	Responsable	Fecha de capacitación	Recursos
Coordinación de la respuesta escolar a emergencias						
Extinción de incendios						
Primeros auxilios						
Evacuación						
Tráfico vehicular						
Otros						

Nota: Tomado de "Guía Plan Escolar para la Gestión del Riesgo", por Sistema Nacional para la Prevención y Atención de Desastres,2010, p. 59.

6.1.5.3 Equipamiento para la respuesta

"El equipamiento para la respuesta a emergencia incluye todos aquellos recursos físicos y funcionales que puede requerir la IE para ejecutar los servicios de respuesta" (Sistema Nacional para la Prevención y Atención de Desastres, 2010, p. 61) entre ellos se encuentran:

- ✓ **Equipos contra incendios**

Son aquellos que permiten ejecutar la extinción de incendios. Se sugiere diligenciar la Tabla 38, en la que se relacionan los equipos existentes y su estado, la cantidad de equipos requeridos, el responsable de su manejo, el plazo de adquisición y/o mantenimiento, y los recursos necesarios para la adquisición de los elementos.

Tabla 38

Equipamiento contra incendios

Equipamiento contra incendios						
Descripción del equipamiento	Verificación de existencia y condición ¿Existe?	Estado: Bueno, regular, malo	Cantidad de equipos requeridos	Responsable	Fecha de adquisición	Recursos
Detectores de humo						
Sprinkles o rociadores						
Mangueras						
Hidratantes						
Extintores tipo ABC						
Extintores Solkaflam para equipos eléctricos						
Otros						

Nota: Tomado de "Guía Plan Escolar para la Gestión del Riesgo", por Sistema Nacional para la Prevención y Atención de Desastres,2010, p. 61.

- ✓ **Equipamiento para primeros auxilios**

Este equipamiento contiene todos los elementos necesarios para la prestación de los primeros auxilios. En la Tabla 39 se muestra la información a diligenciar con respecto al equipamiento necesario en la IE:

Tabla 39

Equipamiento para primeros auxilios

Equipamiento para primeros auxilios						
Equipo para primeros auxilios	Verificación de existencia y condición ¿Existe?	Estado: Bueno, regular, malo	Cantidad de Equipos requeridos	Responsable	Fecha de adquisición	Recursos
Camillas						
Inmovilizadores cervicales						
Inmovilizadores para extremidades						
Botiquín						

Nota: Tomado de "Guía Plan Escolar para la Gestión del Riesgo", por Sistema Nacional para la Prevención y Atención de Desastres,2010, p. 62.

Otros

- ✓ **Señalización**

La señalización es la acción que permite orientar a las personas dentro de la IE, por ejemplo, las rutas de evacuación, principalmente cuando existe una emergencia.

En la Tabla 40, se muestran las señales principales aplicables en la IE. Señales reguladas por "la Norma Técnica Colombiana emitida por el ICONTEC NTC 4596. Señalización para instalaciones y ambientes escolares, además de otras normas como la NTC 1931 Protección contra incendios: señales de seguridad y NTC 1461 colores y señales de seguridad" (Sistema Nacional para la Prevención y Atención de Desastres, 2010, p. 62).

Tabla 40

Tipos de señalización

Tipo de señal	Características	Ejemplo
Señales de prohibición	Indican prohibiciones o limitaciones dentro de un área de la IE o fuera de ella. Tienen fondo blanco, el símbolo o mensaje en negro y la banda circular y la banda cruzada en rojo.	
Señales de precaución o advertencia	Advierten sobre la existencia de un peligro. Tienen un fondo triangular o rectangular de color amarillo y tanto el mensaje, el símbolo como la banda son de color negro.	
Señales de obligación o reglamentarias	Indican el cumplimiento de reglas o normas al interior de una zona o de la IE. Tienen un fondo circular de color azul con el símbolo de color blanco y los textos complementarios de color negro.	
Señales de información de salidas de emergencia y primeros auxilios	Indican la ubicación de las salidas de emergencia, las instalaciones de primeros auxilios, las rutas de evacuación. Tienen forma rectangular o cuadrada con fondo verde y el símbolo o flecha direccional de color blanco.	
Señales de protección contra incendios	Muestran la ubicación de los equipos contra incendios. Son de forma cuadrada o rectangular con fondo de color rojo y símbolos en color blanco.	

Nota: Tomado de "Guía Plan Escolar para la Gestión del Riesgo", por Sistema Nacional para la Prevención y Atención de Desastres,2010, p. 63.

Una vez descritos los diferentes tipos de señales visuales, la IE deberá identificar sus necesidades en cuanto señalización, para esto se puede diligenciar la Tabla 41:

Tabla 41

Necesidades de señalización

	Necesidades de señalización				
Tipo de señal	Número de señales existentes	Número de señales requeridas	Responsable	Fecha de adquisición	Recursos
Señales de prohibición					
Señales de precaución o advertencia					
Señales de obligación o reglamentarias					

Señales de información de salidas de emergencia y primeros auxilios	
Señales de protección contra incendios	

Nota: Tomado de "Guía Plan Escolar para la Gestión del Riesgo", por Sistema Nacional para la Prevención y Atención de Desastres,2010, p. 64.

- ✓ **Sistema de alarma**

"La IE debe adoptar un sistema de timbre, campana o sirena para activar la movilización en caso de evacuación, no se recomienda usar megáfonos o altavoces, ya que una voz alterada o confusa puede generar pánico" (Sistema Nacional para la Prevención y Atención de Desastres, 2010, p.65). Para definir las necesidades del sistema de alarma, se sugiere diligenciar la Tabla 42:

Tabla 42

Necesidades del sistema de alarma

	Necesidades del sistema de alarma				
Características del sistema de alarma	Verificación de la característica (Cumple / No cumple)	Modificaciones requeridas	Responsable	Fecha de acción de mejora	Recursos
Cubre todas las zonas donde hay estudiantes y empleados					
Es distinta al sonido de cambio de clases					

Es exclusiva para casos de emergencia
La conoce toda la comunidad educativa
Dispone de un sistema alterno para el suministro de energía

Nota: Tomado de "Guía Plan Escolar para la Gestión del Riesgo", por Sistema Nacional para la Prevención y Atención de Desastres,2010, p. 65.

- ✓ **Comunicaciones**

La IE debe disponer de mecanismos de comunicación que permitan la activación de los servicios de respuesta tanto internos como externos (cuando se requiera).

Se sugiere diligenciar la Tabla 43 para determinar las necesidades de la IE en este aspecto:

Tabla 43

Necesidades de equipos para comunicaciones

	Necesidades de equipos para comunicaciones					
Equipos para comunicaciones	Verificación de existencia y condición ¿Existe?	Estado: Operativo /No operativo	Cantidad de equipos requeridos	Responsable	Fecha de adquisición	Recursos
Teléfono fijo						
Teléfono celular						
Otro						

Nota: Tomado de "Guía Plan Escolar para la Gestión del Riesgo", por Sistema Nacional para la Prevención y Atención de Desastres,2010, p. 66.

6.1.3.4 Entrenamiento

"Esta actividad permite practicar de manera periódica la prestación efectiva de todos los servicios de respuesta a emergencias" (Sistema Nacional para la Prevención y Atención de Desastres, 2010, p. 66), definidas en la Tabla 35.

Una de las prácticas de entrenamiento más utilizadas son los simulacros, con los cuales se entrena a la comunidad educativa lo que incluye a las brigadas, para que sean capaces de

responder a situaciones de emergencia y poder detectar fallas que permitan establecer medidas de mejoramiento.

Las IE pueden realizar simulacros generales relacionados con: formas de comportamiento durante el desplazamiento; tiempos de desplazamiento; funcionamiento y capacidad de las brigadas; capacidad de las rutas de evacuación y puntos de encuentro; capacidad de los estudiantes y docentes para seguir instrucciones; ubicación y acceso al equipamiento; efectividad de la alarma. (Sistema Nacional para la Prevención y Atención de Desastres, 2010, p. 66).

Para realizar la preparación del simulacro, se recomienda seguir los pasos descritos en la figura 12:

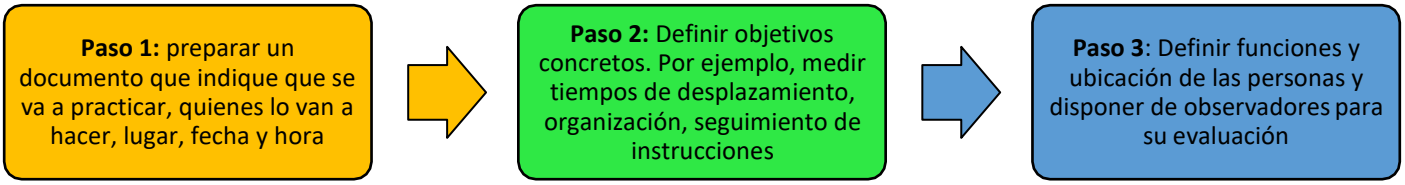


Figura 14 Pasos para preparar el simulacro. Tomado de "Guía Plan Escolar para la Gestión del Riesgo", por Sistema Nacional para la Prevención y Atención de Desastres,2010, p. 67.

