Propuesta desde la gestión de proyectos de un modelo de GRC (Gobierno, riesgo, y cumplimiento) enfocado a la administración de tecnologías de la información y comunicaciones para mejorar los procesos empresariales de la Defensoría del Pueblo de Bogotá, D.C.

Zuñiga Barros, Jorge Eliecer

Corporación Universitaria Minuto de Dios

Rectoría Virtual

Programa Especialización en Gerencia de Proyectos

junio de 2024

IMPLEMENTACIÓN MODELO GRC EN LA DEFENSORIA DEL PUEBLO

Propuesta desde la gestión de proyectos de un modelo de GRC (Gobierno, riesgo, y cumplimiento) enfocado a la administración de tecnologías de la información y comunicaciones para mejorar los procesos empresariales de la Defensoría del Pueblo de Bogotá, D.C.

Zuñiga Barros, Jorge Eliecer

Trabajo de Grado presentado como requisito para optar al título de Especialista en Gerencia de Proyectos

Asesor
Sergio Andrés Zabala Vargas
Doctor en Tecnología Educativa

Corporación Universitaria Minuto de Dios

Rectoría Virtual

Programa Especialización en Gerencia de Proyectos

junio de 2024

Contenido

Lista **de tablas**

Lista de figuras

Lista de gráficos

Resumen

El presente proyecto se evidencia en la institución en estudio, la dificultad para alcanzar los objetivos estratégicos de la entidad y el desarrollo de los proyectos trasversales, falta de formación y aplicación de las políticas definidas por TIC, además se evidencia una desarticulación de los procesos TI, integridad de la información, así como riesgos en la consecución de los objetivos de los procedimientos de las TIC. Teniendo como objetivo principal diseñar un modelo de GRC (Gobierno, riesgo, y cumplimiento) enfocado a la administración de tecnologías de la información y comunicaciones para mejorar los procesos empresariales de la Defensoría del Pueblo de Bogotá, D.C, proponiendo mejoras en los procedimientos, que contribuyan a un mayor control y prevención de riesgos de forma integrada. Metodológicamente, se encuentra inmerso dentro del paradigma mixto, de tipo es descriptivo con un diseño de campo, como población se seleccionaron los seis (6) empleados del departamento de tecnología de la información de la Defensoría del Pueblo de Colombia sede Bogotá. Y como informante clave el jefe de seguridad de información de la entidad. Se pretende identificar el alcance que tienen los recursos, riesgos de TI y la aplicación de los estándares de gestión TI para maximizar utilidades y hacer procesos verdaderamente efectivos que vayan alineados a los objetivos, visión de la organización y estándares de calidad de acuerdo con las normas actuales. Teniendo en cuenta el diseño y el diagnostico de aplicabilidad, se debe implementar la normatividad de acuerdo con las políticas y normas de referencia estandarizadas, para proponer a las organizaciones públicas la investigación de los recursos de tecnologías de la información y estándares de gestión de TI con el fin de que estas puedan ser aplicadas y utilizadas de una manera más apropiada para mejorar la calidad de los servicios y fortalecer los procesos.

Palabras clave: - GRC, ISO, TI, Organizaciones, Normas, Estándares

Abstract

This project is evident in the institution under study, the difficulty in achieving the strategic objectives of the entity and the development of transversal projects, lack of training and application of the policies defined by ICT, in addition, a disarticulation of the IT processes is evident. . , integrity of the information, as well as risks in achieving the objectives of the ICT procedures. Having as its main objective to design a GRC (Government, Risk, and Compliance) model focused on the administration of information and communications technologies to improve the business processes of the Ombudsman's Office of Bogotá, D.C., proposing improvements in procedures, which They will contribute to greater control and prevention of risks in an integrated manner. Methodologically, it is immersed within the mixed paradigm, of a descriptive type with a field design, as a population, six (6) employees of the information technology department of the Colombian Ombudsman's Office, Bogotá headquarters, were selected as an intentional sample. And as a key informant, the head of information security of the entity. The aim is to identify the scope of resources, IT risks and the application of IT management standards to maximize profits and make truly effective processes that are aligned with the objectives, vision of the organization and quality standards in accordance with the regulations. . current. Taking into account the design and the diagnosis of applicability, the regulations must be implemented in accordance with the standardized reference policies and standards, to propose to public organizations the investigation of information technology resources and IT management standards with so that these can be applied and used in a more appropriate way to improve the quality of services and strengthen processes.

Keywords: GRC, ISO, IT, Organizations, Norms, Standards

Introducción

La administración de los recursos de tecnologías de la información y los estándares de gestión y riesgos de TI que hoy en día aplican las entidades públicas del estado colombiano son las apropiadas para mejorar la calidad de los servicios y fortalecer los procesos.

El crecimiento exponencial de la globalización de la información en medios digitales y redes informáticas y de comunicación, como resultado del creciente desarrollo tecnológico ha permitido a las organizaciones, personas y sociedad en general, mejorar el acceso a la información como como insumo principal para la toma de decisiones y el conocimiento colectivo; Sin embargo este crecimiento y facilidad de acceso a la información también ha generado un desafío de alto costo para las áreas de TI, frente al riesgo de comprometer datos relevantes, ya sean de carácter personal, institucional, financiero, o de cualquier otra índole.

De acuerdo al criterio de Celada et al. (2016) “busca el logro de los objetivos organizacionales en función del modelo de negocio planteado, midiendo el riesgo que se quiere asumir para alcanzar los mismos, y actuando con la integridad necesaria, más allá del cumplimiento de normas obligatorias”. (pág. 15).

Es por esto que de cara al riesgo de seguridad, se deben implementar metodologías y prácticas que conlleven a la protección de nuestros datos, manteniéndolos protegidos de accesos ilegales o uso delictivo, garantizando la confidencialidad, integridad y disponibilidad de la información, tarea que se apalanca en estándares predefinidos y normas internacionales en materia de seguridad que pueden compilarse en el llamado SGSI (Sistema de gestión de Seguridad de la Información) que permitirán tener un control, gestión y visión holística del tratamiento de la seguridad de información en una organización.

Si bien parte de los datos que soportan el modelo de GRC residen en aplicaciones tecnológicas y su incorporación permite transformar los datos de una información poderosa a la toma de decisiones y al monitoreo de su comportamiento a través de indicadores de riesgos, GRC no es solo tecnología de información. Es importante que los órganos de gobierno se mantengan en constante comunicación con la administración y con los responsables del modelo, para monitorear las actividades y determinar los planes de acción en caso de ser necesario.

Con base a lo anterior, se pretende elaborar diseñar un modelo de GRC (Gobierno, riesgo, y cumplimiento) enfocado a la administración de tecnologías de la información y comunicaciones para mejorar los procesos empresariales de la Defensoría del Pueblo de Bogotá, D.C, proponiendo mejoras en los procedimientos, el cual según Yaerim et al. (2017)“ busca contribuir a un mayor control y prevención de riesgos de forma integrada, adecuadamente diseñado e implantado que permita establecer una relación directa entre cada una de las actividades realizadas por la organización” (pág. 2).

En el trabajo, se desarrollaron los siguientes aspectos: inicialmente se presenta el En el capítulo 1. Planteamiento del problema, donde se señala la descripción del problema, la pregunta de investigación, el objetivo general, los objetivos específicos, y la justificación de la investigación.

Seguidamente, se presenta el capítulo 2, marco de referencia en el cual se desarrollan el marco de antecedentes, el marco conceptual luego se presenta el marco legal. Luego se procede a desarrollar el capítulo 3, metodología, donde se señala enfoque y alcance de la investigación, la población y muestra, la definición de la población, el instrumento, la descripción de procedimientos, el análisis de información, las consideraciones éticas y los Instrumentos de aceptación y autorización

De la misma forma, capítulo 4 correspondiente a los resultados se presenta el análisis de los datos obtenidos luego de aplicar los instrumentos, por objetivos y luego la discusión de resultados, seguidamente, se presenta el capítulo 5 la propuesta, donde se refleja el modelo de GRC (Gobierno, riesgo, y cumplimiento) enfocado a la administración de tecnologías de la información y comunicaciones para optimizar los procesos de la Defensoría del Pueblo de Bogotá, D.C., luego las conclusiones, recomendaciones, y finalmente los anexos.

1. PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción del problema

El crecimiento exponencial de la globalización de la información en medios digitales y redes informáticas y de comunicación, como resultado del creciente desarrollo tecnológico ha permitido a las organizaciones, personas y sociedad en general, mejorar el acceso a la información como como insumo principal para la toma de decisiones y el conocimiento colectivo; generando un desafío para las áreas de TIC, frente al riesgo de comprometer datos relevantes, ya sean de carácter personal, institucional, financiero, o de cualquier otra índole.

Por lo cual, las organizaciones se han preocupado por implementar sistemas de GRC (Gobierno, riesgo, y cumplimiento) enfocado a la administración de tecnologías de la información y comunicaciones que permitan el seguimiento y cumplimiento de los objetivos, identificando las entradas y salidas de la información, así como su monitoreo y gestión de riesgos.

En opinión de Vázquez (2015, cómo se citó en Guzmán et al., 2017) “El modelo GRC es…una capacidad de la organización para potenciar el ahorro de los costos, la optimización operativa, el mejoramiento continuo, la eficiente gestión de riesgos y controles, y la gestión integrada del desempeño con fuertes niveles de aseguramiento”. (pág. 48).

En este sentido, la aplicación de un modelo de gestión de riesgos y cumplimiento, enfocado en la administración de las TIC en las instituciones públicas, permitiría obtener grandes beneficios, mediante la optimización de recursos, prevención de riesgos, mayor capacidad de respuesta, pudiendo ser mucho más eficaces en el cumplimiento de las metas y objetivos, así como ofrecer a los ciudadanos mayor seguridad sobre la información que manejan de ellos.

En España, (García, 2018) elaboró un estudio en las universidades públicas, donde determinó:

> no cuentan con un sistema integral que dé respuesta a las responsabilidades que afrontan en materia de Gobierno Corporativo, Gestión de Riesgos y Cumplimiento Normativo, en el mejor de los casos, funciones mínimas y parciales son desarrolladas por Unidades o Servicios muy dispersas en su estructura administrativa”….lo cual deriva en una inadecuada ejecución de las políticas públicas institucionales, que provoca ineficiencias en el empleo de fondos públicos y riesgos de incumplimiento normativo en el ejercicio de responsabilidades de los Órganos de Gobierno y responsables públicos. (pág. 13-14)

A nivel latinoamericano, el estudio realizado por López eta al. (2017) en las pequeñas y medianas empresas de México, demostró que para aplicar un de modelo de Gobernabilidad, Riesgos y Cumplimiento, debe estar a las necesidades. De cada organización tomando en consideración, dar seguimiento a los proyectos, visualizando la estructura de la misma, para lo

cual es imprescindible relacionar los objetivos e indicadores, así como los niveles empresariales dando seguimiento, control y cumplimiento a las metas trazadas, midiendo y priorizando los riesgos, asegurando así el cumplimento de los objetivos. Sin embargo, “solo 1l 1 % de las % cuenta con dos o más sistemas de gestión implementados e integrados. La mayoría de estas empresas gestionan su documentación de forma tradicional…lo que representa un enorme reto para la seguridad de la información y el almacenamiento de datos” (pág. 4)

En el caso colombiano, (Salah, 2017) elaboró una investigación en la Gobernación de Magdalena, donde se identificaron una serie de brechas en la arquitectura empresarial y los sistemas de información de la Entidad que indican donde se está y donde se quiere llegar, además, las estructuras de gobierno no están claramente definidas, así como sus metas, roles para determinar la toma de decisiones sobre los principales dominios de TIC.

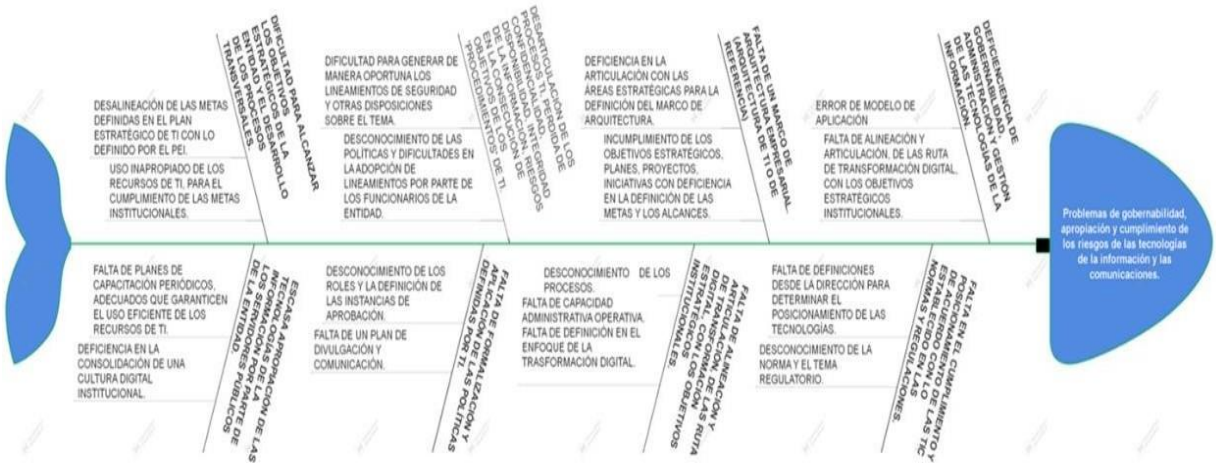
Además, “existen riesgos asociados a los procesos que pueden desencadenar en situaciones que pongan en riesgo la continuidad impactando de forma financiera, de cumplimiento, operativos; entre otros” (pág. 207), los cuales mediante la aplicación de un modelo de GRC (Gobierno, riesgo, y cumplimiento) enfocado a la administración de tecnologías de la información y comunicaciones, se pueden mitigar.

Tal es el caso, de la Defensoría del Pueblo de Bogotá, D.C., donde según observaciones asistemáticas realizadas por los investigadores, existen ineficiencias tecnológica, dificultad para alcanzar los objetivos estratégicos de la entidad y el desarrollo de los proyectos trasversales, falta de formación y aplicación de las políticas definidas por TIC, además se evidencia una desarticulación de los procesos TI, integridad de la información, así como riesgos en la consecución de los objetivos de los procedimientos de las TIC, además, se observa una falta de alineación y articulación de las rutas de trasformación digital con los objetivos estratégicos institucionales, así como un marco de arquitectura empresarial.

Aunado a ello, se pudo evidenciar que existen deficiencias de gobernabilidad y gestión de las TIC, además de una ausencia de cumplimiento y posicionamiento de acuerdo a lo establecido en las normas y regulaciones vigentes.

Lo anteriormente expuesto, podría ocasionar que existiese un uso ineficiente de los recursos públicos, perdida de confidencialidad, así como una atención poco eficaz a los ciudadanos, además, un manejo inadecuado de la información, debido a la escasa implementación y utilización de herramientas que permitan dar seguimiento a la gestión de Riesgos y Cumplimiento proporciona, lo cual ocasiona una menor capacidad de respuesta, y poca verificación, del cumplimiento legal o regulatorio, así como poca considerando de los riesgos y las debilidades existentes.