De igual forma, para desarrollar y evaluar un simulacro general, se deberán seguir los pasos mostrados a continuación:

1. dete

cción del peligro: percepción de señales como calor, humo, ruidos, gritos, sonidos y movimientos anormales; 2. activación de la alarma: tiempo que les toma a los responsables la activación de la alarma y al personal realizar la evacuación; 3. preparación o alistamiento para la salida: tiempo desde que se comunica la decisión de evaluación hasta que empieza a salir la primera persona; 4. Salida: tiempo desde que empieza a salir la primera persona hasta que sale la última. (Sistema Nacional para la Prevención y Atención de Desastres, 2010, p. 67).

Los pasos mencionados anteriormente deben ser evaluados para poder definir las medidas

de mejoramiento requeridas para perfeccionar el simulacro. Se sugiere diligenciar la siguiente tabla:

Tabla 44

Evaluación del simulacro

Evaluación del simulacro Simulacro No: Fecha: Objetivo:						
Actividad	Tiempo empleado	Dificultades	Acciones de mejoramiento requeridas	Responsable	Plazo	Recursos
Detección del peligro Alarma Alistamiento para la salida Salida						

Nota: Tomado de "Guía Plan Escolar para la Gestión del Riesgo", por Sistema Nacional para la Prevención y Atención de Desastres,2010, p. 68.

6.1.6 Paso 6 Ejecución de la respuesta

Esta línea de acción "está conformada por las acciones que de manera real se llevan a cabo durante una emergencia real" (Sistema Nacional para la Prevención y Atención de Desastres, 2010, p. 69).

6.1.6.1 Procedimiento básico de respuesta a emergencias

De llegar a presentarse una emergencia, la respuesta en general deberá estar alineada a la que se presenta en la figura 13:

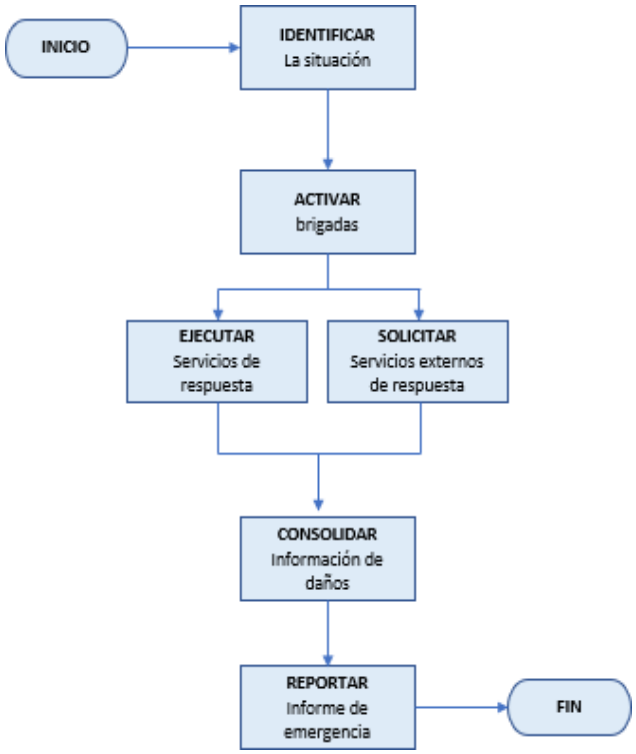


Figura 15 Procedimiento básico de respuesta a emergencias. Tomado de "Guía Plan Escolar para la Gestión del Riesgo". *Fuente:* por Sistema Nacional para la Prevención y Atención de Desastres,2010, p. 70.

Se inicia el proceso de respuesta a emergencias identificando la situación presentada, seguidamente se activan las brigadas existentes, capacitadas y entrenadas, las cuáles serán las encargadas de ejecutar los servicios de respuesta internos, y si la situación lo amerita, solicitar

servicios de respuesta externos, finalmente se consolidará la información de daños presentados en la tabla 45, y se realizará el reporte del informe de la emergencia presentada.

6.1.6.2 Reporte de daños

Se sugiere diligenciar la tabla mostrada a continuación, "para consolidar la información relacionada a los daños y/o pérdidas generadas por un evento y facilitar el reporte de manera ordenada" (Sistema Nacional para la Prevención y Atención de Desastres, 2010, p. 70).

Tabla 45

Reporte de daños

Reporte de daños		
Fecha del evento	Diligenciado por	Teléfono
Fenómeno al que está asociada la emergencia		
Sismo ( )	Vendaval ( )	Incendio estructural ( )
Inundación ( )	Tormenta eléctrica ( )	Explosión ( )
Deslizamiento ( )	Caída de árbol ( )	Estampida de estudiantes ( )
Avalancha ( )	Incendio forestal ( )	Accidente de laboratorio ( )
Accidente de tránsito ( )	Toma armada ( )	Atentado terrorista ( )
Contaminación ( )	Descarga eléctrica ( )	Otro (cuál)
Descripción general del evento Daños y/o pérdidas ocurridas		
Tipo y número de personas afectadas solicitados Estudiantes ( )		Tipo de servicios de respuesta Ambulancia ( )
Docentes ( )		Bomberos ( )
Personal administrativo ( )		Policía ( )
Personal de servicios generales ( )		Policía de tránsito ( )
Directivos ( )		Manejo de servicios públicos ( )
Visitantes ( )		Otro (cuál)
Otro (cuál)		Descripción de los daños en las edificaciones
Tipo y número de edificaciones afectadas		
Descripción de necesidades_____		

Nota: Tomado de "Guía Plan Escolar para la Gestión del Riesgo", por Sistema Nacional para la Prevención y Atención de Desastres,2010, p. 71.

6.1.7 Paso 7 Preparación para la recuperación

Esta línea de acción permite que las IE, se preparen para su recuperación después de ocurrir un incidente de gran impacto, de tal forma que se permita garantizar la recuperación del

acceso y permanencia a los servicios educativos, propiciando el retorno a la normalidad. Es así como “la preparación para la recuperación tiene como propósito central dotar de un sentido de normalidad a la comunidad, evitar la deserción escolar y mejorar las condiciones previas al evento” (MEN,2015, p. 54).

La IE “debe, en cabeza del gobierno escolar identificar sus propias necesidades, priorizarlas y planificar su solución para garantizar el derecho a la educación” (Sistema Nacional para la Prevención y Atención de Desastres, 2010, p. 73).

6.1.7.1 Valoración de la situación

Para definir su proceso de recuperación, la IE deberá realizar las verificaciones a las que haya lugar para poder valorar su situación actual, identificando las necesidades que presenta e impiden su proceso de recuperación.

A modo de ejemplo se muestra la tabla 46, la cual relaciona algunas inspecciones que debe hacer la IE para valorar su situación actual:

Tabla 46

Valoración de necesidades de la IE

Identificación general y valoración de necesidades de la IE			
Fecha de la emergencia			
Lugar de la emergencia			
Tipo de emergencia			
Información general	Si	No	Detalle de necesidades
Está funcionando la I. E			
Las instalaciones escolares son seguras Dispone de agua limpia			
Dispone de equipamiento (pupitres, tableros, etc.) Dispone de materiales escolares (cuadernos, textos guía, etc)			
Dispone de docentes			
Existen adultos / jóvenes que puedan ejercer como docentes			
Niños / Niñas están asistiendo a la I. E Niños / Niñas dejan de asistir a la I. E			
Si la IE no puede ser usada, existen sitios donde se pudieran dar clases			
Estos sitios son suficientes para la cantidad de niños y niñas			
Estos sitios son accesibles Estos sitios son seguros			
Se brindan mensajes especiales a los niños y niñas sobre salud			
Se brindan mensajes especiales a los niños y niñas sobre peligros potenciales			

Se brindan mensajes especiales a los niños y niñas sobre formas de protección

Nota: Tomado de "Guía Plan Escolar para la Gestión del Riesgo", por Sistema Nacional para la Prevención y Atención de Desastres,2010, p. 74.

Con la verificación de estas condiciones la IE estará en capacidad de identificar cuáles de esas necesidades será capaz de resolver, y con cuales requerirá ayuda de entes externos (el estado, ONG, ayuda humanitaria, etc.), además, se agiliza la disponibilidad de información cuando ésta sea requerida.

Una vez se identifiquen las necesidades prioritarias que impiden continuar con la prestación del servicio del establecimiento educativo, se establece un plan de acción que permita cumplir con los siguientes objetivos: definir con los actores cercanos a la escuela el hábitat escolar posible de acuerdo con la situación; acordar las prioridades para mejorar las condiciones del hábitat escolar; establecer responsables y tiempos para mejorar el hábitat escolar; definición o flexibilización del currículo y planes de estudio acorde con las necesidades de los estudiantes y disponibilidad de docentes. (Sistema Nacional para la Prevención y Atención de Desastres, 2010, p. 75).

6.1.7.2 Ejecución de la recuperación

Para ejecutar la recuperación, la IE deberá llevar a cabo las actividades establecidas en el plan de acción definido en el punto anterior, que le permita seguir prestando el servicio educativo. Así mismo, la IE deberá realizar actividades de seguimiento, que permitan verificar si las acciones emprendidas contribuyen a satisfacer las necesidades identificadas, para posteriormente realizar las mejoras requeridas. Estas actividades de seguimiento deberán enfocarse en que durante la prestación del servicio se brinde protección a la comunidad educativa. (Ver tabla 47).

Tabla 47

Ejecución de las acciones para la recuperación

Ejecución de las acciones para la recuperación					
	Ejecución			Seguimiento	
Necesidad a satisfacer	Ejecutor (Interno / Externo)	Acciones a desarrollar	Fecha de ejecución	Cumplimiento Si/No	Acciones de mejoramiento

Nota: Tomado de "Guía Plan Escolar para la Gestión del Riesgo", por Sistema Nacional para la Prevención y Atención de Desastres,2010, p. 76.

6.1.8 Comunicación, consulta y seguimiento

Las actividades de comunicación y consulta son transversales durante todo el proceso de administración del riesgo, e involucra a todos los interesados, por lo que se sugiere difundir y socializar la presente metodología, para que todos los integrantes de la comunidad educativa se apropien de la misma.

En este sentido, "la comunicación y consulta con las partes involucradas, tanto internas como externas, debería tener lugar durante todas las etapas del proceso para la gestión del riesgo" (NTC ISO31000, 2011, p. 22).

En cuanto a las actividades de seguimiento, se hace necesario realizar un constante monitoreo a la administración del riesgo, manteniendo especial cuidado con los riesgos de corrupción, ya que, por sus propias particularidades, se convierte en un riesgo difícil de detectar.

Teniendo en cuenta el modelo de las tres líneas de defensa, le corresponderá al consejo directivo, al CARAE y a la secretaría de educación, realizar las actividades de seguimiento durante el proceso de administración del riesgo.

Se puede concluir que, con la construcción de la presente metodología, las IE públicas del departamento del Atlántico contarán con una herramienta que les permitirá administrar los diferentes tipos de riesgos y estar en la capacidad de responder ante las emergencias que se puedan presentar, garantizando el cumplimiento de sus objetivos tanto institucionales como de

procesos.

6.2 Operacionalización de la metodología

Las diferentes IE del Departamento del Atlántico operacionalizarán la presente metodología por medio de una herramienta tecnológica, una plataforma web, denominada GRIE (Gestión de Riesgos en las IE), la cual estará diseñada bajo los framework angular y express, y el gestor de base de datos mongodb.

Se utilizan angular y express por las ventajas que ofrecen para la creación y programación de aplicaciones web, y sus características tales como, evitar escribir código repetitivo y la facilidad para ordenar el desarrollo, lo que asegura desarrollos más rápidos y en menos tiempo posibilitando modificaciones y actualizaciones automáticas.

Por su parte, mongodb se utiliza como gestor de base de datos NoSQL, orientado a documentos y de código abierto que guarda estructuras de datos con un esquema dinámico, ofreciendo gran escalabilidad y flexibilidad lo que se refleja en una integración de datos más fácil y rápida.

Teniendo en cuenta lo anterior, esta plataforma web, mostrará el camino a seguir por cada una de las fases de la metodología, además permitirá el registro de la información de administración del riesgo de cada IE.

A continuación, se definirá la estructura del sistema GRIE, el caso de uso del sistema, y algunos pantallazos de la interfaz gráfica.

6.2.1 Estructura del sistema GRIE

El sistema GRIE está conformado por 7 módulos, correspondientes con los pasos de la metodología, los cuales permitirán realizar el registro del proceso de administración de riesgos y

respuesta a emergencias de cada IE; cada módulo incluye varios componentes, y cada componente varios subcomponentes.

Tabla 48

Estructura del sistema GRIE

Módulos	Componentes	Subcomponentes
1. Presentación institucional	Identificación de la institución	Identificación Conocimiento de la institución
	Identificación de la sede	n/a
2. Política de administración del riesgo	Lineamientos de la política	n/a
3. Identificación del riesgo	Caracterización del contexto	Contexto externo Contexto interno Contexto del proceso Identificación de activos de seguridad digital
	Identificación del riesgo	n/a
4. Valoración de riesgos	Análisis de riesgos	Determinar probabilidad Determinar consecuencias Estimar el nivel de riesgo inicial - Inherente
	Evaluación de riesgos	Valoración de los controles Nivel de riesgo residual Tratamiento del riesgo
	Reporte del plan de tratamiento de riesgos	n/a
5. Preparación para la respuesta a emergencias	Organización para la respuesta a emergencias	n/a
	capacitación	n/a
	Equipamiento para la respuesta	n/a
	Entrenamiento	n/a
6. Ejecución de la respuesta	Procedimiento básico de respuesta a emergencias	n/a
	Reporte de daños	n/a
7. Preparación para la recuperación	Valoración de la situación	n/a
	Ejecución de la recuperación	n/a

6.2.2 Caso de uso del sistema

Los módulos descritos anteriormente, se tradujeron como casos de uso. Cada caso de uso tiene una función específica dentro del sistema, y es ejecutada por un responsable, que puede ser, el representante de la IE, el representante de la secretaría de educación o el propio sistema de gestión de riesgos GRIE.

A continuación, se muestra el caso de uso primario o de alto nivel del sistema

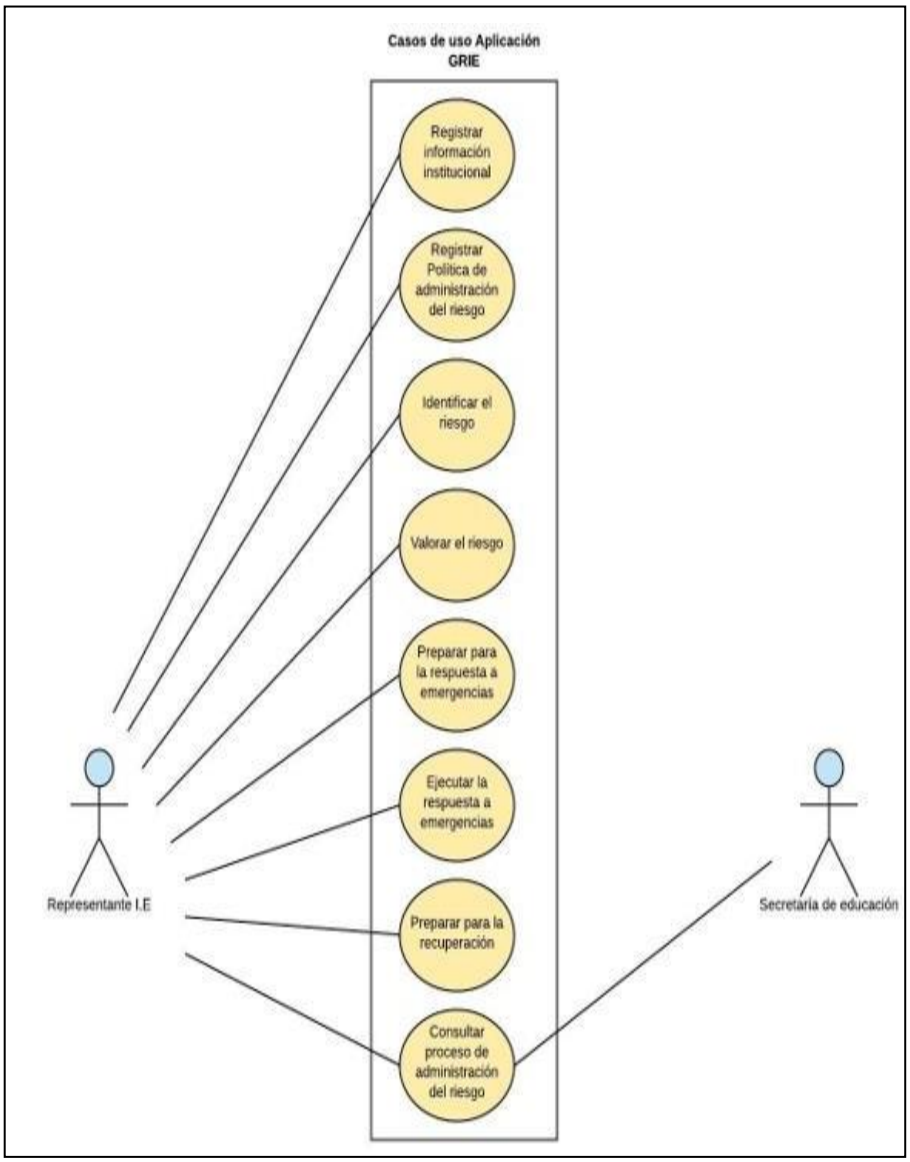


Figura 16 Caso de uso sistema GRIE. *Fuente:* elaboración propia

6.2.3 Pantallazos de la interfaz gráfica del sistema GRIE

A continuación, se presentan algunos pantallazos de la interfaz gráfica de la herramienta web:

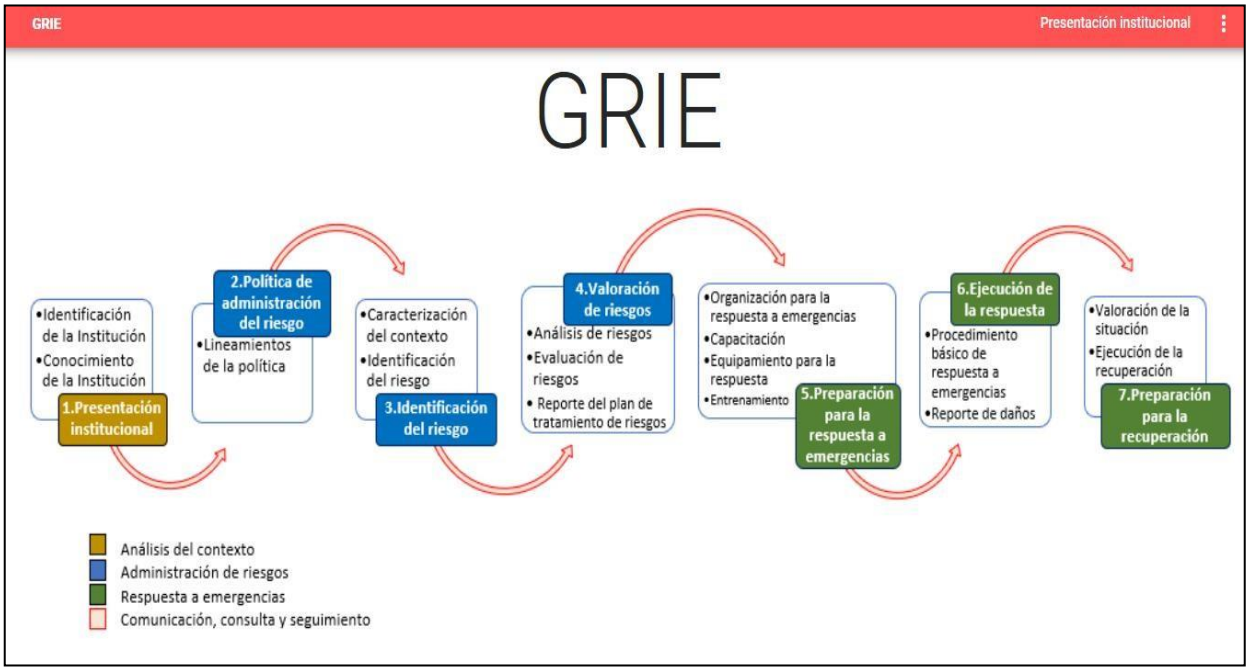


Figura 17 Interfaz principal Sistema GRIE. *Fuente:* elaboración propia

Figura 18 Interfaz presentación institucional. *Fuente:* elaboración propia

Figura 19 Interfaz identificación de la sede. *Fuente:* elaboración propia

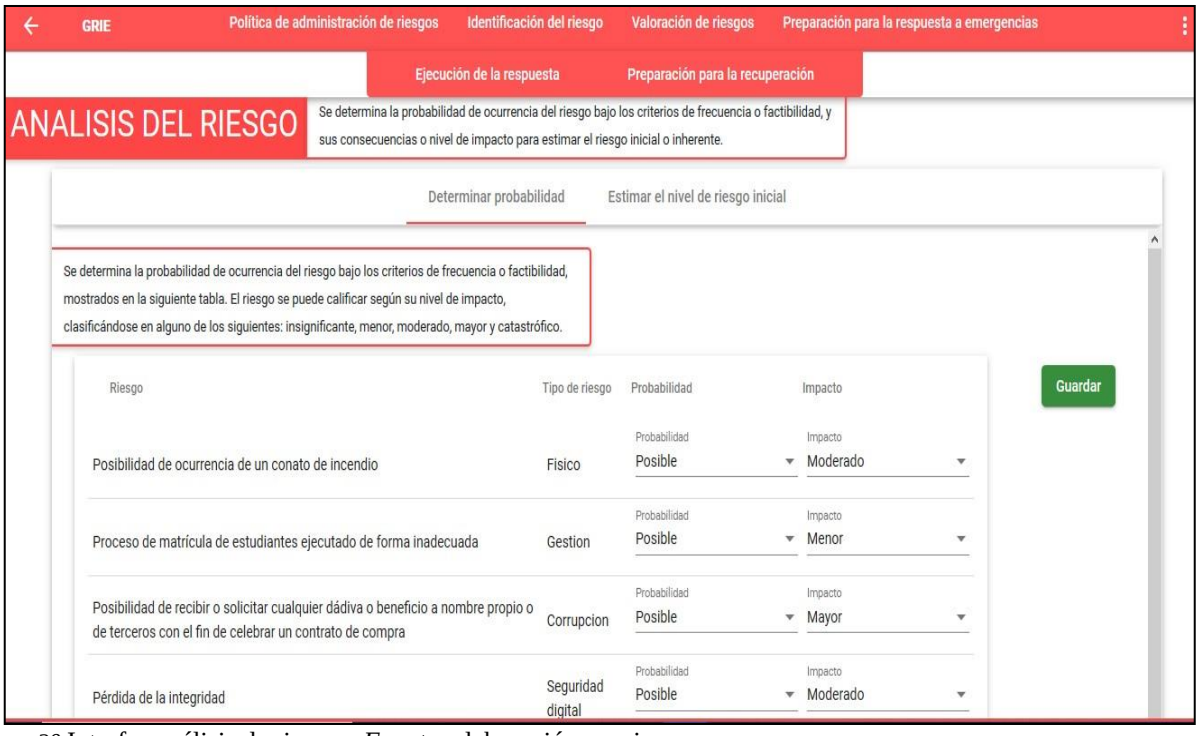


Figura 20 Interfaz análisis de riesgos. *Fuente:* elaboración propia

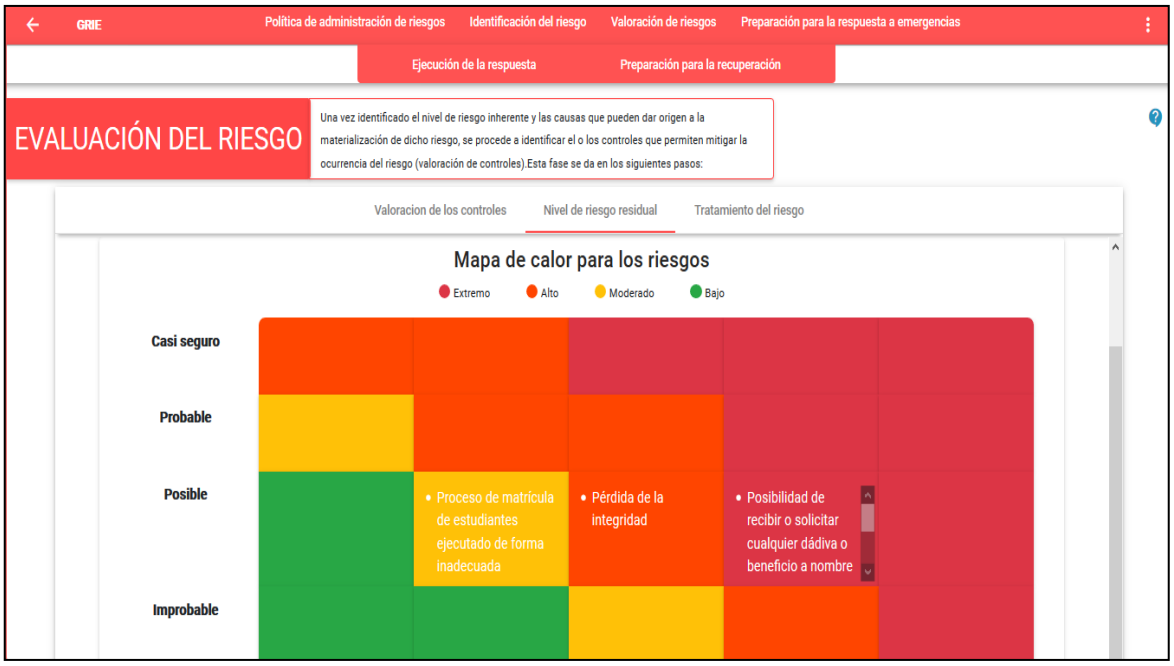


Figura 21 Interfaz evaluación de riesgos. *Fuente:* elaboración propia

Figura 22 Interfaz preparación para la respuesta a emergencias. *Fuente:* elaboración propia

7. Resultados

Para realizar la validación de la presente propuesta metodológica, se utilizó como instrumento la técnica cualitativa: grupo focal de expertos, desarrollándose el cuestionario mostrado en el anexo 5.