Figura 1. ***Diagrama de causa – efecto***



Fuente: Elaboración propia (2024)

1.1.1 La pregunta de investigación

¿Cuál es el efecto de proponer, desde la gestión de proyectos y el uso de las TIC, un modelo de gobierno, riesgo y cumplimiento GRC para mejorar los procesos empresariales de la Defensoría del pueblo de Bogotá, D.C.?

1.2. Objetivos de investigación

1.1.2 Objetivo general

Diseñar un modelo de GRC (Gobierno, riesgo, y cumplimiento) enfocado a la administración de tecnologías de la información y comunicaciones para mejorar los procesos empresariales de la Defensoría del Pueblo de Bogotá, D.C, proponiendo mejoras en los procedimientos, que contribuyan a un mayor control y prevención de riesgos de forma integrada.

1.1.3 Objetivos específicos

Diagnosticar el alcance que tienen los recursos, riesgos de TIC y la aplicación de los estándares de gestión TIC en la Defensoría del Pueblo de Bogotá, D.C., estableciendo las falencias existentes.

Identificar los componentes que hacen parte del modelo de GRC (Gobierno, riesgo, y cumplimiento), enfocado a la administración de tecnologías de la información y comunicaciones, para mejorar los procesos de la Defensoría del Pueblo de Bogotá, D.C

Proponer un modelo de GRC (Gobierno, riesgo, y cumplimiento) enfocado a la administración de tecnologías de la información y comunicaciones para optimizar los procesos de la Defensoría del Pueblo de Bogotá, D.C.,

1.2 Justificación de la investigación

La Defensoría del Pueblo de Bogotá, D.C, es un ente público, el cual tal como lo refleja su portal web (Defensoría del Pueblo, s.f.) es la “encargada de defender, promocionar, proteger y divulgar los derechos humanos, las garantías y libertades de los habitantes del territorio nacional y de los colombianos residentes en el exterior…” motivo por el cual, debe estar a la vanguardia de los avances tecnológicos, contribuyendo con la política digital del país, procurando dar una atención eficiente a todos los ciudadanos que garantice la trasparencia y confiabilidad de la información que manejan.

En este sentido, es necesario, que la institución, pueda ofrecer seguridad a los ciudadanos respecto a la información que manejan, mediante el diseño de un modelo de GRC (Gobierno, riesgo, y cumplimiento) enfocado a la administración de tecnologías de la información y comunicaciones que permita la mejora de los procesos en la Defensoría del Pueblo de Bogotá, D.C, en pro de la eficiencia institucional.

Desde el punto de vista teórico, la investigación resulta relevante, ya que se expondrán diferentes teorías referentes a GRC (Gobierno, riesgo, y cumplimiento) enfocado a la administración de tecnologías de la información y comunicaciones, los cuales enriquecerán el conocimiento, además de poder servir de insumo a futuras investigaciones que se realicen sobre el tema.

Cabe acotar, que (Pareja, 2022) señala “el Gobierno, Riesgo y Cumplimiento (GRC), es clave para tomar mejores decisiones, mitigar amenazas, lograr los objetivos de la compañía y alinear la empresa con su estrategia para centralizar la información, tener convergencia, transparencia, control interno, auditoría e investigación”.

Desde el punto de vista práctico, dando cumpliendo a los objetivos propuestos, luego de realizar el análisis de los resultados del estudio en base a las falencias encontradas, se propondrá un modelo de GRC (Gobierno, riesgo, y cumplimiento) enfocado a la administración de tecnologías de la información y comunicaciones para optimizar los procesos de la Defensoría del Pueblo de Bogotá, D.C., lo cual se traducirá en beneficios tanto para la institución como para los ciudadanos, ya que; se podrán convertir en fortalezas las debilidades detectadas en el estudio.

Desde el punto social, el estudio es relevante, Ya que; con base a las falencias encontradas se propondrá un modelo de GRC (Gobierno, riesgo, y cumplimiento) enfocado a la administración de tecnologías de la información y comunicaciones para optimizar los procesos de la Defensoría del Pueblo de Bogotá, D.C., lo cual beneficiará a la ciudadanía, al ofrecerles mayor transparencia, y un servicio más eficiente.

2. MARCO DE REFERENCIA

2.1. Marco de Antecedentes

En este apartado se presentan estudios realizados con anterioridad sobre GRC (Gobierno, riesgo, y cumplimiento), los cuales sirven como fuente de información secundaria los cuales sirven de aporte para dar cumplimiento a los objetivos planteados. se hizo una búsqueda de los antecedentes investigativos que se publicaron de tesis de maestrías, especialización y doctorales en el ámbito iberoamericano. La búsqueda se hizo a través de las bases de datos que se encuentran en las redes virtuales como Skopus, Scielo, Reaserch, Isuu, en todos los repositorios que se pudieron encontrar de universidades, en revistas indexadas, teniendo en consideración estudios, que estuvieran publicadas desde hace siete años a la fecha

Inicialmente, se presenta el estudio realizado por López et al. (2017) titulado Propuesta de un sistema de gobierno, riesgos y cumplimiento para ser alineado a distintas normativas y regulaciones en pequeñas y medianas empresas. El cual tuvo como objetico elaborar una propuesta de un sistema de gobierno, riesgos y cumplimiento para ser alineado a distintas normativas y regulaciones en pequeñas y medianas empresas.

Metodológicamente, se enmarca en un paradigma post positivista, cualitativo de tipo de campo, realizando un análisis de las herramientas existentes en el mercado que ayudan a la administración de un sistema de gestión de riesgos de cumplimiento: El desarrollo de la herramienta a la medida fue descartado por la dificultad que significa asumir el riesgo en cuanto a la seguridad y el aseguramiento de la calidad por parte del departamento de TI.

Los resultados demuestran, que el diseño de un sistema que permita dar trazabilidad al cumplimiento de objetivos, identificando las actividades que se realizan, los roles, las responsabilidades, así como los datos de entrada y salida de cada una de ellas, aportaría valor de forma importante al seguimiento y al cumplimiento de los objetivos organizacionales. Para ello será necesario el uso de una plataforma que ya cuente con las características de seguridad y aseguramiento de calidad requeridas.

El citado antecedente, resulta se apoyó al presente estudio, debido a la importante y relevante información y bibliografía actualizada sobre sobre sistemas de GRC (Gobierno, riesgo, y cumplimiento), los cuales sirven como fuente de información secundaria, siendo de utilidad para conformar el marco referencial del presente estudio.

Dentro de este contexto, se presenta a García (2018), quien elaboró un trabajo de grado para optar al título de doctor en estado de derecho y gobernanza global, para la universidad de Salamanca en España, el cual lleva por nombre: gobernanza, gestión de riesgos y cumplimiento

normativo en la universidad pública, teniendo como propósito principal proponer un modelo de Universidad Pública, una concepción de Universidad, para que la deduciremos propuestas para las funciones corporativas de gobierno, gestión de riesgos y cumplimiento normativo que llevan a cabo.

La metodología utilizada se enmarca en un enfoque cualitativo, de tipo documental con un diseño bibliográfico, así mismo, se aplicaron entrevistas y reuniones de trabajo con profesionales de referencia en los campos de estudio. En uso de los principios heurísticos, se acudió a la modelización como idea, para establecer las líneas que definen el arquetipo de universidad sugerido. Se concluyó que el arquetipo de Universidad sugerido proporciona una respuesta efectiva a los desafíos actuales en materia de Gobierno, Gestión de Riesgos y Cumplimiento normativo.

El citado antecedente, es un aporte al presente estudio, debido a la valiosa y actualizada información sobre gobierno, riesgo y cumplimiento, lo cual sirvió de guía para la construcción del marco conceptual.

En este orden de ideas, Gutierrez & Sanchez (2018), elaboraron un estudio titulado: Diseño de un Modelo de Gestión de Riesgos basado en ISO 31.000:2012 para los Procesos de Docencia de Pregrado en una Universidad Chilena. Este estudio propone un modelo de gestión de riesgos, basado en la norma ISO 31000:2012 para el área de docencia de pregrado.

La gestión integral del riesgo es un componente estratégico esencial que permite establecer los puntos de control para evitar incumplimientos de los objetivos de la organización. El modelo propuesto permite apoyar los procesos de acreditación a través de indicadores orientados a mejorar la eficiencia de los procesos docentes. Para esto, el modelo genera matrices de riesgo y establece Indicadores Claves de Riesgo (KRI).

La aplicación del modelo se realiza en la Universidad Católica del Norte (UCN) en Chile, la cual cuenta con sedes en Antofagasta y Coquimbo en las que se imparten 35 carreras. Los resultados obtenidos permitieron definir riesgos inherentes y residuales en los procesos docentes y el establecimiento de controles sobre los procesos críticos.

Se concluye, que el principal riesgo de la docencia de pregrado de la UCN, corresponde a la falta de vinculación con los egresados y la generación de contactos con el medio, los cuales permiten retroalimentar a las carreras de su proceso formativo y realizar actividades de extensión de nutran la formación de los estudiantes, esto debido a la falta de sistematización de los datos de los egresados y el medio. Por otra parte, existe una fuerte amenaza de falla en el sub-proceso de progresión de los estudiantes que está dada por la incapacidad de sostener equipos de apoyo y nivelación a estudiantes de primer año a nivel institucional, ya que actualmente su

financiamiento se realiza con proyectos externos. En tercer lugar, el sub-proceso de dotación académica-docente presenta falencias en la evaluación de desempeño y en la realización de clases por parte de los académicos de las más altas jerarquías en el pregrado.

El citado antecedente, es un aporte al presente estudio, debido a la valiosa y actualizada información sobre el tema en estudio, lo cual sirvió de guía para la construcción del cuadro de operacionalización de las variables, sus dimensiones e indicadores. En segundo lugar, sirve de guía el desarrollo del marco teórico de la presente investigación.

Dentro de este contexto, Ixcamparic (2018) elaboró un estudio para optar al grado de magíster en administración financiera en la universidad de San Carlos de Guatemala, intitulado: análisis financiero de la implementación del modelo de gestión grc – gobierno, riesgo y cumplimiento en empresas comercializadoras de motocicletas en Guatemala, el cual tuvo como objetivo principal analizar el impacto financiero de implementar el modelo de gestión GRC en empresas comercializadoras de motocicletas en Guatemala, para determinar si el modelo permite minimizar los riesgos operativos y mejorar los resultados financieros

Metodológicamente, se encuentra bajo un enfoque cuantitativo de tipo exploratorio con un diseño de campo, la población estuvo conformada por las empresas comercializadoras de motocicletas, como técnica se utilizó a observación directa, así como entrevistas a expertos, gerentes administrativos, financieros, y cualquier persona involucrada directa o indirectamente en la implementación del modelo de gestión GRC en empresas comercializadoras de motocicletas. Se realizó análisis del balance general, estado de resultados, cálculo e índices de rentabilidad, proyección de estados financieros y los beneficios en la mitigación de riesgos operativos.

Se concluyó, que la implementación del modelo de gestión GRC en las empresa comercializadoras de motocicletas en Guatemala, dio como resultado incrementos en los índices de rentabilidad desde 1% hasta 18%; permitió además, mitigar 6 (seis) riesgos operativos y proyectó una ganancia del 2% como resultado del ejercicio para el año 2017, lo cual comprueba la hipótesis planteada.

El citado antecedente, es un aporte de este estudio, desde las referencias teóricas, ya que permite visualizar un contenido nuevo para la construcción de marco de referencia. De igual manera, es de utilidad al momento de diseñar un modelo de GRC (Gobierno, riesgo, y cumplimiento) enfocado a la administración de tecnologías de la información y comunicaciones para mejorar los procesos empresariales de la Defensoría del Pueblo de Bogotá, D.C; dado que la misma brinda herramientas relacionadas con los aspectos aplicativos a la investigación.

Seguidamente, Oviedo (2020), quien elaboró un estudio para optar a de magíster en gobierno de tecnología informática en la universidad del Norte, titulado: Modelo de Gobierno y Gestión de Riesgos Ti para las Universidades Públicas de Colombia: Caso de Estudio Universidad Popular del Cesar, el cual tuvo como objetivo Diseñar un modelo de gobierno y gestión de riesgos de TI para las universidades en la universidad caso de estudio. Bajo los postulados teóricos de ISACA (2018), Deloitte (2014), Selig (2008), MIT (2014), Nataliia & Oleksii (2019), entre otros.

Metodológicamente, el estudio se enmarco dentro del enfoque cualitativo, mediante el desarrollo de tres fases: 1. Investigación y exploración, en la cual se analizaron los marcos de trabajo, estándares existentes para un eficiente modelo de gobierno y gestión de riesgos de TI, en la fase 2. Valoración de riesgos, se efectuó un análisis de la investigación de riesgos, según su base de datos, analizando los controles existentes en la institución para el tratamiento de los mismos, así como también la temática de seguridad en el marco de transformación digital, de acuerdo Marco de la Transformación Digital para el Estado Colombiano, propuesto en Julio del 2020.

En la fase 3. Elaboración del Modelo de Gobierno y Gestión de Transformación Digital y Riesgo de TI para Universidades, se llevó a cabo el modelo de Gobierno y Gestión de Transformación Digital y Riesgo rediseñando controles existentes, indicadores y definiendo nuevas acciones a tomar para una mayor eficiencia del mismo, así como la forma de mitigar y tratar los riesgos. Fase cuatro: Plan de implementación del Modelo de Gobierno y Gestión de Transformación Digital y Risks una vez definidos los procesos se elaboró un plan o guía de implementación el cual contiene las distintas actividades a realizar de acuerdo a sus prioridades. Los resultados demostraron que la fase con mayor nivel de madurez es la de preparación, sin embargo, carece de un ejercicio cimentado en la gestión de riesgos que permita elevar el nivel de las fases restantes, para lo cual este modelo propone la ejecución de la ventana de AREM, aunado a ello, se evidenció la necesidad de crear nuevos indicadores planteados en materia de la organización, el cliente, la innovación, y las operaciones.

Asimismo, se evidencio, la inexistencia de crecimiento sostenible de la tecnología que apoye el modelo educativo, interrupción completa en la continuidad del negocio y el uso indebido del rol de administrador de los sistemas de información, y la pérdida de información por malware o su propagación en la red. En base a lo cual, se propuso un modelo para gobernar y gestionar los riesgos de TI en la Universidad en estudio.

Se concluyó, que planteamiento de un modelo debe partir de buenos cimientos, en el caso de este proyecto se inicia con los objetivos del gobierno de las tecnologías de la información

como aristas principales, seguido de la selección de actividades a priori en cada marco, haciendo una integración entre la gestión tradicional y no tradicional de riesgos, la ciberseguridad y la transformación digital.

El citado antecedente, es un gran aporte a la presente investigación debido a la literatura referente modelo para gobernar y gestionar los riesgos de TI, relacionado directamente con la variable objeto de estudio, además del modelo presentado lo cual servirá de guía para el desarrollo del modelo que se pretende proponer en la presente investigación.

En este orden y dirección, Buitrago & Vásquez (2020) elaboraron una investigación como requisito para optar al título de: Magister en gerencia de sistemas de información y proyectos tecnológicos, para la universidad EAN, intitulada: diseño de un modelo de gobierno de ti para el ministerio de ciencia, tecnología e innovación desde el marco de trabajo COBIT. Teóricamente se basó en los postulados de Lefort (2003), Rojas (2015),
Lagos & Vecino (2014), Villuendas (2011), entre otros.

Metodológicamente, se consideró de enfoque mixto, de tipo descriptivo, la población estuvo conformada por los 34 funcionarios y contratistas del Ministerio en estudio, como técnica se utilizó la observación revisando revisión de información necesaria para el proceso de análisis de la situación actual y medición del nivel de madurez como instrumento se diseñó una encuesta nivel de madurez del Gobierno de TI de Min Ciencias con cinco alternativas de respuesta, realizando la evaluación de los lineamientos de Gobierno de TI definidos en el Marco de Referencia de Arquitectura Empresarial (MRAE) versión de octubre de 2019.

Los resultados demuestran, que éste alcanza los objetivos propuestos, lográndose realizar el análisis de la situación actual, la identificación del nivel de madurez y las brechas existentes del gobierno de TI. También se definen los catalizadores para interacción de gobierno y gestión de TI, la definición de procesos según COBIT, el diseño de indicadores KPI y KGI, los lineamientos para gestión de riesgos según COBIT; que conforman el modelo de gobierno de TI propuesto para Min Ciencias según COBIT y su plan de implementación.

Se concluye, que en la medición del nivel de madurez de los procesos de gobierno de TI analizados en el proyecto se obtiene que se encuentran en un nivel de madurez 2, y las acciones propuestas se orientan a alcanzar el nivel deseado por la Entidad (4 gestionado cuantitativamente). Asimismo, se constató que parte del éxito en la implementación de un modelo de Gobierno de TI, requiere el compromiso y vinculación de la alta dirección de la Entidad, además de poner en marcha la propuesta de gobierno de TI que conlleva un ajuste en la cultura organizacional, en busca de la satisfacción de los usuarios y la generación de valor de las TI.

El antecedente citado, sirve de aporte a la presente investigación debido a la información sobre la variable de estudio, así como la metodología utilizada la cual servirá de base para desarrollar el marco metodológico, además de poder tomar como base el modelo propuesto.

Por otra parte, López (2017) elaboró un artículo para la revista Electrónica sobre Tecnología, Educación y Sociedad, titulado: Propuesta de un sistema de gobierno, riesgos y cumplimiento para ser alineado a distintas normativas y regulaciones en pequeñas y medianas empresas, el cual tuvo como objetivo la implementación de la Gobernabilidad, Riesgos y Cumplimiento (GRC). Teóricamente basado en Anderson (2009), Tarantino (2008), ISO31000, entre otros.

En el documento se revisan distintas herramientas que existen en el mercado y que permiten definir y dar seguimiento a esquemas de GRC, sin embargo, cada una tiene sus propias limitaciones, ventajas y desventajas, por lo que se decidió la creación de una ontología propia y el uso del Semantic Web Builder (SWB) para su uso diario.

Se concluye, que es necesaria la creación de una ontología adecuada a las necesidades de cada organización, que permita documentar, dar seguimiento y visualizar el esquema de Gobernabilidad, Riesgos y Cumplimiento de la organización.

2.2. Marco conceptual

2.2.1. (GRC) Gobierno, Riesgo y Cumplimiento

De acuerdo al criterio del Grupo Abierto de Cumplimiento y Ética (OCEG) (2015, como se citó en Celada et al. 2016) “es un modelo de capacidad que permite a una organización lograr los objetivos abordando la incertidumbre y actuando con integridad” (pág. 15). Al respecto, Pareja (2022), señala: “permite cumplir los objetivos, reducir la incertidumbre, optimizar los recursos, las capacidades de los equipos; así como alinear, ejecutar y examinar constantemente a la organización, facilitando la cooperación, coordinación y colaboración entre los diferentes equipos de la organización”. (pág. 6).

Por otra parte, Vázquez (2015, como se citó en Guzmán et al. 2017) “es una capacidad de la organización para potenciar el ahorro de los costos, la optimización operativa, el mejoramiento continuo, la eficiente gestión de riesgos y controles, al igual que la gestión integrada del desempeño con fuertes niveles de aseguramiento” (pág. 48).

2.2.1.1. Gobernabilidad

En opinión de López et al. (2017) “Para realizar un análisis de las deficiencias, se involucran tres áreas de la toma de decisiones: quién está gobernando, quién está siendo gobernado, y qué recursos o activos han de ser desplegados en el proceso”. (pág. 7). Al respecto, Guzmán et al. (2017) indican:

> tiene como propósito crear el mayor grado de coordinación entre la relación de la junta directiva, consejo de administración, accionistas y partes interesadas en cuanto a la actividad económica se refiere, creando una base sólida bajo una estructura que sirva como soporte a la hora de la toma de decisiones y así potencializar su competitividad como organización. (pág. 28).

2.1.1.2. Riesgo

Para Celada et al. (2016) es de suma relevancia, generar una lista de los eventos que pueden generar, incrementar, apresurar o retardar el logro de los objetivos de la compañía. Con tal fin se debe considerar si los riesgos son generados interna o externamente, así como los resultados colaterales que puedan producir los mismos”. (pág. 59). En opinión de Guzmán et al. (2017) El riesgo “La gestión de riesgos como pilar para la toma de decisiones debe estar soportada en la planificación de procesos relacionados, siempre con un enfoque prospectivo, que permita disminuir la probabilidad y el impacto de eventos negativos para la compañía y partes interesadas.”. (pág. 34).

Por su lado, Celada et al. (2016) infieren:

> La gestión de riesgos como pilar para la toma de decisiones debe estar soportada en la planificación de procesos relacionados, siempre con un enfoque prospectivo, que permita disminuir la probabilidad y el impacto de eventos negativos para la compañía y partes interesadas. (pág. 58)

2.1.1.3. Cumplimiento

De acuerdo al criterio de Guzmán et al. (2017) El Cumplimiento es el resultado de que una organización cumpla con sus obligaciones nacionales e internacionales, así como también normas, reglamentos, políticas y procedimientos internos de la institucional. (pág. 43). Al respecto, López et al. (2017) exponen: es “el actuar en conformidad o de acuerdo a las leyes, regulaciones, protocolos o estándares establecidos”. (pág. 10).

Tecnologías de la información y comunicaciones como herramientas para la Gestión de GRC (Gobierno, riesgo, y cumplimiento

De acuerdo al criterio de López et al. (2017), todos los sistemas necesarios para medir el control de procedimientos en las organizaciones deben estar bien documentados para garantizar su eficacia, por lo cual, es un reto para las empresas el tener que adaptar los sistemas tecnológicos las necesidades existentes, de acuerdo al ramo al que se dediquen y el entorno en el que se desenvuelven, así como poder alcanzar los estándares establecidos. En este sentido, los mecanismos para monitorear el control y la forma para medir su eficacia deben estar documentados.

De acuerdo al criterio un Palao (2010, como se citó en Muñoz & Ulloa, 2011) un sistema de GRC (Gobierno, riesgo, y cumplimiento) enfocado a la administración de tecnologías de la información y comunicaciones: "integra e institucionaliza las buenas prácticas para garantizar que TI en la empresa soporta los objetivos del negocio. Facilita que la empresa aproveche al máximo su información, maximiza los beneficios, capitaliza las oportunidades y gana ventajas competitivas". (pág. 29)

Actualmente existen en el mercado aplicaciones automatizadas que permiten el cumplimiento con alguno de estos estándares, sin embargo, Seguidamente, se demuestra un análisis de las herramientas existentes en el mercado de acuerdo a (López et al. 2017) que ayudan a la administración de un sistema de gestión de GRC (Gobierno, riesgo, y cumplimiento):

Tabla 1. Análisis de las aplicaciones de GRC (Gobierno, riesgo, y cumplimiento):

Herramienta / Sitio	Descripción
SecureGRC https://www.egestalt.com/securegrc-ent.html	Solución integral de monitoreo de seguridad de TI y gestión de cumplimiento que simplifica y reduce el tiempo necesario para la vigilancia de la seguridad, el cumplimiento normativo y el proceso de certificación
ORCA GRC Suite http://www.gcpglobal.com/orca- descripción.php	La diversidad de soluciones en prevención de riesgos que ofrece ORCA y el respaldo de expertos multidisciplinarios para la entrega de servicios consultivos le permite diferenciarse de la mayoría de sus competidores dando como resultado la optimización operativa, la reducción de costos y la simplificación de las operaciones, así como el mejoramiento de la visibilidad y la toma de decisiones para propiciar un Gobierno Corporativo

SoftExpert GRC Suite http://www.softexpert .es/gestión-gobierno-riesgos-reglamentaciones.php	más eficiente. Ofrece una estructura de gobernanza que posibilita una tomada de decisión eficaz y cambios comportamentales. Ofrece a la organización una implementación viable y eficiente de la gobernanza corporativa y de TI.
ARIS Risk & Compliance Manager http://www.softwarea g.com/corporate/solutions/ebpm/grc/overview/default.asp	Software para mejorar la gestión de riesgo del cumplimiento.

Fuente: López et al (2017, pág. 13)

2.3. Marco legal

Constitución Política de Colombia: Por medio de la cual se promulga el marco jurídico, democrático y participativo que garantiza el orden político, económico y social justo, así como el compromiso a impulsar la integración de la comunidad latinoamericana.

Decreto 612 de 2018: Por el cual se fijan las directrices para la integración de los planes institucionales y estratégicos al plan de acción por parte de las entidades del estado.

Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Ley 527 de 1999: Por la cual se define y regula el uso de los mensajes de texto, comercio electrónico y firmas digitales.

Ley 1341 de 2009: Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

Ley Estatutaria 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.

Decreto 025 de 2014: Por el cual se modifica la estructura orgánica y se establece la organización y funcionamiento de la Defensoría del Pueblo.

Decreto 2573 de 2014: Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

Decreto 943 de 2014: Modelo Estándar de Control Interno (MECÍ)

Resolución 1014 de 2013: Por la cual se adopta el Plan Estratégico de la Defensoría del Pueblo para la vigencia 2013-2016.

Resolución 1296 de 2014: Manual de Supervisión e Interventoría de la Defensoría del Pueblo.

Norma NTC ISO 9001: Sistemas de Gestión de la Calidad.

Norma NTCGP 1000:2009: Norma Técnica de Calidad en la Gestión Pública – ICONTEC.

Norma NTC-ISO-IEC 27001: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos.

Norma NTC-ISO-IEC 27002: Tecnología de la información. Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información.

3. METODOLOGÍA

3.1. Enfoque y alcance de la investigación

El presente estudio se encuentra inmerso dentro del paradigma mixto, el cual de acuerdo con el criterio de Hernández et al. (2016) es cuando “se recolectan y analizan datos cuantitativos y cualitativos y la interpretación es producto de toda la información en su conjunto. (pág. 534). Al respecto, (Ruiz, 2011) “recolecta, analiza y vincula datos cuantitativos y cualitativos en un mismo estudio o una serie de investigaciones para responder a un planteamiento”. (pág. 159). El presente estudio se considera de enfoque mixto, ya que se utilizaron técnicas cualitativas, como la entrevista y una encuesta que será analizada de forma cuantitativa.

Es de hacer notar, que el tipo es descriptivo, según Arias (2016) “consiste en la caracterización de un hecho, fenómeno, individuo o grupo, con el fin de establecer su estructura o comportamiento” (pág. 24). En cuanto al diseño de investigación es no experimental, el cual de acuerdo al criterio de Bonilla (2011) “está exenta del ejercicio del control y manipulación de las variables en estudio. Es decir, los hechos o fenómenos son estudiados en su ambiente natural, tal y como se manifiestan” (pág. 54). El estudio se considera de diseño no experimental ya que no se manipularon las situaciones, sino que se presentaron tal como se desarrollaron.

Asimismo, se encuentra inmerso en un diseño de campo, el cual según Cabezas et al. (2018) “se realiza en el mismo lugar geográfico donde se desarrollan los hechos” (pág. 74). Al respecto, Bavaresco (2013) “se realiza en el propio sitio donde se encuentra el objeto de estudio. Ello permite el conocimiento más a fondo del problema por parte del investigador y puede manejar los datos con más seguridad” (pág. 28). En este sentido, la presente investigación se considera de campo, ya que la información fue recolectada en la Defensoría del Pueblo de Bogotá, D.C.

3.2. Población y muestra

3.2.1. Definición de la población

La población estuvo conformada por los (6) empleados del departamento de tecnología de la información de la Defensoría del Pueblo de Colombia sede Bogotá v como informante clave, el jefe de seguridad de información de la entidad.

3.2.2. Instrumento(s)

Como instrumentos para abordar el ámbito cualitativo, se utilizó una entrevista estructurada dirigida al jefe de seguridad de la información de la entidad objeto de estudio, contentiva de tres preguntas abiertas, mediante las cuales expreso sus opiniones y experiencias sobre Gobierno, riesgo, y cumplimiento, en un clima cálido y empático, de forma tal que emitiera sus criterios de forma clara y precisa. (ver anexo A)

Aunado a ello, para la parte cuantitativa se aplicó un cuestionario tipo encuesta contentivo de ocho (8) ítems cerrados con opciones múltiples, dirigidos a seis (6) colaboradores de la organización quienes emitieron desde su punto de vista el estado actual del Gobierno, riesgo, y cumplimiento. (ver anexo B)

Es de hacer notar, que para medir los riesgos existentes se realizó una matriz identificación y evaluación de riesgos existentes en la Defensoría del pueblo de Bogotá, D.C. (ver Tabla 14. matriz de identificación y valoración de riesgos)

3.3. Descripción de procedimientos

Para dar cumplimiento a los objetivos específicos se llevó a cabo el siguiente procedimiento: en el objetivo 1 dirigidos a diagnosticar el alcance que tienen los recursos, riesgos de TIC y la aplicación de los estándares de gestión TIC en la Defensoría del Pueblo de Bogotá, D.C., estableciendo las falencias existentes, se elaboró un diagnóstico: Este diagnóstico estará dividido en tres etapas:

- Etapa 1: Entrevista con el jefe de seguridad de la información de la entidad (defensoría del pueblo): en esta fase se obtuvo un panorama claro y verídico del estado actual de la organización, basándonos en su política de seguridad e informes internos y externos.

- Etapa 2: se aplicó el cuestionario tipo encuesta a los colaboradores de la institución que permitan desde su punto de vista el estado actual del Gobierno, riesgo, y cumplimiento.

- Etapa 3: en esta etapa se realizó el análisis de resultado armando un plan de trabajo que permitirá entregar a la organización un resultado global del estado actual de estos tres componentes (gobierno, riesgo y cumplimiento,)

Seguidamente, en el objetivo 2 relativo a identificar los componentes que hacen parte del modelo de GRC (Gobierno, riesgo, y cumplimiento), enfocado a la administración de tecnologías de la información y comunicaciones, para mejorar los procesos de la Defensoría del Pueblo de Bogotá, D.C, inicialmente se identificaron los componentes del modelo y cómo podemos aplicarlos para dar un diagnóstico, luego se realizó la identificación y evaluación de riesgos.

En cuanto al objetivo 3, referido a proponer un modelo de GRC (Gobierno, riesgo, y cumplimiento) enfocado a la administración de tecnologías de la información y comunicaciones para optimizar los procesos de la Defensoría del Pueblo de Bogotá, D.C., Esta fase contempla la elaboración y presentación del informe final, en el cual se consolidan los resultados de análisis de vulnerabilidades y ejecución de Hardening, en donde se le permite a la defensoría conocer el estado final de la evaluación de seguridad técnica e implementación de Hardening sobre la infraestructura.