Para la selección de los integrantes del grupo focal se establecieron como criterios los siguientes: tener experiencia en el sector educativo como rector o coordinador, específicamente en IE públicas de básica y media, y/o ser docente con conocimientos sobre riesgos en este sector.

Se seleccionaron 23 expertos, cuya experiencia en IE oscila entre los 10 y 50 años, los cuales evaluaron los siguientes criterios: la base teórica de la propuesta, su pertinencia, coherencia metodológica, factibilidad de aplicación y la importancia y/o contribución de los resultados previstos.

Para realizar la calificación de la validación, se establecieron como rangos los valores del 1 al 5, donde 1 representa “totalmente en desacuerdo” y 5 “totalmente de acuerdo”.

Una vez realizada la validación de la propuesta metodológica, se obtuvieron los siguientes resultados:

Base teórica de la propuesta: 4,7 Pertinencia: 4, 7

Coherencia metodológica: 4, 7 Factibilidad de aplicación: 4,5

Importancia y/o contribución de la propuesta metodológica: 4,8

Lo anterior demuestra que los 23 expertos otorgan a los criterios solicitados, valores promedio superiores a 4,5 valor suficientemente alto que valida la presente propuesta metodológica.

De igual manera, se les presentó la herramienta web GRIE, solicitándoles su opinión con

respecto al diseño de la interfaz gráfica, su coherencia con respecto a la metodología, y si consideran que esta herramienta permitiría la operacionalización de la presente propuesta, obteniendo los siguientes resultados:

Facilidad de uso: 4, 7

Coherencia de los módulos de software: 4, 7

Operacionalización de la metodología: 4,8

Adicionalmente, se muestran algunas de las apreciaciones de los expertos en cuanto a la metodología y la herramienta tecnológica:

- ✓ "*Es una herramienta que se hace necesaria en las IE, ya que esta figura en lo concerniente a la gestión del riesgo es casi nula*". Coordinador I.E. Técnica Agropiscícola de Rotinet
- ✓ "*Me parece pertinente, puesto que se convertiría en una herramienta básica para la prevención en las IE, teniendo en cuenta los diferentes contextos de las mismas".* Coordinador IE Dolores María Ucrós de Soledad
- ✓ *"Está bien documentada y de fácil manejo para los usuarios".* Docente con experiencia en manejo de riesgos en IE. IED Villanueva
- ✓ *"Buena herramienta web que permitiría la operacionalización de la metodología".* Coordinador IET Francisco de Paula Santander de Soledad.

Con estos resultados, se demuestra que los expertos consideran que el sistema GRIE facilitaría la operacionalización de la presente metodología en las IE.

8. Conclusiones

Con el desarrollo de la presente investigación, se puede concluir que, a través de la metodología propuesta, las IE podrán administrar sus riesgos, diseñar controles que permitan disminuir su probabilidad de ocurrencia e impacto y ejecutar acciones de respuesta a emergencias que permitan evitar y/o minimizar la afectación de la prestación del servicio educativo.

Al realizar cada uno de los pasos de la presente propuesta metodológica, se obtendrá la información referente a la identificación de la IE, la conformación del CARAE, comité encargado de coordinar las actividades relacionadas a la administración del riesgo, la política que permitirá establecer los fines generales de la institución con respecto a la administración del riesgo, la caracterización del contexto externo, interno, de procesos y de activos de seguridad digital, así como la identificación de los diferentes tipos de riesgos, físicos, de gestión, de corrupción y de seguridad digital, obteniéndose los diferentes mapas de riesgo que le permitirán a la institución tener una visión general de sus riesgos y sus planes de tratamiento. Por último, se obtienen todas las acciones relacionadas con la respuesta a emergencias, es decir, el plan de contingencia, que permitirá que la IE esté preparada frente a las eventualidades que se puedan presentar, asegurando de esta forma el logro de sus objetivos tanto institucionales como de procesos.

Adicionalmente, a través de cada uno de los módulos de la herramienta web GRIE, se podrá registrar la información correspondiente a cada paso de la metodología, con lo que se garantiza su operacionalización dentro de la IE, y el seguimiento correspondiente por parte de la secretaría de educación.

Referencias

Departamento Administrativo de la Función Pública (2018a). Anexo 5. Análisis y priorización de causas. 1-7

Departamento Administrativo de la Función Pública. (2018b). Guía para la administración del riesgo y el diseño de controles en entidades públicas: Riesgos de Gestión, Corrupción y Seguridad Digital. 1–93.

Fraser, J. R. S., & Simkins, B. J. (2016). The challenges of and solutions for implementing enterprise risk management. Business Horizons, 59(6), 689–698. https://doi.org/10.1016/j.bushor.2016.06.007

Fuse, M., Ozawa, S., & Miura, S. (2012). Role of the Internet for risk management at school. 2012 International Conference on Information Technology Based Higher Education and Training, ITHET 2012, March 2011. https://doi.org/10.1109/ITHET.2012.6246046

Gong, M. Z., & Subramaniam, N. (2018). Principal leadership style and school performance: mediating roles of risk management culture and management control systems use in Australian schools. Accounting and Finance, 1–40. https://doi.org/10.1111/acfi.12416

ICONTEC. (2009). Norma Técnica Colombiana NTC-ISO / IEC. 571. ICONTEC. (2011). Norma Técnica Colombiana NTC-ISO 31000. 571.

Instituto Distrital de Gestión de Riesgos y cambio climático. (2015). Lineamientos para la Elaboración del plan Escolar de Gestión de Riesgos y Cambio Climático PEGR-CC. Alcaldía Mayor de Bogotá., 1–45. Recuperado de:

http://www.sire.gov.co/documents/82884/83933/ANEXO+TECNICO+PEGR-CC.pdf/bd7a3036-cb93-4459-82d1-e775053ef0ee

Lewis, J. (2019). The fluidity of risk: Variable vulnerabilities and uncertainties of behavioural response to natural and technological hazards. Disaster Prevention and Management: An International Journal, 28(5), 636–648. https://doi.org/10.1108/DPM-01-2019-0014

Ley 1581. Diario Oficial No. 48.587, Bogotá, Colombia, 18 de octubre de 2012

Ley 1712. Diario Oficial No. 49.084, Bogotá, Colombia, 6 de marzo de 2014 Ley N°1523. Diario Oficial 48411, Bogotá, Colombia, 24 de abril de 2012.

McEntire, D. (2012). Understanding and reducing vulnerability: From the approach of liabilities and capabilities. Disaster Prevention and Management, 21(2), 206–225. https://doi.org/10.1108/09653561211220007

Ministerio de Educación Nacional (2008). Guía para el mejoramiento institucional de la autoevaluación al plan de mejoramiento. In Serie Guías No. 34.

Ministerio de Educación Nacional (2015) Guía N°59: Lineamientos para la Formulación de Planes Escolares para la Gestión del Riesgo. Recuperado de https://redes.colombiaaprende.edu.co/ntg/men/pdf/lineamientos_formulacion_plane s_escolares.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones (2018). Lineamientos Para La Gestión De Riesgos De Seguridad Digital En Entidades Públicas Viceministerio De Economía Digital Dirección De Gobierno Digital Modelo De Gestión De Riesgos De Seguridad Digital (Mgrsd). Anexo 4, 1–38. Recuperado de:

https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P% C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc- 58f801d3657b

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). Guía para la Gestión y Clasificación de Activos de Información. 5, 18. https://www.mintic.gov.co/gestionti/615/articles5482_G5_Gestion_Clasificacion.pdf

Moyo, M., Abdullah, H., & Nienaber, R. C. (2013). Information security risk management in small-scale organisations: A case study of secondary schools computerised information systems. 2013 Information Security for South Africa - Proceedings of the ISSA 2013 Conference, 1–6. https://doi.org/10.1109/ISSA.2013.6641062

Öznacar, B. (2019). The risk analysis perceptions of "top level administrators" of ministry of education in the context of risk management: sample of northern cyprus and turkey. Revista inclusiones, vol. 6, no. 2, pp. 237,248, https://doi.org/10.1017/CBO9781107415324.004

Paton, D., & Johnston, D. (2004). Disaster Prevention and Management: An International Journal. An International Journal An International Journal Iss An International Journal Iss Disaster Prevention and Management: An International Journal Iss Universitas Negeri Semarang At, 10(18), 270–277. https://doi.org/10.1108/EUM0000000005930

Pattanajureepan, P., Sirisuthi, C., & Ieamvijarn, S. (2013). Development of risk management system in private school general education. Asian Social Science,

10(1), 276–282. https://doi.org/10.5539/ass.v10n1p276

Pérez Fernández, B., Sáenz Gómez, P., & Gómez Vega, W. (2016). Gestión del riesgo en una institución educativa de la ciudad de San José de Cúcuta, Colombia. Revista Virtual Universidad Católica Del Norte, 0(48), 183-214–214.