3.4. Análisis de información

Por tratarse de un estudio mixto se utilizarán técnicas cualitativas y cuantitativas, en este sentido, la entrevista se analizó de manera cualitativa, presentada en tablas y una estructura consciente significativa conceptual mientras, que para la encuesta e utilizó la estadística descriptiva, específicamente frecuencias absolutas y descriptivas, representadas en gráficos y tablas sinópticas de doble entrada.

3.5. Consideraciones éticas

Para evitar invadir la privacidad es importante que el equipo de investigación se acerque a los informantes clave de forma respetuosa, teniendo en cuenta los valores y problemáticas particulares de cada grupo. Es imprescindible que a través de las preguntas formuladas no se indague más allá del límite moral o cultural impuesto por la persona entrevistada o por su grupo de pertenencia. Para ello, y como parte de la preparación de la investigación, las y los investigadores deben interiorizarse en la cultura y valores propios de las personas que van a entrevistar. Esto minimizará la invasión de la privacidad de las personas estudiadas. A su vez, se les debe sobre el alcance de la protección de la confidencialidad que puede ser asegurada en cada investigación.

Se les notificará a la muestra y el informante clave, que el uso de la información es meramente investigativo, asimismo, serán tratados con respeto y empatía, garantizándoles la confidencialidad de la información aportada.

3.6. Instrumentos de aceptación y autorización

Se procedió a comunicarse telefónicamente con participantes a las instituciones en estudio, de forma tal que aceptarán la aplicación de los instrumentos, coordinando de acuerdo a sus actividades el momento ideal para aplicarlos.

4. HIPÓTESIS

4.1. Las variables

4.1.1. Variable(s) independiente(s)

La variable independiente del presente estudio es tecnologías de la información y comunicaciones (Tic), la cual de acuerdo al artículo 6 denle Ley 1341 de 2009. “son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes”.

4.1.2. Variable(s) dependiente (s)

Modelo de GRC (Gobierno, riesgo, y cumplimiento), definida por e acuerdo al criterio del Grupo Abierto de Cumplimiento y Ética (OCEG) (2015, como se citó en Celada et al. 2016) “es un modelo de capacidad que permite a una organización lograr los objetivos abordando la incertidumbre y actuando con integridad” (pág. 15).

4.2. Planteamiento de la hipótesis

Los datos que soportan el modelo de GRC (Gobierno, riesgo, y cumplimiento) residen en aplicaciones tecnológicas y su incorporación permite transformar los datos de una información poderosa a la toma de decisiones y al monitoreo de su comportamiento a través de indicadores de riesgos, GRC no es solo tecnología de información

5. RESULTADOS

5.1. Análisis de la entrevista

Tabla 2. Entrevista

Modelo de GRC (Gobierno, riesgo, y cumplimiento) enfocado a la administración de tecnologías de la información y comunicaciones para mejorar los procesos empresariales de la Defensoría del Pueblo de Bogotá, D.C				
Día: 15	**Mes: 11**	**Año: 2023**	**Hora: 2:00**	**Entrevista en audio Duración: 3 minutos 59 segundos**

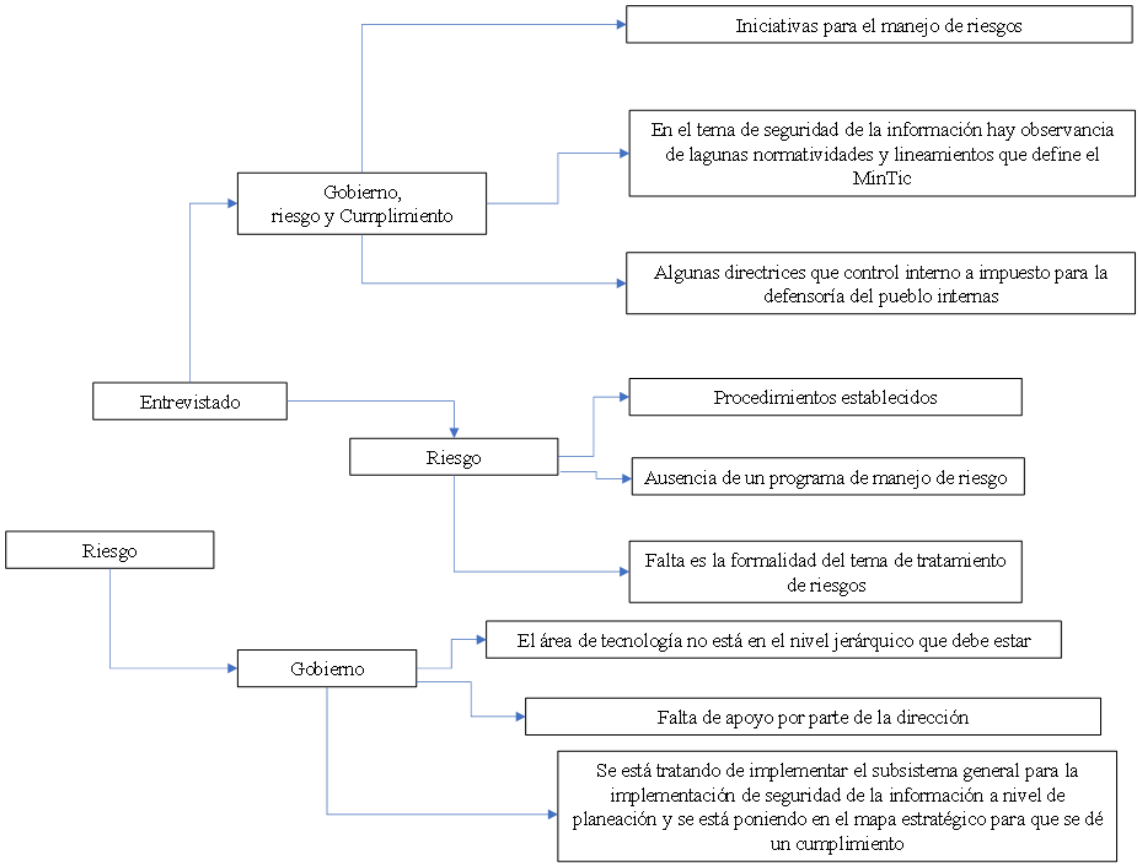
Escenario: Instalaciones de la Defensoría del Pueblo de Bogotá, D.C
Informante: Orlando Burgos Triana jefe de seguridad de la Defensoría del Pueblo de Bogotá, D.C

	Código	Texto de la entrevista
1		**1. ¿Que nos puede contar sobre gobierno, riesgo y**
2		**cumplimiento en la defensoría del pueblo?**
3		La defensoría del pueblo hace aproximadamente hace 3 años ha
4	**Gobierno,**	implementado unas iniciativas para el manejo de riesgos de acuerdo
5	**riesgo y**	a unas normas internacionales, incluyendo la ISO 27001 en el tema
6	**cumplimiento**	de seguridad de la información y haciendo observancia de lagunas
7		normatividades y lineamientos que define el Min Tic y algunas
8		directrices que control interno a impuesto para la defensoría del
9		pueblo internas.
10		**2. ¿En cuanto a riesgo como están blindados?**
11		Hay muchas iniciativas para el tema de riesgo que se manejan como
12		de manera no formal, hay procedimientos establecidos, pero no hay
13		como tal un programa de manejo de riesgo, ni un modelo especifico,
14	**Riesgo**	en curso hay una contratación para definir un modelo de riesgos y
15		un modelo de tratamiento de riesgos.
16		Están en riesgo, no se está al 100% en cuanto al manejo de riesgos.
17		Si, históricamente no se ha materializado ningún riesgo referente a
18		seguridad de la información, ni perdida de datos, ni perdida de
19		disponibilidad, pero si falta es la formalidad del tema de tratamiento
20		de riesgos, pueden existir procedimientos, pueden existir
21		instructivos, pueden existir tareas que ejecuten los funcionarios del
22		área de tecnología en cuanto al manejo de riesgo, pero la formalidad
23		no se ha dado.
24		3. **En cuanto gobierno como detecta la entidad**
25		El tema de gobierno es complicado en el área de tecnología, cuando
26		el área de tecnología no está en el nivel jerárquico que debe estar,
27		si usted coloca un área de tecnología que no está siendo apoya por
28		la dirección que no está a nivel estratégico en la institución, 4
29		direcciones y más de 16 delegadas y siempre esporádicamente sale
30		alguna contratación en el tema de tecnología y conectiva en alguna
31		regional que sale de la esfera de control del área de tecnología y

Gobierno	con eso se va perdiendo un poco el tema de gobernabilidad que es muy importante para el área, para que se dé eso se han dado algunas iniciativas y Se está tratando de implementar el subsistema general para la implementación de seguridad de la información a nivel de planeación y se está poniendo en el mapa estratégico para que se dé un cumplimiento y el apoyo de la dirección que es lo más importante para que se dé el tema de gobierno.

Fuente: elaboración propia (2024)

Figura 2. Estructura consciente significativa conceptual entrevista



Fuente: Elaboración propia (2024)

Memorando de la Entrevista

De acuerdo a la información suministrada por jefe de seguridad de la Defensoría del Pueblo de Bogotá, D.C aproximadamente hace 3 años ha implementado unas iniciativas para el manejo de riesgos de, más no hay como tal un programa de manejo de riesgo, ni un modelo especifico, asimismo, indicó que no se ha materializado ningún riesgo referente a seguridad de

la información, ni perdida de datos, ni perdida de disponibilidad, pero si falta es la formalidad del tema de tratamiento de riesgos, pueden existir procedimientos, pueden existir instructivos, pueden existir tareas que ejecuten los funcionarios del área de tecnología en cuanto al manejo de riesgo, pero la formalidad no se ha dado.

Además, no existe el nivel jerárquico que debe estar, de la misma forma, expresó que el área de tecnología no está siendo apoya por la dirección. Se está tratando de implementar el subsistema general para la implementación de seguridad de la información a nivel de planeación y se está poniendo en el mapa estratégico para que se dé un cumplimiento y el apoyo de la dirección que es lo más importante para que se dé el tema de gobierno.

5.2. Análisis del instrumento

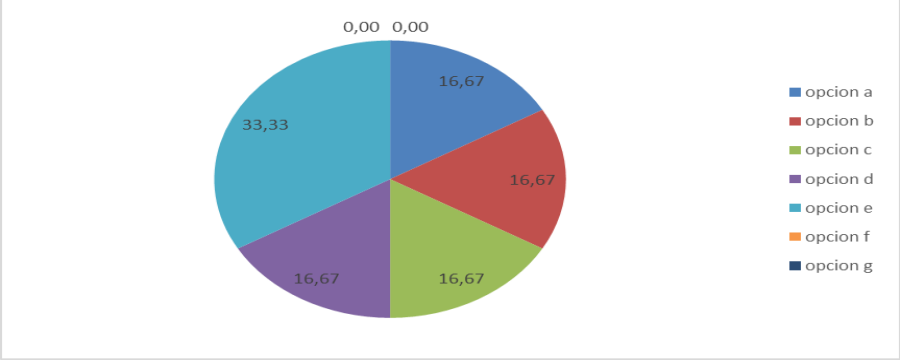
Ítems 1: ¿Usted cree que con la implementación de un modelo GRC se puede conseguir la automatización o mejora de los procesos? Seleccione que beneficios traería la implementación de este.

Tabla 3. Beneficios de la implementación de un modelo *GRC*

Pregunta	Respuestas	Fa	Fr
¿Usted cree que con la implementación de un modelo GRC se puede conseguir la automatización o mejora de los procesos? Seleccione que beneficios traería la implementación de este	opción a	1	16,67
	opción b	1	16,67
	opción c	1	16,67
	opción d	1	16,67
	opción e	2	33,33
	opción f	0	0,00
	opción g	0	0,00
	Total	6	100,00

Fuente: elaboración propia (2023)

Gráfico 1. Beneficios de la implementación de un modelo GRC



Fuente: Elaboración propia (2023)

De acuerdo con los resultados expuestos en la tabla 3 y el grafico 1, se evidencia que el 33,33 % de los encuestados expresó que mejora la atención de los usuarios, mientras que el 16,67 % indicaron que mejora los tiempos de respuesta, reduce los costos operacionales y mejora la satisfacción de los ciudadanos respectivamente.

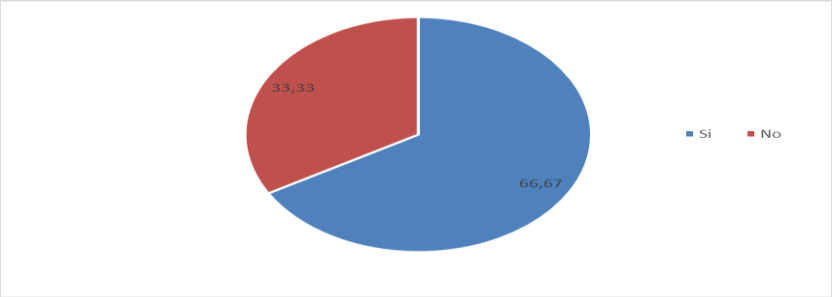
Ítems 2: ¿La entidad hace uso de tecnologías basadas en software libre o código abierto?

Tabla 4*. Tecnologías basadas en software libre o código abierto*

Pregunta	Respuestas	Fa	Fr
¿La entidad hace uso de tecnologías basadas en software libre o código abierto?	Si	4	66,67
	No	2	33,33
	Total	6	100,00

Fuente: Elaboración propia (2023)

Gráfico 2*. Tecnologías basadas en software libre o código abierto*



Fuente: Elaboración propia (2023)

Los resultados expuestos en la presente tabla y grafico reflejan que el 66,67 % de los encuestados indicaron que la entidad hace uso de tecnologías basadas en software libre o código abierto, mientras que 3,33 % indico la opción no

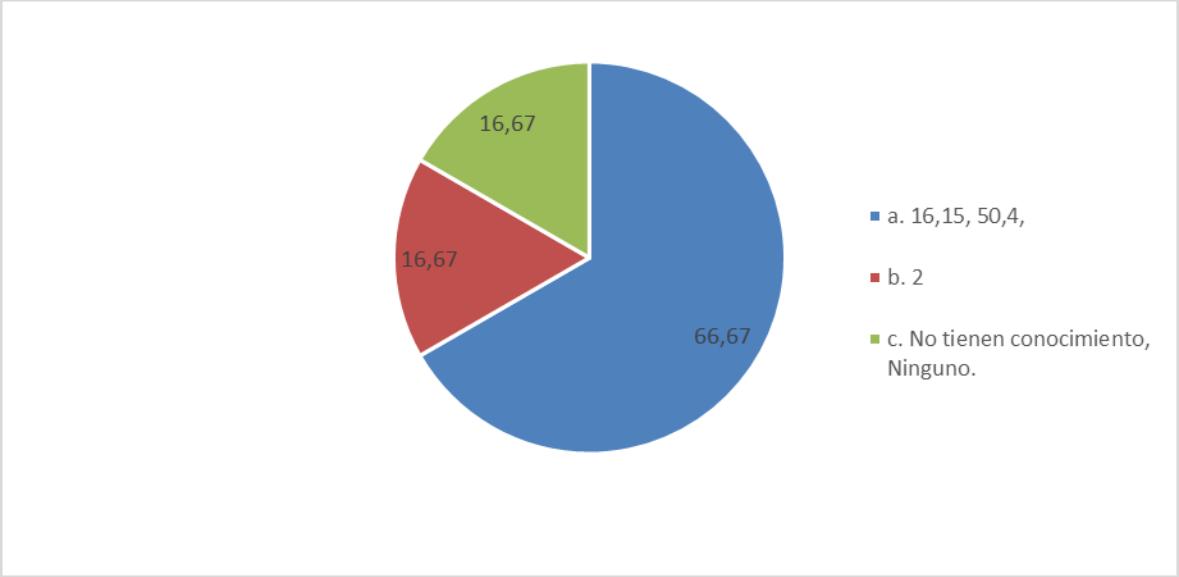
Ítems 3: Con respecto a los procesos de la entidad indique:

Tabla 5. Procesos de la entidad

Pregunta	Respuestas	Fa	Fr
Con respecto a los procesos de la entidad indique	a. 16,15, 50,4,	4	66,67
	b. 2	1	16,67
	c. No tienen conocimiento, Ninguno.	1	16,67
	Total	0	100,00

Fuente: Elaboración propia (2023)

Gráfico 3. ***Procesos de la entidad***



Fuente: Elaboración propia (2023)

Los resultados expuestos en la presente tabla y grafico demuestran que el 66,67 % de los encuestados expresaron que la entidad tiene 16, 15, 50 y 4 procesos, el 16,67% indicó que 2 procesos se han mejorado en el marco de referencia de la arquitectura empresarial y que no tienen conocimiento de mejora de procesos según lo establecido en el modelo de seguridad de la información respectivamente.

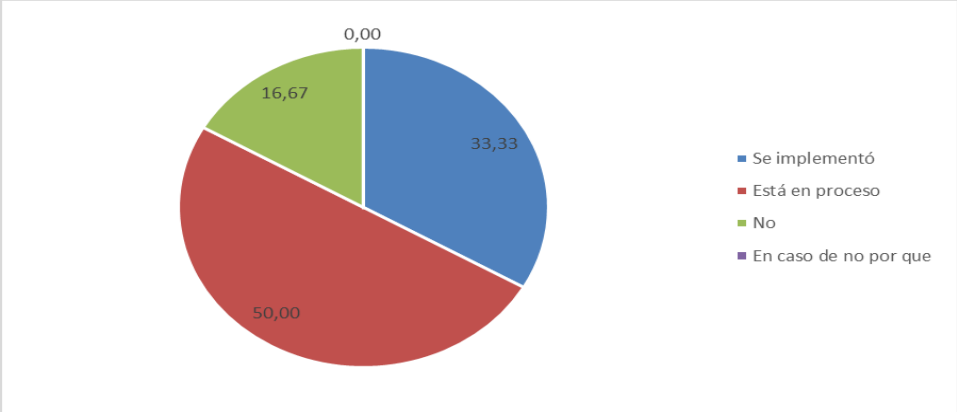
Ítems 4: ¿Su entidad implementó un plan de la seguridad de la información?

Tabla 6. ***Plan de la seguridad de la información***

Preguntas	Respuestas	Fa	Fr
¿Su entidad implementó un plan de la seguridad de la información?	Se implementó	2	33,33
	Está en proceso	3	50,00
	No	1	16,67
	En caso de no por que	0	0,00
	Total	6	100, 00

Fuente: Elaboración propia (2023)

Gráfico 4. ***Plan de la seguridad de la información***



Fuente: elaboración propia (2023)

En la presente tabla y grafico se evidencia que el 50,00 % de los encuestados expresaron que la entidad está en proceso de implementación de un plan de la seguridad de la información. Mientras 33,33 % expresó si se implementó y el 16,67 % opina que no.

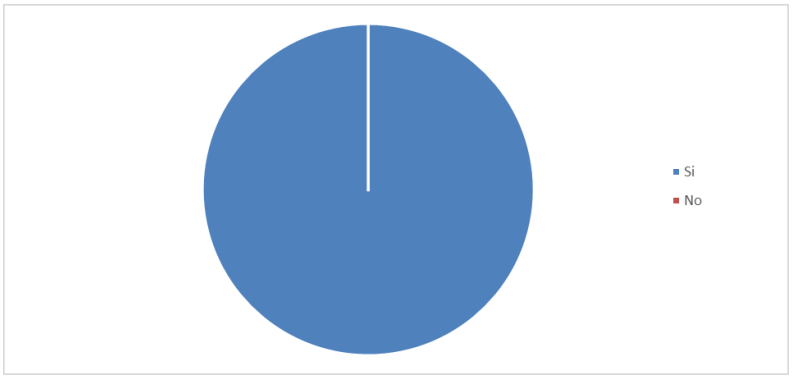
Ítems 5: De acuerdo con su conocimiento ¿usted cree que la entidad necesita la implementación de modelo de GRC?

Tabla 7. ***Necesidad de implementación de un modelo de GRC***

Pregunta	Respuestas	Fa	Fr
De acuerdo con su conocimiento ¿usted cree que la entidad necesita la implementación de modelo de GRC?	Si	6	100,00
	No	0	0,00
	Total	6	100,00

Fuente: elaboración propia (2023)

Gráfico 5. ***Necesidad de implementación de un modelo de GRC***



Fuente: elaboración propia (2023)

En la presente tabla se evidencia que el 100 % de los encuestados expresaron que la entidad necesita la implementación de modelo de GRC

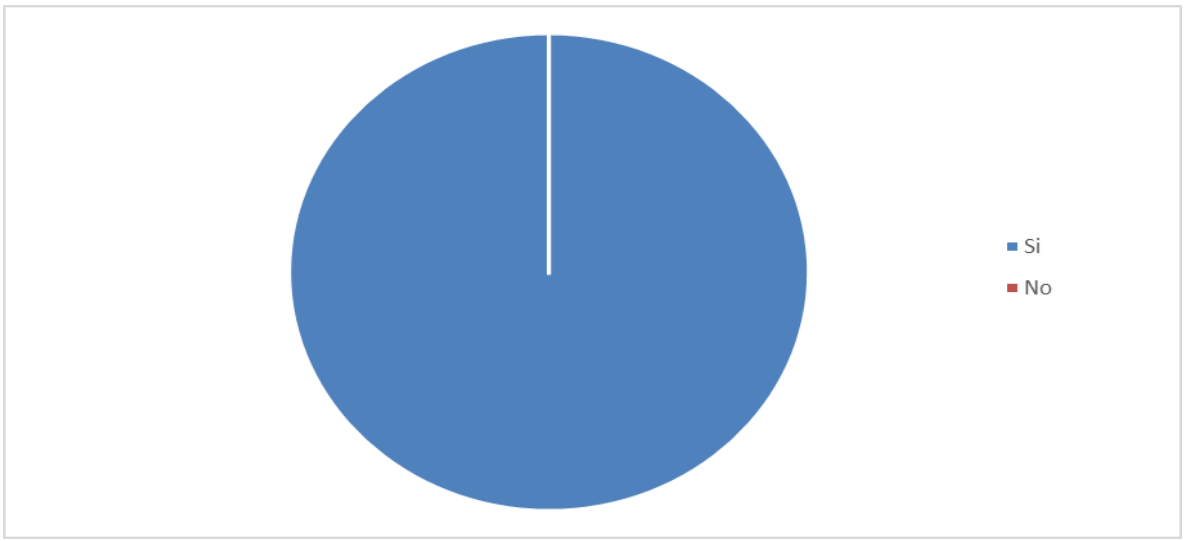
Ítems 6: ¿Usted cree que con la implementación de un modelo GRC mejorarían los procesos que tiene la entidad en cada una de sus áreas o correspondencias?

Tabla 8. Mejora de procesos con la implementación de un modelo GRC

Pregunta	Respuestas	Fa	Fr
¿Usted cree que con la implementación de un modelo GRC mejorarían los procesos que tiene la entidad en cada una de sus áreas o correspondencias?	Si	6	100,00
	No	0	0,00
	Total	6	100,00

Fuente: elaboración propia (2023)

Gráfico 6. Mejora de procesos con la implementación de un modelo GRC



Fuente: Elaboración propia (2023)

En la presente tabla se observa que el 100 % de las unidades informantes señalan que con la implementación de un modelo GRC mejorarían los procesos que tiene la entidad en cada una de sus áreas o correspondencias

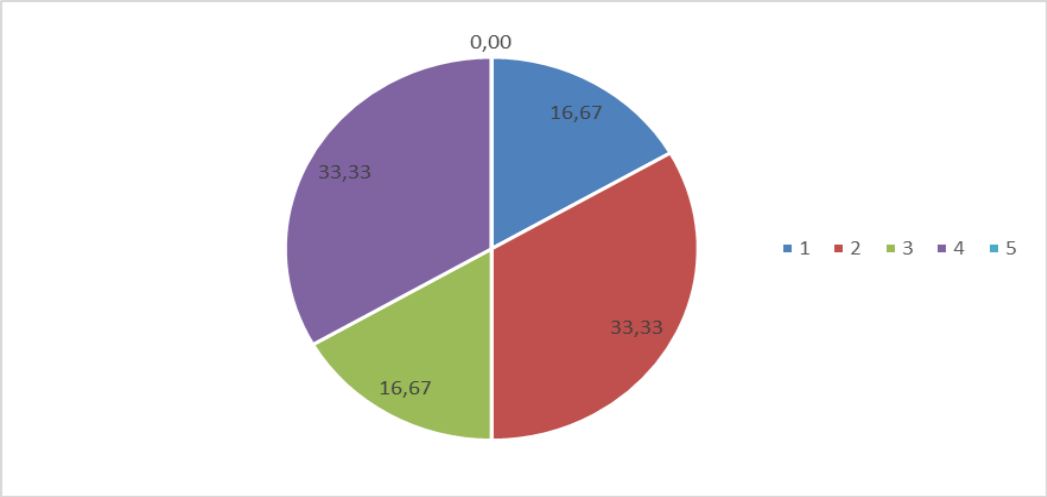
Ítems 7: ¿Usted cree que la entidad está haciendo buen uso de los recursos tecnológicos en cada una de sus áreas? Califique del 1 al 5, donde 1 es la más baja y 5 la más alta.

Tabla 9*. Uso de los recursos tecnológicos*

Pregunta	Respuestas	Fa	Fr
¿Usted cree que la entidad está haciendo buen uso de los recursos tecnológicos en cada una de sus áreas? Califique del 1 al 5, donde 1 es la más baja y 5 la más alta.	1	1	16,67
	2	2	33,33
	3	1	16,67
	4	2	33,33
	5	0	0,00
	Total	6	100,00

Fuente: Elaboración propia (2023)

Gráfico 7. Uso de los recursos tecnológicos



Fuente: Elaboración propia (2023)

En la presente tabla y gráfico, se evidencia que el 33,33 % de los encuestados seleccionaron la opción 2 y 4 respectivamente, mientras que el 16,67% indico las opciones 1 y 3 respectivamente.

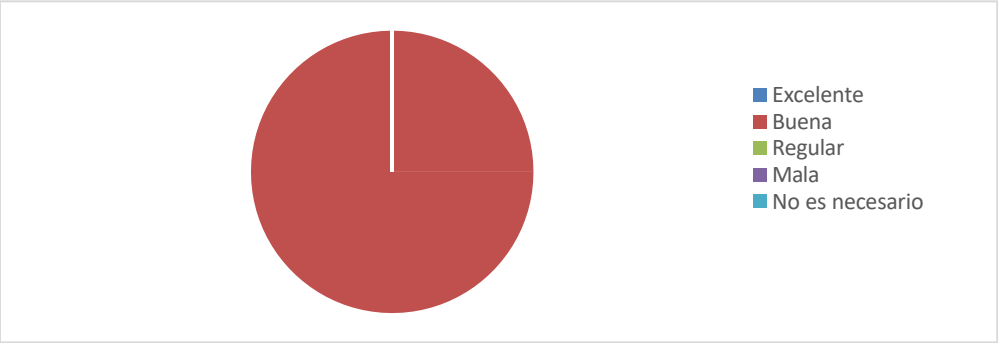
Ítems 8. ¿Cómo considera usted la aplicación de esta encuesta?

Tabla 10*. Aplicación de la encuesta*

Pregunta	Respuestas	Fa	Fr
¿Cómo considera usted la aplicación de esta encuesta?	Excelente	0	0,00
	Buena	6	100,00
	Regular	0	0,00
	Mala	0	0,00
	No es necesario	0	0,00
	Total	6	100,00

Fuente: Elaboración propia (2023)

Gráfico 8. Aplicación de la encuesta



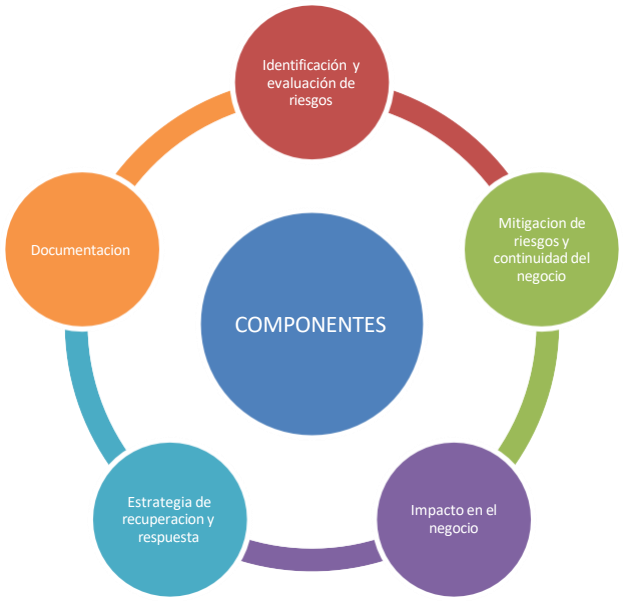
Fuente: Elaboración propia (2023)

Los resultados expuestos en la presente tabla y grafico reflejan que el 100 % de los encuestados indicaron que les parece buena la aplicación de esta encuesta.

5.3. Identificación y valoración de riesgos

Inicialmente se identificaron los componentes del modelo para determinar de que forma se integraran para desarrollar el modelo de GRC que se espera proponer, tal como se refleja en la figura siguiente:

***Gráfico 9. Componentes Modelo GRC para la defensoría del pueblo de* Bogotá, D.C**



Fuente: Elaboración propia (2023) basado en (MINTIC, 2019)

5.4. Identificación y evaluación de riesgos

Para identificar y evaluar los riesgos existentes, se tomaron en consideración los cinco activo más críticos, de acuerdo con el análisis GAP de la defensoría y los resultados de la entrevista al jefe de seguridad de la institución, elaborando una matriz de identificación y valoración de riesgos, la cual se basó en los siguientes criterios:

Tabla 11. Categorización de la probabilidad

Valor	Nivel	Descripción	Frecuencia
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales y/o la eficacia de los controles es alta.	No se ha presentado en los últimos 5 años
2	Improbable	El evento puede ocurrir en algún momento y/o la eficacia de los controles es moderada.	Al menos una vez en los últimos 5 años
3	Posible	El evento podría ocurrir en algún momento y/o la eficacia de los controles es baja.	Al menos una vez en los últimos 2 años
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias y/o la eficacia de los controles es nula.	Al menos una vez en el último año
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias y/o no existen controles o si existen es nula su eficacia.	Más de una vez al año

Fuente: Elaboración propia (2023)

Tabla 12. Categorización impacto

Valor	Nivel	Descripción
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la organizacion y/o la eficacia de los controles es alta.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la organizacion y/o la eficacia de los controles es moderada.
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la organizacion y/o la eficacia de los controles es baja.