Ruiz, E. (2015). System information management for risk reduction (GIRE System) in schools of Costa Rica. ISCRAM 2015 Conference Proceedings - 12th International Conference on Information Systems for Crisis Response and Management, 2015- Janua.

Şahin, S., & Ak, Ö. F. (2018). A new approach to school management: Determination of student related risks according to the internal control. Universal Journal of Educational Research, 6(4), 672–690.

Sistema Nacional para la Prevención y Atención de Desastres. (2010). Guía Plan Escolar para la Gestión del Riesgo. Proyecto de Asistencia Técnica en Gestión del Riesgo a Nivel Municipal y Departamental en Colombia. Recuperado de: http://cedir.gestiondelriesgo.gov.co/archivospdf/4-GPEGRColombia.pdf

Savelides, S. Mihiotis, A. Koutsoukis, N. (2015). Crisis management for secondary education: a survey of secondary education directors in Greece, International Journal of Educational Management, Vol. 29 Iss 1 pp. 18 – 43

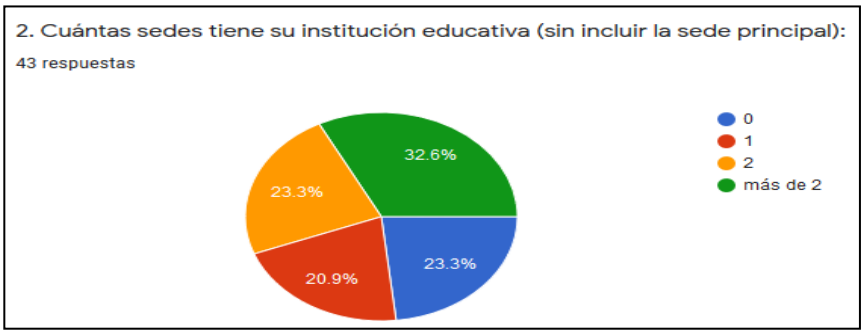
Yasuda, H. (2010). A risk management system to oppose cyber bullying in high school: Warning system with leaflets and emergency staffs. Informatica (Ljubljana), 34(2), 255–259.

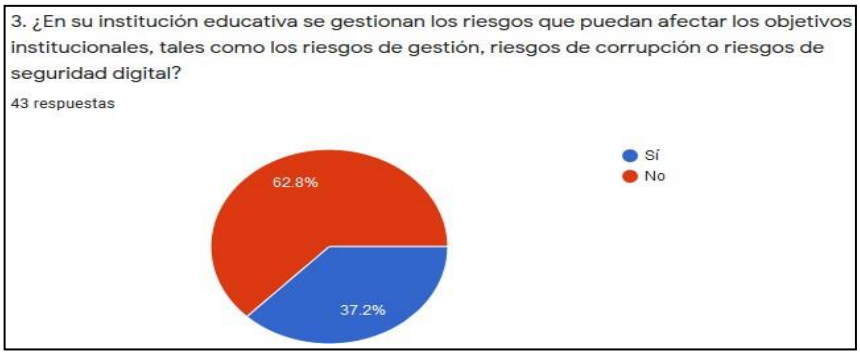
Anexos

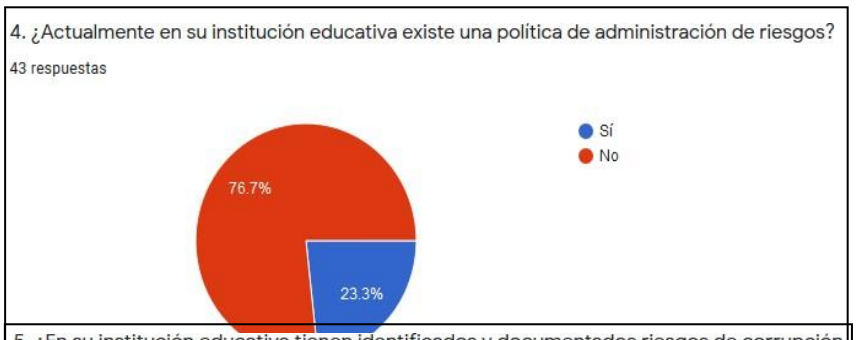
Anexo 1. Encuesta sobre la administración del riesgo aplicada a las Instituciones Educativas Públicas del departamento del Atlántico.

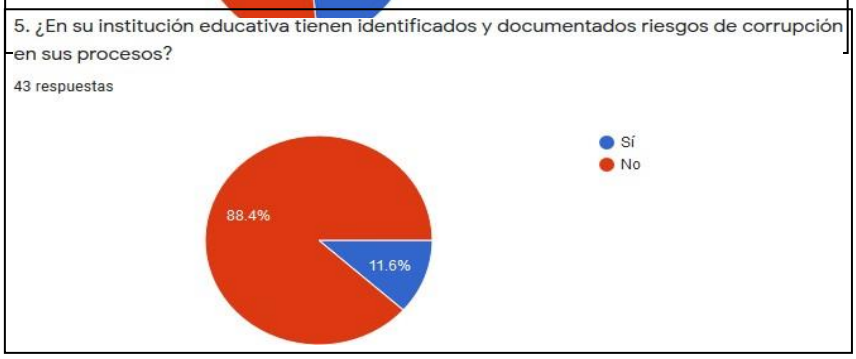
Este anexo muestra la encuesta realizada a 43 IE del departamento del Atlántico, con su respectivo resultado:

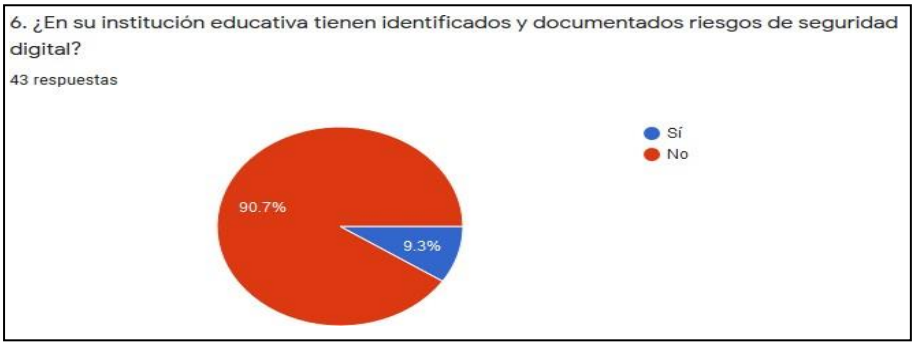
1. Nombre de la Institución Educativa: _____