4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la organizacion y/o la eficacia de los controles es nula.
5	Crítico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la organizacion y/o no existen controles o si existen es nula su eficacia.

Fuente: Elaboración propia (2023)

Tabla 13. Categorización del análisis y evaluación de los controles

Valor cuantitativo	**Valor cualitativo**	**Descripción**
5	Alta	El control es efectivo porque ha permitido el total cumplimiento del objetivo para el cual fue diseñado. Es un control documentado, se hace seguimiento y tiene responsables y recursos definidos para su implementación.
4	Moderada	El control es efectivo porque cumple el objetivo aunque no en su totalidad. Es un control documentado, se hace seguimiento y tiene responsables y recursos definidos para su implementación.
3	Baja	El control es poco efectivo porque no ha sido útil para dar cumplimiento al objetivo por el cual fue diseñado. Es un control no documentado, aunque tiene definidos seguimiento, responsables y recursos para su implementación.
2	Nula	El control no es efectivo porque no ha sido útil para dar cumplimiento al objetivo por el cual fue diseñado. Es un control no documentado, no se hace seguimiento, no tiene responsables, ni recursos definidos para su implementación.
1	No existen controles	----------

Fuente: Elaboración propia (2023)

A Continuación, basado en los valores de las tablas de categorización anteriormente expuestas, el análisis GAP de la defensoría y los resultados de la entrevista al jefe de seguridad de la institución se presentan la matriz de identificación y valoración de riesgos:

Tabla 14. matriz de identificación y valoración de riesgos

ETAPA I											ETAPA II			ETAPA III			
IDENTIFICACIÓN DEL RIESGO							RIESGO PURO				DESCRIPCION Y CALIFICACION DE LOS CONTROLES EXISTENTES PARA MITIGAR LOS RIESGOS			ANALISIS Y VALORACION DEL RIESGO CON CONTROLES			
												Controles		RIESGO RESIDUAL			
No.	Activo	Amenaza	Vulnerabilidad	Riesgo	No.	Efectos	IMPACTO	PROBABILIDAD	TOTAL	No	Descripción del control	Efecto del control		PROBABILIDAD		IMPACTO	
												Disminuye Probabilidad	Disminuye Impacto	Valor	Nivel	Valor	Nivel
1	Informes de Riesgo de vulneración de DH e infracciones al DIH(Sistema de Alertas tempranas)	Perdida de información	Debilidad en la seguridad de la información	Divulgacion de información sensible	R1	Robo de información clasificada	5	5	10	C1	Fortalecer el sistema de seguridad	X		3	Posible	5	Critico
2	Perdida, filtración y manipulación de información sensible.	Exposicion de información confidencial y de uso interno	Desconocimiento e imcumplimiento de los lineamientos de seguridad de la información	Perdida de confidencialidad de los sistemas de información	R2	Apropiación de información confidencial	4	5	9	C2	Capacitar a los funcionarios en la política de privacidad y seguridad de la información.	X		3	Posible	5	Critico
3	Informes de seguridad informática y monitoreo de recursos (Area de TI)	Incorrecta parametrización de los permisos sobre la información de los informes.	Administracion inadecuada de documentos sensibles.	Perdida de confidencialidad de la documentación.	R3	Publicación de información sencible o reservada de la entidad o daño jurídico.	4	5	9	C3	Clausula de confidencialidad de la información al personal y restrinción de acceso a la documentación sencible.	X		3	Posible	5	Critico
4	Base de datos de victimas de conflicto armado (Area victimas)	Incorrecta administación de los datos.	Manipulación inadecuada de los datos sencibles de las victimas.	Perdida de integridad	R4	Publicación de información privada.	4	5	9	C4	Supervisar toda las actividades de acceso a la base de datos y automatizar la auditoria con una plataforma especializada y protección de base de datos.	X		3	Posible	5	Critico
5	Sistema interinstitucional de justicia transicional. (Defen-Min justicia)	Falla en el funcionamiento del sistema.	Error que genere perdida de datos.	Manipulación inadecuada de la información por personas externas.	R5	Divulgación de la información por personas externas.	4	5	9	C5	Generar un plan de Backup y clausula de confidencialidad de la información.	X		3	Posible	5	Critico

Fuente: Elaboración propia (2023)

La evaluación de riesgos es de alta relevancia en las entidades y con el fin de que se tomen las mejores decisiones se recomienda para obtener un resultado favorable se tomen inicialmente. Los riesgos ya identificados y de alto impacto dentro de la organización en este componente debemos evaluar e identificar cada uno de ellos en la defensoría del pueblo para lograr los objetivos propuestos dentro del modelo en marco de su salida a producción en un futuro validando el resultado que arroje la consultoría.

Dentro de nuestro modelo GRC se debe abarcar si bien principalmente los riesgos de alto impacto, también se deben tener en cuenta todos los riesgos que se pueden presentar dentro de la organización, y con ello establecer las estrategias que permitan mitigar y enfrentar estos riesgos y dar continuidad al negocio

5.5. Identificación de riesgos

Su objetivo conocer los riesgos, sus principales causas teniendo como fuente fundamental los factores internos y/o externos y sus resultados. Para la identificación de los riesgos se realizan las siguientes actividades:

• Reuniones de trabajo con los líderes de los procesos y/o coordinadores de grupo área o su designado. (VER ANEXO D)

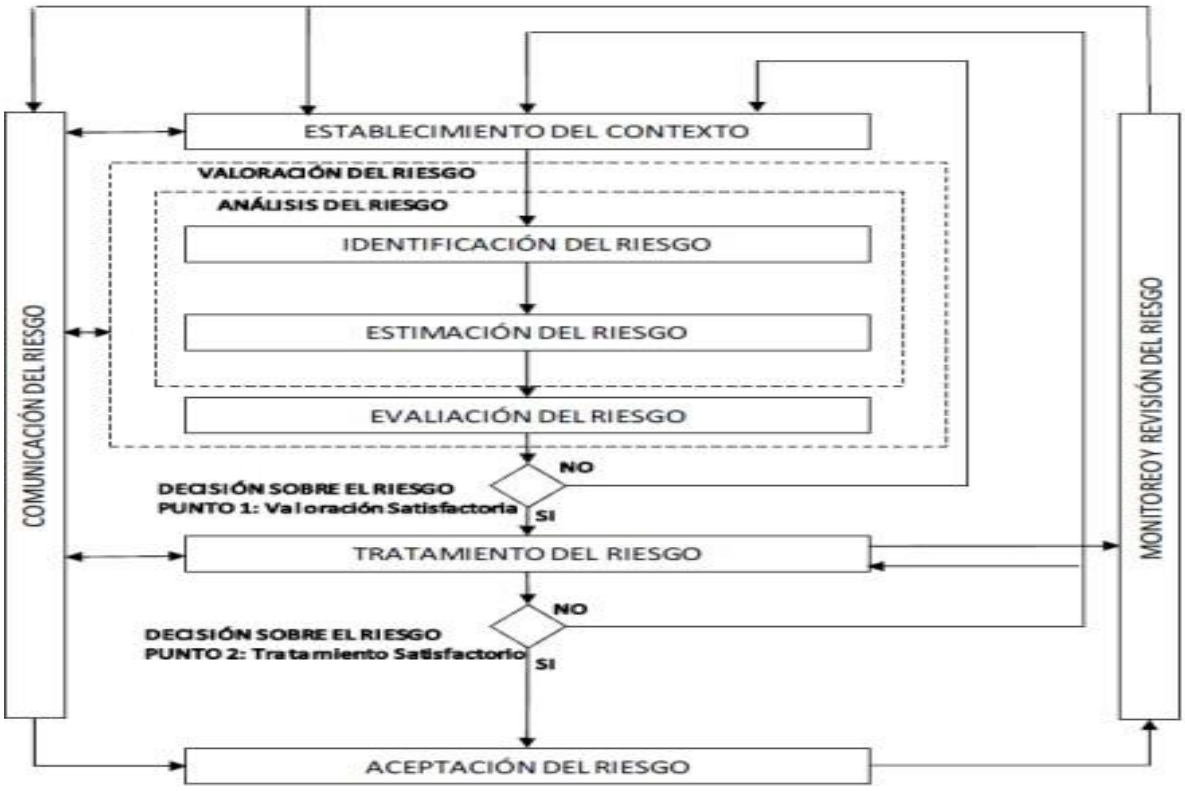
• Identificar y escribir los posibles hechos o amenazas de seguridad, de estos se estimarán las correcciones y procedimientos que permitan la operación natural del proceso.

• Determinar las causas internas y externas, aplicando metodología de análisis causal como las que se mencionan a continuación con el fin de establecer el origen del riesgo.

• Definir los posibles efectos o consecuencias de materializase los riesgos de seguridad y privacidad (Lo que podría ocasionar).

5.6. Monitoria de procesos de gestión

Figura 3. Monitoria de procesos de gestión



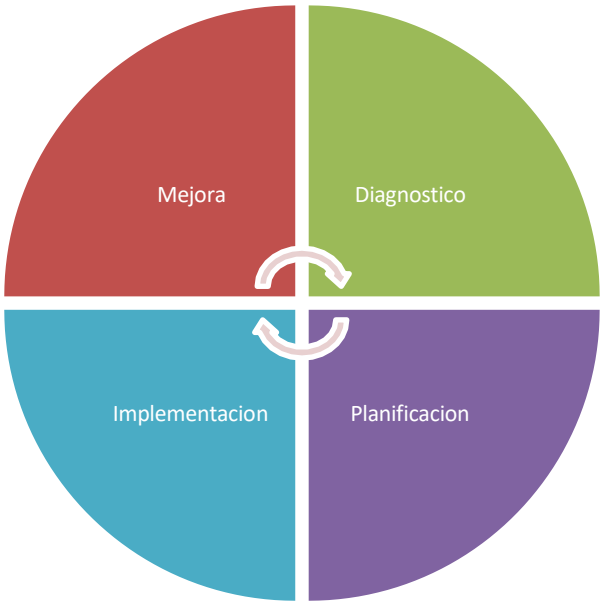
Fuente: NTC-ISO31000 (pág. 17)

5.7. Mitigación de riesgos y continuidad del negocio

Se tiene como producto final, al estructurar el plan mitigación de riesgos, para los diferentes procesos de la Defensoría del Pueblo, haciendo un diagnóstico de los recursos con los que encuentra actualmente la organización, validando los diferentes métodos para la continuidad del negocio.

5.8. Continuidad del negocio

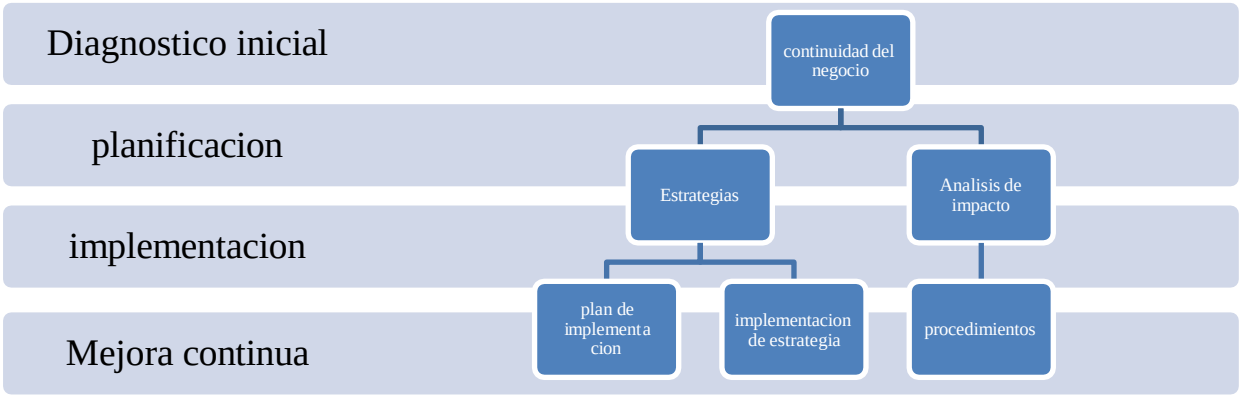
Gráfico 10. Marco de seguridad y privacidad de la información



Fuente: MINTIC (2019)

Seguidamente, se presenta las fases a tener en cuenta para dar continuidad a los procesos de la defensoría del pueblo de Bogotá, D.C, fases diagnóstico inicial, planificación, implementación, mejora continua.

Gráfico 11. Fases de diagnostico



Fuente: Elaboración propia (2023)

- Diagnóstico inicial: se busca saber el estado actual de la defensoría del pueblo y las posibles vulnerabilidades

- Planificación: estrategias de trabajo y análisis de posible impacto en la compañía

- Implementación: se ponen en marcha las mejoras y procedimientos establecidos

- Mejora continua: se lleva un seguimiento de los pasos anteriores para la mitigación de vulnerabilidades

5.9. Impacto en el negocio

Para este componente se tuvo en cuenta los hallazgos y los riesgos que están afectando la continuidad del negocio actualmente en la defensoría del pueblo, como impacto que se quiere reducir el tiempo de respuesta y de remediaciones teniendo en cuenta las vulnerabilidades en cada una de las áreas. Lo cual, tener claridad en cada uno de los procesos y medir el nivel de impacto que tendrá en cada una de las dependencias, el diagnóstico será un instrumento que permitirá evidenciar el estado actual de la organización.

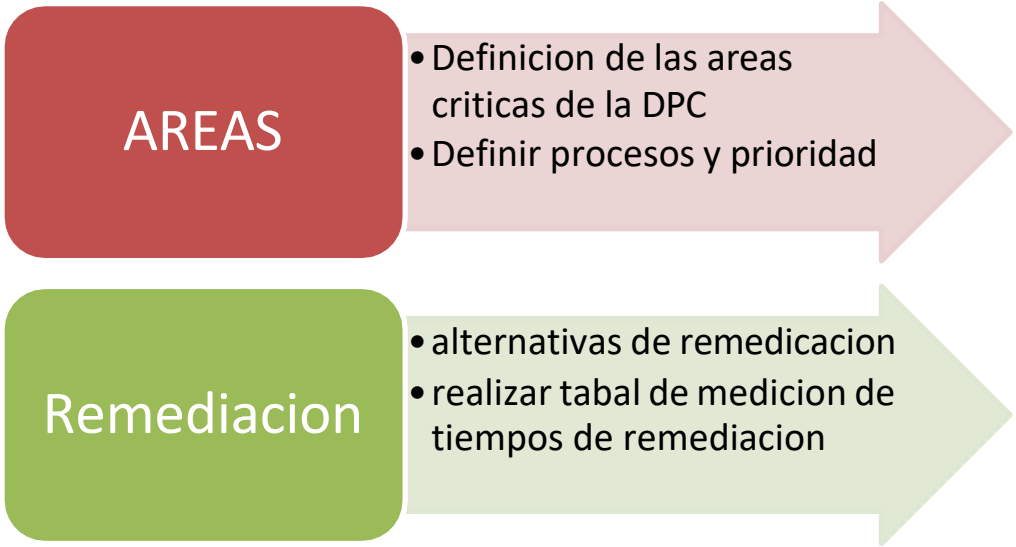
Para ello se tendrán en cuenta las siguientes fases:

- Definir las áreas y los procesos críticos y darle prioridad en la mitigación.

- Verificar las alternativas de corrección más adecuadas de acuerdo con el impacto.

De acuerdo el siguiente gráfico, se debe llevar un seguimiento de los tiempos y la medición de las remediaciones.

Gráfico 12. Fases Impacto En El Negocio



Fuente: Elaboración propia (2023)

5.10. Tiempos de mitigación

Los tiempos de remediación se recomiendan con base a lo señalado por el MINTIC (2019), a partir de la siguiente descripción. - Corto Plazo: La vulnerabilidad debe ser corregida inmediato o antes de 30 días. - Mediano Plazo: La vulnerabilidad debe ser corregida antes 60 días. - Largo Plazo: La vulnerabilidad puede ser corregida antes de 90 días

Tabla 15. Categorización de los tiempos de mitigación

PLAZO	TIEMPO (MESES)	CRITICIDAD
CORTO	30	ALTO
MEDIANO	60	MEDIANO
LARGO	90	BAJO

Fuente: Elaboración propia (2023) basada en el Mintic (2019)

Tabla 16. Tiempos de mitigación

Descripción	Plazo	Criticidad
Informe final	Mediano plazo	Mediano
Establecer los tiempos	Corto plazo	Alto
Alternativas de corrección	Largo Plazo	Bajo
Identificar y definir los procesos	Largo plazo	Bajo

Fuente: Elaboración propia (2023)

Al finalizar esta fase se entregará un documento final donde se consignará las áreas críticas, los hallazgos, los tiempos de mitigación y las recomendaciones que den continuidad del negocio.

5.11. Estrategias de recuperación y respuesta

Como plan de continuidad del negocio este componente es de suma importancia, Se deben definir los requerimientos y los tiempos de interrupción de la continuidad del negocio dentro de las diferentes áreas. Una vez que ya se hallen los procesos críticos, para ello se debe construir una metodología que permita por medio de pasos tomar decisiones acertadas, mitigando los hallazgos y reduciendo el tiempo de recuperación.

El Informe final de recuperación y respuesta debe contener lo siguiente:

- Procesos críticos
- Prioridad para cada proceso
- Tiempos de respuesta

5.12. Documentación (procedimientos, políticas etc.)

Se debe documentar Los procedimientos y políticas que se establecerán de acuerdo con los hallazgos y los procesos críticos que permitan impacten al negocio, reflejando en el modelo propuesto que es el resultado final las políticas y procedimientos

6. Propuesta

6.1. Modelo de GRC (Gobierno, riesgo, y cumplimiento) enfocado a la administración de tecnologías de la información y comunicaciones para optimizar los procesos de la Defensoría del Pueblo de Bogotá, D.C., esta sección se describe la fase de la propuesta, la cual se presenta completa en el anexo E.

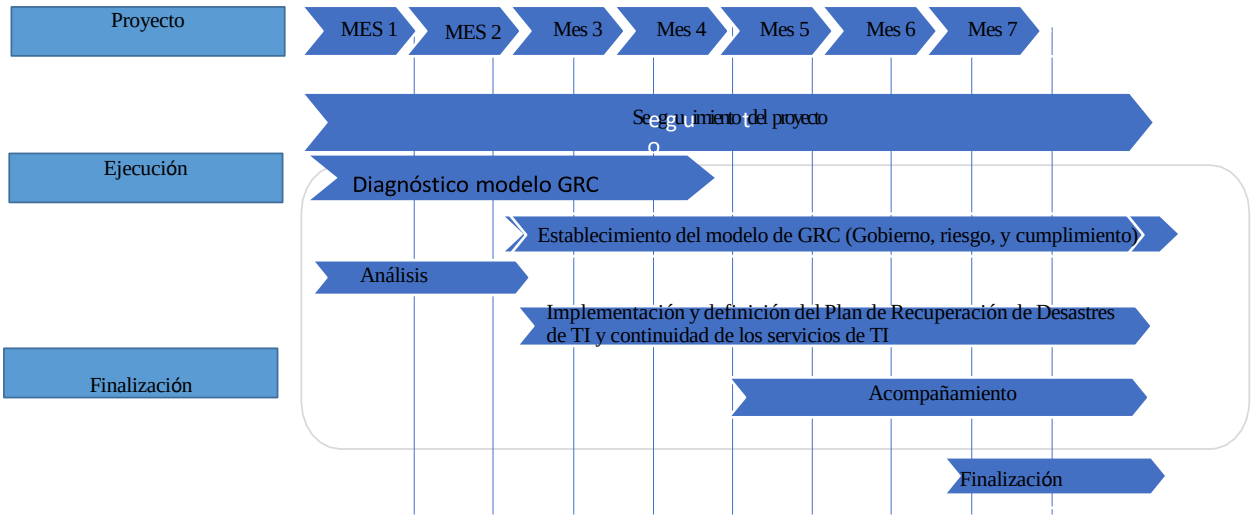
FASE 1. Definición y análisis de procedimiento de continuidad del negocio	• Informe y matriz de riesgos • Plan de tratamiento de riesgos con controles definidos para la continuidad del negocio
Fase 2. Análisis de impacto dentro de la organización	• Informe de Análisis de Impacto. •
Fase 3. Identificación de estrategias de recuperación	• Informe de estrategias de recuperación y sus remediaciones
Fase 4. Informe de recuperación	• Plan de recuperación y contingencia
Fase 5. Pruebas	• Plan de pruebas • Informe de pruebas
Fase 6. Acompañamiento	• Acompañamiento e implementación • Informe con las actividades de acompañamiento realizadas para • asegurar la parametrización, instalación, configuración y despliegue a toda la Entidad de la herramienta escogida por la entidad. • Informe con el seguimiento realizado al tercero del plan de capacitación y apropiación de la herramienta escogida

Tabla 17. Fase de ejecución

Fuente: Elaboración propia (2023)

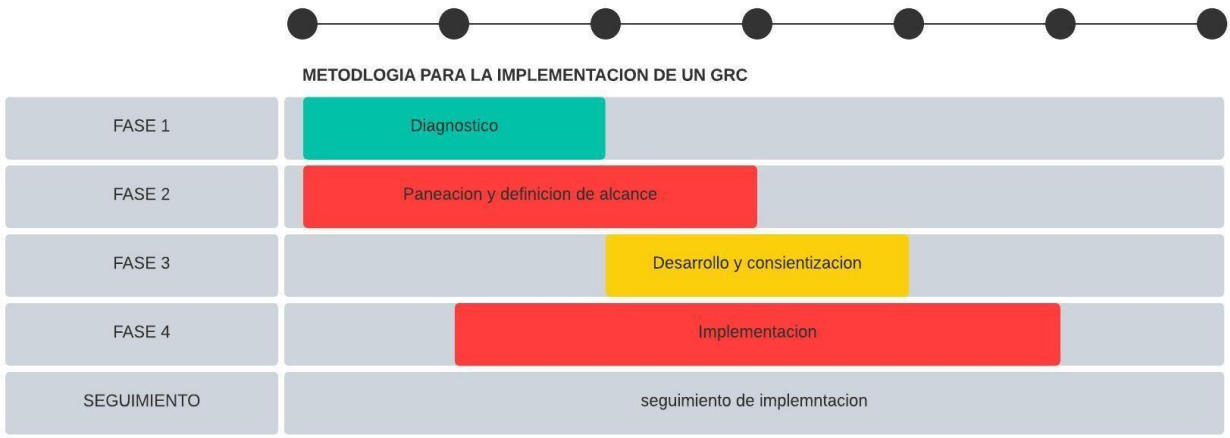
Cronograma del proyecto

Gráfico 13. Cronograma del proyecto



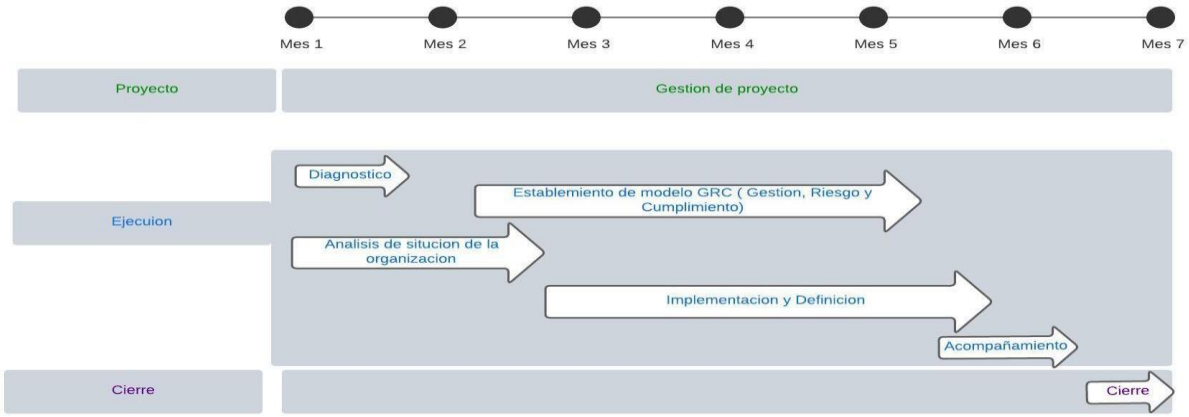
Fuente: Elaboración propia (2023)

Gráfico 14. Metodología para la implementación de un GRC



Fuente: Elaboración propia (2023)

Gráfico 15. Fase final



Fuente: Elaboración propia (2023)

CONCLUSIONES

Luego de aplicar los instrumentos diseñados y analizar los resultados obtenidos se llega a las siguientes conclusiones:

En cuanto al diagnóstico del alcance que tienen los recursos, riesgos de TIC y la aplicación de los estándares de gestión TIC en la Defensoría del Pueblo de Bogotá, D.C., estableciendo las falencias existentes, se evidenció que en la institución se han implementado unas iniciativas para el manejo de riesgos, sin embargo, no existe un programa de manejo de riesgos ni un modelo especifico, no existe una formalidad en cuanto a la identificación de los riesgos.

Aunado a ellos se constató que el área de tecnología no está siendo apoya por la dirección; se está tratando de implementar el subsistema general para la implementación de seguridad de la información a nivel de planeación y se está poniendo en el mapa estratégico para que se dé un cumplimiento y el apoyo de la dirección que es lo más importante para que se dé el tema de gobierno, demás, no existe un nivel jerárquico definido.

De la misma forma, se pudo constatar, que la implementación de un modelo GRC puede conseguir la automatización o mejora de los procesos, asimismo, se evidenció que hacen uso de tecnologías basadas en software libre o código abierto, además, se determinó que los colaboradores no tienen conocimiento exacto de cuantos procesos maneja la institución. Aunado a ello, se pido constatar que está en proceso la implementación plan de la seguridad de la información. Pudiendo determinar que se necesita la implementación de modelo de GRC, debido a que mejoraría los procesos que tiene la entidad en cada una de sus áreas o correspondencias, asimismo, se evidenció que en la entidad no se hace un buen uso de los recursos tecnológicos.

Por otra parte, al identificar los componentes que hacen parte del modelo de GRC (Gobierno, riesgo, y cumplimiento), enfocado a la administración de tecnologías de la información y comunicaciones, para mejorar los procesos de la Defensoría del Pueblo de Bogotá, D.C, se determinó que son cinco: identificación y evaluación de riesgos, mitigación de riesgos y continuidad del negocio, impacto del negocio, estrategias de recuperación y documentación, siendo el riesgo mayor la divulgación de la información.

Finalmente, en la propuesta dellmodelo de GRC (Gobierno, riesgo, y cumplimiento) enfocado a la administración de tecnologías de la información y comunicaciones para optimizar los procesos de la Defensoría del Pueblo de Bogotá, D., en base a las falencias encontradas se desarrolló un modelo de GRC, de forma tal que se conviertan en fortalezas las debilidades existentes, por lo que se desarrolló una metodología para la implementación del modelo de GRC basada en cinco fases: diagnostico, planeación y definición de alcance, desarrollo y concientización, implementación y seguimiento de implementación.

Recomendaciones

Una limitante de la investigación es que este estudio se desarrolló a nivel exploratorio, dada la inexistencia de aplicaciones en el entorno de la Defensoría del Pueblo de Bogotá, D.C, por lo que este modelo solo ha sido evaluado en una organización, teniendo pendiente su puesta en marcha, por lo que se hace necesario replicar este trabajo en otras áreas de acreditación y en diferentes instituciones con el fin de validar su construcción. Posteriores investigaciones deberían evaluar empíricamente la propuesta metodología y su aceptación como herramienta de apoyo procesos de calidad.

Para futuros estudios se destaca la necesidad de investigar cómo integrar los procesos de gestión de riesgos en el resto de los procesos académicos de una universidad con miras al mejoramiento de la calidad de como un todo.

}

Referencias

American Psychological Association. (2010). *Manual de publicaciones de la American Psychological Association.* México: Manual Moderno.

Arias, F. (2016). *El Proyecto de Investigación. Introducción a la Metodología.* Episteme.

Bavaresco, A. (2013). *Proceso Metodológico en la Investigación. Cómo hacer un Diseño de <investigación.* Imprenta Internacional, C.A.

Bonilla, E. (2011). *Metodologíia de la Investigación. UN Enfoque Práctico.* Uniguagira.

Buitrago, L., & Vásquez, Y. (2020). *diseño de un modelo de gobierno de ti para el ministerio de ciencia, tecnología e innovación desde el marco de.* Bogotá D.C, Colombia: Universidad EAN. Recuperado el 18 de 3 de 2023, de https://repository.universidadean.edu.co/bitstream/handle/10882/10613/BuitragoLiliana2020.pdf?sequence=1&isAllowed=y

Cabezas, E., Andrade, D., & Torres, J. (2018). *Introducción a la metodología de la investigación científica.* Universidad de las FuerzasmArmadas ESPE.

Celada, E., Quintero, G., & Ríos, T. (2016). *Gobierno, Riesgo y Cumplimiento Báscios para PYMES.* Medellín, Colombia: Universidad EAFIT. Recuperado el 22 de 3 de 2023, de https://core.ac.uk/download/pdf/47253077.pdf

Defensoria del Pueblo. (s.f.). Recuperado el 27 de 1 de 2023, de https://www.defensoria.gov.co/

Fundación Universitaria Konrad Lorenz. (10 de Julio de 2014). *Para Autores: Revista Latinoamericana de Psicología*. Obtenido de http://publicaciones.konradlorenz.edu.co/index.php/rlpsi/about/submissions#onlineSubmissions

García, J. (2018). Gobernanza, Gestión de Riesgos y Cumplimiento Normativo en la Universidad Pública. Un Nuevo Modelo de Universidad Eficiencia Interna para un Escenario de Competitividad Global. Salamanca, España: Universidad de Salamanca. Recuperado el 1 de 28 de 2023, de https://gredos.usal.es/bitstream/handle/10366/139776/REDUCIDA_Gobernanzagesti%C3%B3nriesgos.pdf?sequence=1&isAllowed=y

Guzmán, R., Rodríguez, L., & Rodróguez, N. (2017). *Diseñar una Gu+ia de Implementación del Modelo de Gobierno, Riesgo y Cumplimiento (GRC) en el centro de salud R.D., en República Dominicacan.* Universidades APEC y Valencia. Recuperado el 15 de 1 de 2023, de https://bibliotecaunapec.blob.core.windows.net/tesis/TPG_CI_MAI_02_2017_ET170551.pdf

Hernández, R., Fernández, C., & Baptista, P. (2006). *Metodología de la investigación.* México: MacGraw-Hill.