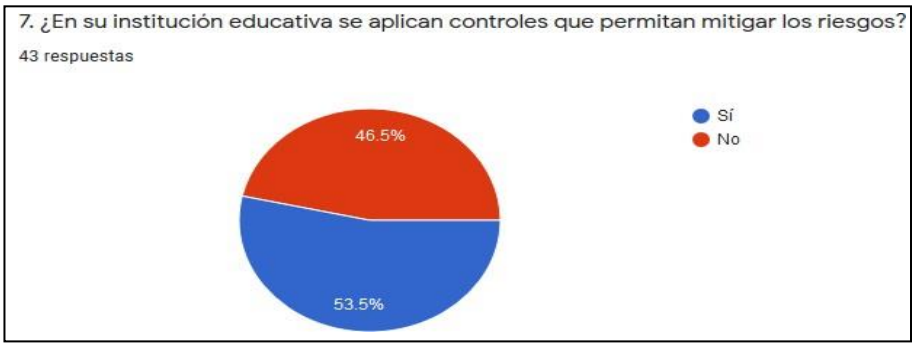




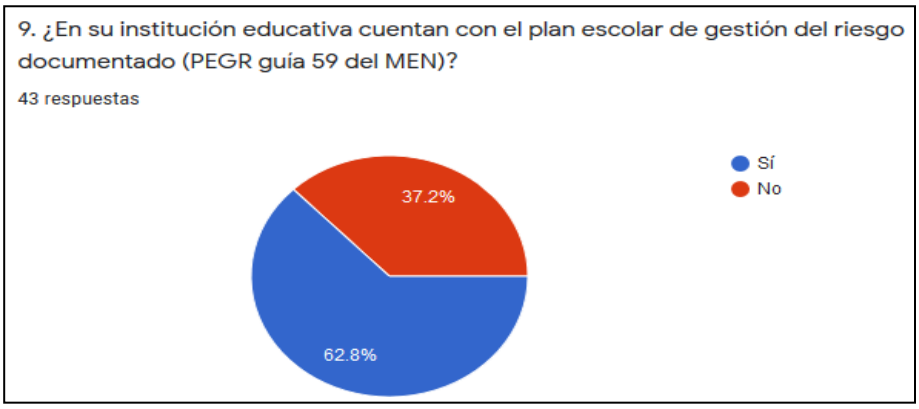




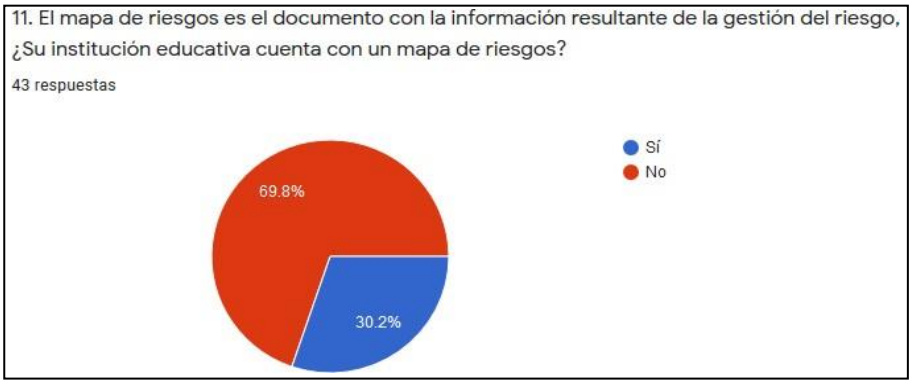

6. ¿En su institución educativa tienen identificados y documentados riesgos de seguridad digital?
43 respuestas
Sí
No
90.7%
9.3%


7. ¿En su institución educativa se aplican controles que permitan mitigar los riesgos?
43 respuestas
Sí
No
46.5%
53.5%

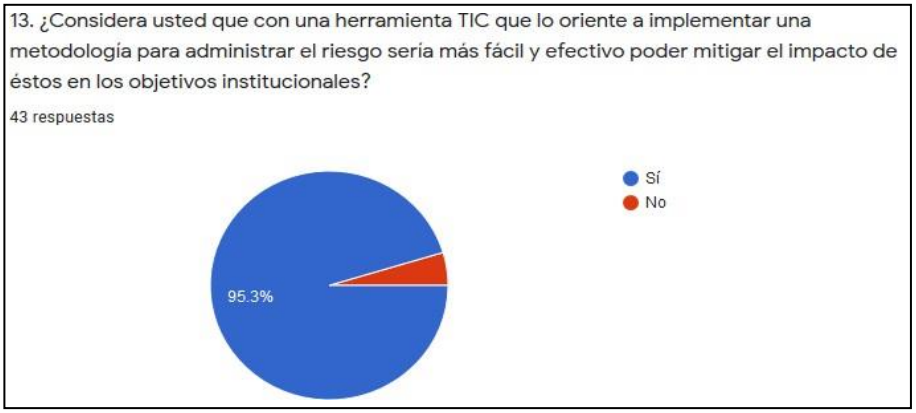

8. ¿En su institución educativa tienen evidencias de la ejecución de los controles que permitan mitigar los riesgos?
43 respuestas
Sí
No
79.1%
20.9%


9. ¿En su institución educativa cuentan con el plan escolar de gestión del riesgo documentado (PEGR guía 59 del MEN)?
43 respuestas
Sí
No
37.2%
62.8%


10. ¿El PEGR está operativo, es decir, funcionando y con las brigadas conformadas (evacuación, primeros auxilios, contra incendios)?
43 respuestas
Sí
No
79.1%
20.9%


11. El mapa de riesgos es el documento con la información resultante de la gestión del riesgo, ¿Su institución educativa cuenta con un mapa de riesgos?
43 respuestas
Sí
No
69.8%
30.2%


12. Teniendo en cuenta las respuestas anteriores, qué tan preparada está su I.E para identificar, evaluar y gestionar los riesgos actuales y emergentes que se presentan? (responda de 1 a 5, donde 5 es muy preparada)
43 respuestas
1
2
3
4
5
32.6%
39.5%
20.9%


13. ¿Considera usted que con una herramienta TIC que lo oriente a implementar una metodología para administrar el riesgo sería más fácil y efectivo poder mitigar el impacto de éstos en los objetivos institucionales?
43 respuestas
Sí
No
95.3%

Anexo 2. Política de administración del riesgo de la Institución Educativa Atlántico para la Gente

Introducción

Teniendo en cuenta que la política de administración del riesgo establece los principios básicos de actuación para el control y la gestión de los riesgos de toda naturaleza a los que se enfrentan las entidades, la Institución Educativa Atlántico Para la Gente presenta a continuación el marco de acción que le permitirá tomar decisiones relativas a la administración del riesgo.

Términos y definiciones

✓ **Gestión del riesgo**: proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

✓ **Riesgo de gestión**: posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

✓ **Riesgo de corrupción:** posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado

✓ **Riesgo de seguridad digital:** combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales.

✓ **Riesgo inherente:** es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

✓ **Riesgo residual:** nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento

✓ **Impacto:** se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

✓ **Control:** medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

✓ **Amenazas:** situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

✓ **Mapa de riesgos:** documento con la información resultante de la gestión del riesgo.

✓ **Probabilidad**: se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad

(Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018, págs. 8,9)

Objetivo

Fortalecer el desempeño de la Institución Educativa Atlántico Para la Gente a través de parámetros que permitan una adecuada administración de riesgos físicos, de gestión, corrupción y seguridad digital, asegurando de esta forma el logro de los objetivos institucionales y de procesos.

Alcance

La administración del riesgo en la Institución Educativa Atlántico Para la Gente estará presente en todos los procesos de la institución, de igual forma se incluirá en todas las sedes, con el fin de garantizar un adecuado conocimiento y control de los riesgos en toda la IE.

Niveles de aceptación del riesgo

En la I. E Atlántico Para la Gente se consideran aceptables los riesgos que se encuentren en el

nivel de riesgo bajo.
Los riesgos de corrupción no tienen nivel de aceptación, por lo tanto, son inaceptables.

Niveles para calificar el impacto

El nivel para calificar el impacto se clasifica en: insignificante, menor, moderado, mayor y catastrófico.
En los riesgos físicos el nivel de impacto se califica como sigue:

Impacto	Descriptor
Catastrófico	Los efectos del evento afectan entre el 76% y el 100% de la Institución Educativa. Generación de muertes y/o pérdidas de grandes montos de dinero.
Mayor	Los efectos del evento afectan entre el 51% y el 75% de la Institución Educativa. Generación de alguno heridos y/o pérdidas económicas considerables
Moderado	Los efectos del evento afectan entre el 26% y el 50% de la Institución Educativa. Generación de lesiones personales de no mucha gravedad y/o pérdidas económicas
Menor	Los efectos del evento afectan entre el 1% y el 25% de la Institución Educativa. Generación de lesiones personales muy leves y/o pequeñas pérdidas económicas
Insignificante	Los efectos del evento no afectan la infraestructura de la Institución Educativa. No se generan heridos ni pérdidas económicas de consideración.

Para los riesgos de gestión, el nivel de impacto se califica de la siguiente manera:

Impacto	Descriptor
Catastrófico	Interrupción de las operaciones de la Institución Educativa por más de cinco (5) días Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. Pérdida de información crítica para la Institución que no se puede recuperar Imagen institucional afectada en el orden regional o nacional por actos o hechos de corrupción comprobadas.
Mayor	Interrupción de las operaciones de la Institución Educativa por más de tres (3) días Sanción por parte del ente territorial Pérdida de información crítica para la Institución que puede ser recuperada de forma parcial o incompleta Imagen institucional afectada en el orden regional o nacional por incumplimiento en la prestación del servicio a la comunidad educativa
Moderado	Interrupción de las operaciones de la Institución Educativa por más de dos (2) días

	Reclamaciones o quejas de la comunidad educativa que podrían implicar una denuncia o demanda ante el ente territorial Inoportunidad en la información, ocasionando retrasos en la atención de la comunidad educativa Imagen institucional afectada en el orden regional o nacional por retrasos en la prestación del servicio a la comunidad educativa
Menor	Interrupción de las operaciones de la Institución Educativa por algunas horas Reclamaciones o quejas de la comunidad educativa que implican investigaciones internas disciplinarias Imagen institucional afectada en el orden local por retrasos en la prestación del servicio a la comunidad educativa
Insignificante	No hay interrupción de las operaciones de la Institución Educativa No se generan sanciones por parte de Ningún ente No se afecta la imagen institucional de forma significativa

En los riesgos de corrupción los niveles de impacto se definen para cada riesgo, siguiendo lo mostrado en la siguiente tabla:

No.	**Pregunta:** **Si el riesgo de corrupción se materializa podría…**	**Respuesta**	
		SI	**NO**
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		

11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		
Responder afirmativamente de UNA a CINCO preguntas genera un impacto **moderado** Responder afirmativamente de SEIS a ONCE preguntas genera un impacto **mayor** Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto **catastrófico**			
Moderado: Genera medianas consecuencias para la Institución Educativa			
Mayor: Genera altas consecuencias para la Institución Educativa			
Catastrófico: Genera consecuencias desastrosas para la Institución educativa			

Para los riesgos de seguridad digital se manejan los niveles de impacto de la siguiente forma:

Impacto	**Descriptor**
Catastrófico	Afectación muy grave de la integridad, disponibilidad y confidencialidad de la información
Mayor	Afectación grave de la integridad, disponibilidad y confidencialidad de la información
Moderado	Afectación moderada de la integridad, disponibilidad y confidencialidad de la información
Menor	Afectación leve de la integridad, disponibilidad y confidencialidad de la información
Insignificante	Sin afectación de la integridad, disponibilidad y confidencialidad de la información

Tratamiento del riesgo

Es el proceso para modificar el riesgo, buscando su mitigación y/o reducción. La IE Atlántico para la Gente decidirá el tratamiento a aplicar a cada uno, teniendo como opción: aceptarlo, evitarlo, compartirlo o reducirlo.

- ✓ Aceptar el riesgo: Si el nivel de riesgo es bajo no es necesario aplicar controles, por lo tanto, se acepta el riesgo, sin embargo, se debe realizar seguimiento.
- ✓ Evitar el riesgo: Cuando los escenarios de riesgo identificado son muy extremos se puede tomar la decisión de evitar el riesgo, esto es, abandonar o cancelar la(s) actividad(es) que dan lugar al riesgo, y no iniciar y/o continuar con las actividades que lo causan.
- ✓ Compartir el riesgo: Cuando para la IE es muy difícil reducir el riesgo a un nivel aceptable, éste puede ser compartido con otra parte interesada, por ejemplo, por medio de seguros o tercerización.
- ✓ Reducir el riesgo: Se establecen medidas para reducir el riesgo, a través de la implementación de controles, de modo que el riesgo residual sea pueda reevaluar como aceptable para la Institución, es decir de nivel bajo.

Divulgación

La política de administración del riesgo, junto con los mapas de riesgo serán divulgados a través de los canales de comunicación de la IE (Página web, periódico institucional), con el fin de que toda la comunidad educativa se informe de la gestión de riesgos de la Institución.

Capacitación

Se realizará como mínimo una capacitación anual, que se llevará a cabo en alguna de las jornadas institucionales, con el fin de fortalecer las competencias de la comunidad educativa con respecto a la administración de riesgos.

Anexo 3. Ejemplo de caracterización de procesos

Para que la IE realice la caracterización de los procesos, debe registrar para cada uno por lo menos la siguiente información:

- ✓ Proceso: Nombre del proceso que se va a caracterizar
- ✓ Objetivo: Propósito del proceso
- ✓ Alcance: Se explica lo que cubre el proceso, o su campo de aplicación
- ✓ Responsable: Es la persona responsable del funcionamiento y control del proceso
- ✓ Entrada del proceso: Mencionar las entradas o insumos del proceso
- ✓ Actividades claves: listar las actividades claves del proceso
- ✓ Salida del proceso: Mencionar los productos y/o servicios resultados del proceso
- ✓ Cliente del proceso: es quien recibe los resultados del proceso
- ✓ Recursos: Mencionar los recursos (físicos, humanos, tecnológicos) con los que cuenta el proceso
- ✓ Requisitos (Normatividad): Mencionar los requisitos de la norma con los que tiene relación el proceso
- ✓ Documentos institucionales: Mencionar los documentos institucionales con los que se relaciona el proceso
- ✓ Indicadores: Listar los indicadores asociados al proceso

NOMBRE DE LA I. E			
PROCESO	Direccionamiento estratégico y horizonte institucional		
OBJETIVO	Establecer los lineamientos que orientan la acción institucional en todos y cada uno de sus ámbitos de trabajo		
ALCANCE	Aplica para el gobierno escolar, horizonte institucional, autoevaluación y plan de mejoramiento		
RESPONSABLE	Rector		
ENTRADA DEL PROCESO	**ACTIVIDADES CLAVES**	**SALIDA DEL PROCESO**	**CLIENTE DEL PROCESO**
Ley 115 de 1994 Decreto 1860 de 1994 Decreto 1075 de 2015 Políticas y Lineamientos del MEN Necesidades de la comunidad educativa	Planteamiento estratégico: misión, visión, valores institucionales (principios), metas, conocimiento y apropiación del direccionamiento, política de inclusión de personas con capacidades disímiles y diversidad cultural.	Gobierno escolar formalizado Horizonte institucional PMI (Plan de mejoramiento institucional) PEI contextualizado	Comunidad educativa
RECURSOS	**REQUISITOS (NORMATIVIDAD)**	**DOCUMENTOS INSTITUCIONALES**	**INDICADORES**
Humanos: Comunidad educativa Infraestructura: Planta física, salón de reuniones, computador, video beam, internet, papelería Información (documentos): Guía 34	Ley 115 (Ley general de educación) Decreto 1075 (Decreto único reglamentario del sector educación) Decreto 1860 (Decreto que reglamenta parcialmente la ley 115)	PMI PEI	Porcentaje de ejecución del plan de mejoramiento Índice de inclusión Índice de satisfacción con el clima escolar

Otros:			

Anexo 4. Controles para la mitigación de riesgos de seguridad digital

Las IE podrán mitigar los riesgos de seguridad digital empleando los controles sugeridos por el anexo A del estándar ISO/IEC 27001:2013. A continuación, se muestra una lista de ejemplos:

Políticas de seguridad de la información	**Control**
Políticas para la seguridad de la información.	Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.
Responsabilidades de la dirección	La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización
Proceso disciplinario	Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información
Inventario de activos	Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.
Propiedad de los activos	Los activos mantenidos en el inventario deberían tener un propietario.
Devolución de activos	Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
Manejo de activos	Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización
Transferencia de medios físicos	Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte
Política sobre el uso de los servicios de red	Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente
Suministro de acceso de usuarios	Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios
Seguridad de oficinas, recintos e instalaciones	Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
Ubicación y protección de los equipos	Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado
Servicios de suministro	Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
Mantenimiento de equipos	Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas

Anexo 5. Valoración de la propuesta metodológica por parte de expertos

Estimado experto:
Teniendo en cuenta su perfil y experiencia en el sector educativo, específicamente en instituciones públicas de básica y media, usted ha sido seleccionado como experto para solicitar su opinión y retroalimentación, con respecto a la propuesta metodológica presentada en este documento, relacionada con la administración del riesgo en las instituciones educativas públicas del Departamento del Atlántico, soportada en las TIC. Para lograr lo anterior, se le solicita evaluar cinco criterios de acuerdo a su grado de aprobación o desaprobación.

1. **Soporte teórico:**
   ¿Considera usted que la presente propuesta metodológica es consistente con la concepción de administración de riesgos en las IE y lo establecido en la guía 59 del MEN?

Totalmente de acuerdo (5)	De acuerdo (4)	Medianamente de acuerdo (3)	En desacuerdo (2)	Totalmente en desacuerdo (1)

2. **Pertinencia:**
   ¿Considera usted que la aplicación de la presente propuesta metodológica es propicia teniendo en cuenta el contexto de las IE?

Totalmente de acuerdo (5)	De acuerdo (4)	Medianamente de acuerdo (3)	En desacuerdo (2)	Totalmente en desacuerdo (1)

3. **Coherencia metodológica:**
   ¿Considera usted que la estructura de la metodología y la interrelación de sus pasos o etapas, garantizan la efectividad en la administración de riesgos en las IE?

Totalmente de acuerdo (5)	De acuerdo (4)	Medianamente de acuerdo (3)	En desacuerdo (2)	Totalmente en desacuerdo (1)

4. **Factibilidad de aplicación:**
   ¿Considera usted viable la aplicación de la presente propuesta metodológica en las IE, teniendo en cuenta las condiciones particulares de cada una?

Totalmente de acuerdo (5)	De acuerdo (4)	Medianamente de acuerdo (3)	En desacuerdo (2)	Totalmente en desacuerdo (1)

5. **Importancia y/o contribución de la propuesta metodológica**
   ¿Considera usted que la presente propuesta metodológica generará un valor agregado que impactará de manera positiva la gestión de riesgos en las IE?

Totalmente de acuerdo (5)	De acuerdo (4)	Medianamente de acuerdo (3)	En desacuerdo (2)	Totalmente en desacuerdo (1)