Ixcamparic, L (2018) análisis financiero de la implementación del modelo de gestión grc – gobierno, riesgo y cumplimiento en empresas comercializadoras de motocicletas en Guatemala. Tesis de maestría Universidad San Carlos de Guatemala. Recuperado el 04 de 7 de 2024. Disponible: http://biblioteca.usac.edu.gt/tesis/03/03_5860.pdf

López, F., Garduño, E., Romero, A., Alvarado, V., & Caballero, M. (7Enero –Junio de 2017). Propuesta de un sistema de gobierno, riesgos y cumplimiento para ser alineado a distintas normativas y regulaciones en pequeñas y medianas empresas. *Revista Electrónica sobre Tecnología, Educación y Sociedad, 4*(7). Recuperado el 21 de 3 de 2023, de https://www.ctes.org.mx/index.php/ctes/article/view/623/649

Muñoz, I., & Ulloa, G. (2011). Gobierno de TI – Estado del arte. *S&T, 9*(17), 23-53. Recuperado el 8 de 4 de 2023, de https://www.redalyc.org/pdf/4115/411534384003.pdf

(MINTIC), M. d. (2019). *MGGTI.G.GEN.01 – Documento Maestro del Modelo de Gestión y Gobierno de TI.* Recuperado el 7 de 6 de 2023, de https://www.mintic.gov.co/arquitecturati/630/articles-144767_recurso_pdf.pdf

NTC-ISO31000. (s.f.).

Oviedo, A. (2020). *Modelo de Gobierno y Gestión de Riesgos Ti para las Universidades*

Anexo A. Entrevista estructurada

1. Que nos puede contar sobre gobierno, riesgo y cumplimiento en la Defensoría del Pueblo.

2. En cuanto a riesgo ¿cómo están blindados?

3. En cuanto a gobierno ¿cómo detecta la entidad?

-

Anexo B. Cuestionario

1: ¿Usted cree que con la implementación de un modelo GRC se puede conseguir la

automatización o mejora de los procesos? Seleccione que beneficios traería la implementación de este

a. Mejora los tiempos de respuesta
b. Reducir costos operacionales
c. Mejorar disponibilidad de sus servicios
d. Mejorar la satisfacción de los ciudadanos
e. Mejorar la satisfacción de los usuarios internos
f. Otros. ¿Cuál?
g. Ninguna de las anteriores

2. ¿La entidad hace uso de tecnologías basadas en software libre o código abierto?

a. Si
b. No

3. Con respecto a los procesos de la entidad indique

a. ¿Cuántos procesos tiene la entidad?

b. ¿Cuántos procesos se han automatizado o mejorado teniendo en cuenta las definiciones (lineamientos, guías, herramientas y mejores prácticas) del marco de referencia empresarial?

c. ¿Cuántos procesos se han mejorado incorporando esquemas de manejo seguro de la información conforme a lo establecido en el modelo de seguridad y privacidad de la información?

4. ¿Su entidad implementó un plan de la seguridad de la información?

a. Si, se implementó
b. Está en proceso
c. No
d. En caso de no, ¿Por qué?

5: De acuerdo con su conocimiento ¿usted cree que la entidad necesita la implementación de

modelo de GRC?

a. Si

b. No

6. ¿Usted cree que con la implementación de un modelo GRC mejorarían los procesos que tiene la entidad en cada una de sus áreas o correspondencias?

a. Si

b. No

7. ¿Usted cree que la entidad está haciendo buen uso de los recursos tecnológicos en cada una de sus áreas? Califique del 1 al 5, donde 1 es la más baja y 5 la más alta.

a. 1

b. 2

c. 3

d. 4

e. 5

8. ¿Cómo considera usted la aplicación de esta encuesta?

a. Excelente

b. Buena

c. Regular

d. Mala

e. No era necesario

1.3 Anexo C. Informe GAP

Control de versiones y cambios

Elaboró :

Fecha	Autor	Cargo	Versión	Referencia del Cambio
	Alexander Amézquita	TA G15	1.0	N/A
	Orlando Burgos Triana	PE G18	1.0	N/A

Revisó:

Fecha	Autor	Cargo	Versión

Aprobó:

Fecha	Autor	Cargo	Versión

Introducción.

La seguridad de la información es considerada como un componente crítico dentro de la estrategia de Gobierno en Línea (GEL) para las entidades del estado, por este motivo, la recomendación para Iniciar el establecimiento de un Sistema de Gestión de Seguridad de la Información (SGSI), es iniciar con la determinación de la brecha de seguridad (GAP), la cual permitirá determinar el nivel de madurez con que cuenta la entidad en lo relacionado con seguridad de la información y con base en estos resultados, proponer un plan de acción que permita la futura implementación del modelo de seguridad de la información al interior de la Defensoría del Pueblo.

Objetivos.

Objetivo general.

Presentar el informe ejecutivo del análisis GAP realizado en la Defensoría del Pueblo en referencia a la Norma ISO/IEC 27001:2013 con el fin de determinar el grado de general de madurez en el que se encuentra la entidad en términos de la seguridad de la información.

Objetivos específicos.

Presentar los resultados de acuerdo con el siguiente listado:

Nivel de madurez por Dominios

Hallazgos principales.

Recomendaciones.

Alcance.

El análisis de la brecha de seguridad (GAP) realizado en la Defensoría del Pueblo incluyó:

3 procesos estratégicos.

8 procesos y subprocesos misionales.

6 procesos de apoyo.

2 procesos de evaluación.

Metodología.

Elaboración de instrumento de medición.

Para el desarrollo de este instrumento, la Defensoría del pueblo diseño e implemento una aplicación informática que permite la administración de áreas de aplicación, usuarios por áreas, dominios y preguntas de cada uno de ellos.

La aplicación se puso en producción y se aplicó inicialmente la encuesta a los funcionarios del área de sistemas que lideran la implementación del SGSI.

Implementación de instrumento de medición

Se definieron en total 18 procesos como objetivo de la encuesta, a los cuales se aplican las preguntas pertenecientes a los dominios administrativos:

A.5. Política De Seguridad De Información

A.6. Organización De La Seguridad De La Información

A.7. Seguridad De Los Recursos Humanos

A.8. Gestión De Activos

A.17 Aspectos De Seguridad De La Información De La Gestión De Continuidad De Negocio

A.18 Cumplimiento

El proceso (área) de tecnología de las comunicaciones, fue responsable del diligenciamiento de las preguntas de los dominios técnicos:

A.10 Criptografía

A.11 Seguridad Física Y Del Entorno

A.9. Control De Acceso

A.12 Seguridad De Las Operaciones

A.13 Seguridad De Las Comunicaciones

A.14 Adquisición, Desarrollo Y Mantenimiento De Sistemas

A.16 Gestión De Incidentes De Seguridad De La Información.

Consolidación de resultados.

Los niveles de madures del sistema se miden en 6 estados, los cuales están descritos en la siguiente tabla

Nivel de Implementación	% de Cumplimiento	Descripción
Gestionado	**100%**	Los procesos han sido llevados al nivel de mejores prácticas, con base en los resultados de la mejora continua.
		Es posible hacer seguimiento y medir el cumplimiento de los procedimientos, así como tomar acciones correctivas o preventivas cuando se detectan fallas y hacer seguimiento dichas acciones.
Medible	**80%**	Es posible hacer seguimiento y medir el cumplimiento de los procedimientos, aunque no es constante que se tomen acciones correctivas o preventivas.
Definido	**60%**	Los procesos se encuentran totalmente documentados pero la responsabilidad del cumplimiento recae en cada individuo y es poco probable que se detecten desviaciones a los estándares establecidos.
Repetible	**40%**	Los procesos se han desarrollado hasta un punto en el cual procedimientos similares son utilizados por personas diferentes para llevar a cabo la misma tarea, aun cuando estos no se encuentran totalmente documentados.
Inicial	**20%**	Se ha identificado una situación que debe ser tratada y se han implementado acciones aun cuando no hay directivas o procesos documentados relacionados con dichas acciones.
Inexistente	**0%**	Carencia total de procesos relacionados con el SGSI.
		La organización no ha identificado una situación que debe ser tratada.

La verificación tenía como objetivo evidenciar el nivel de madurez de los dominios del anexo A de la Norma ISO 27001, encontrando lo siguiente:

El nivel de cumplimiento de los requisitos esta por el orden de un 56.3 %, El requisito mínimo de madurez de una entidad para lograr una gestión medible en seguridad de la información debe ser igual o superior al 70%.

La calificación obtenida de acuerdo a cada dominio, nos permite evidenciar lo siguiente:

Item	Dominios	Cumplimiento	
5	POLITICA DE SEGURIDAD	52.63 %	
6	ORGANIZACION DE LA SEGURIDAD DE LA INFORMACIÓN	50.00 %	
7	SEGURIDAD DE LOS RECURSOS HUMANOS	90.32 %	
8	GESTIÓN DE ACTIVOS	39.00 %	
9	CONTROL DE ACCESO	50.00 %	
10	CRIPTOGRAFÍA	50.00 %	
11	SEGURIDAD FÍSICA Y DEL ENTORNO	50.00 %	
12	SEGURIDAD DE LAS OPERACIONES	50.00 %	
13	SEGURIDAD DE LAS COMUNICACIONES	50.00 %	
14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	50.00 %	
15	RELACIONES CON LOS PROVEEDORES	67.85 %	
17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	75.00 %	
18	CUMPLIMIENTO	57.69 %	
TOTAL		56.34 %	

Análisis de resultados

Políticas para la seguridad de la información

Aunque en la Defensoría del Pueblo existe una Política de Seguridad de la Información revisada y aprobada por la dirección de esta no ha sido socializada ni divulgada de manera eficiente.

Se recomienda incluir la socialización y divulgación de la política en los procesos de inducción y reinducción institucional para funcionarios, de igual manera debe ser de conocimiento de los contratistas y personal que cumpla funciones públicas en la organización.

Revisión de las políticas para seguridad de la información

Es recomendable realizar la revisión actualización periódica que pueda resultar en ajustes a los lineamientos contenidos en la misma, con el fin de atacar problemáticas que no se contemplaron en versiones anteriores.

Asignación de responsabilidades para la seguridad de la información

Es importante que todas las áreas de la Defensoría y sus funcionarios conozcan e interioricen la responsabilidad transversal del uso de la Políticas de Seguridad, como herramienta que garantiza la disponibilidad, confidencialidad e integridad de los activos de información institucional.

Organización de la Seguridad Organización interna

En el área de TIC se deben asignar responsabilidades específicas a cada funcionario encargado del monitoreo de controles que dependan de Tecnología y asignar el cargo de Analista de Seguridad de la Información a un funcionario que se encargue de la implementación del SGSI.

Contacto con las autoridades

Se debe formalizar y definir en el “Plan de Contingencia de TI”, la lista de contactos definidos y conocidos por el personal de tecnología, seguridad el cual debe contener: número de personal encargado de la seguridad física, autoridades policiales, personal de mantenimiento correctivo, personal de mantenimiento a UPS, aire acondicionado, bases de datos, empresa de Energía, IPS etc. estos se deben encontrar en un lugar visible ante un eventual fallo no programado.

Seguridad de la información en gestión de proyectos

Se recomienda realizar los estudios de seguridad de los ingenieros que implementan proyectos de que involucren información sensible, clasificada o reservada, definiendo las cláusulas contractuales de confidencialidad y el tratamiento de la información.

Teletrabajo

Verificar si es necesaria la implementación de un concentrador de VPN para soporte y trabajo de los administradores en caso de falla.

Términos condiciones del empleo

Con respecto a seguridad de la información todos los funcionarios deben conocer la política y saber de su obligatorio cumplimiento.

Toma de conciencia, educación y formación en la seguridad de la información

Se deben realizar actas de instrucción y socialización de seguridad de la información de forma periódica, adicionalmente se debe realizar un cronograma de capacitación del SGSI y se deben evaluar evidencias y nuevas formas de sensibilización

Proceso disciplinario

En la política debe estar definido el alcance disciplinario que conllevaría el incumplimiento o violación de las políticas de seguridad emitidas por la Defensoría del Pueblo.

Inventario de activos

Cada una de las áreas institucionales, debe revisar y mantener actualizada periódicamente la información, definida en los catálogos de información pública, clasificada y reservada.

Uso aceptable de los activos

Se deben realizar jornadas y campañas de capacitación en el manejo del sistema RAEI para el registro y la identificación de activos de información.

Manejo de activos

Se debe incluir en la política de seguridad, el manejo de los activos asignados a funcionarios.

Transferencia de medios de soporte físicos

Diseñar procedimientos y formatos generales para la entrega de información física o digital, esto debe ir alineado con la clasificación de la información y el programa de gestión documental.

Política sobre el uso de controles criptográficos

Crear política de uso de cifrado para almacenamiento de archivos, transferencia de archivos.

Protección contra códigos maliciosos.

Se debe evaluar la viabilidad de la adquisición de un sistema de protección contra virus informáticos y malware diferente al que provee el mismo sistema operativo para las estaciones de trabajo de usuario final y definir un plan de despliegue de esta solución a nivel regional.

Copias de respaldo de la información

Se debe implementar un procedimiento de verificación de respaldos de manera periódica dependiendo del activo que se resguarda y su criticidad, e incluirlo dentro del Plan de Atención de Desastres de TI.

Registro y seguimiento

Se debe contar con procedimientos documentados para la correlación de eventos e incidentes de seguridad.

Control de software operacional

Se deben implementar controles a nivel de dominio que permitan la implementación de restricciones sobre software no licenciado y la verificación oportuna de uso ilegal de software.

Gestión de la vulnerabilidad técnica

Se debe implementar un procedimiento documentado para la ejecución de test de penetración y análisis de vulnerabilidades.

Resultados y avances en la implementación PHVA:

Se encuentran desarrollados documentalmente los siguientes productos en el marco de la implementación del SGSI:

1. POLITICA DE SEGURIDAD DE LA INFORMACION:

Se definió el objetivo, alcance, nivel de aplicación, se encuentra aprobado y publicado como documento general y de carácter transversal para todas las áreas institucionales.

Se han realizado ajustes y verificación de aplicación al interior del área de TI.

2. PLAN DE TRATAMIENTO DE RIESGOS:

El plan de tratamiento de riesgos se enfoca en las guías de Risk IT Framework de ISACA, se encuentra en revisión y consta de tres fases principales:

1era Fase: (Pendiente de aprobación y ejecución)

Diagnostico

En esta fase se realizará la ejecución de una auditoria de seguridad y ética hacking para evaluar el estado actual de la Defensoría en materia de protección de datos. Los profesionales del área de TI con conocimientos y experiencia en seguridad de la información evaluaran la completitud de los activos de información de los procesos, y en coordinación con el área de Gestión Documental, se ajustarán las tablas de retención de la información, y se diseñaran los manuales y clausulas requeridas.

2da Fase: (Pendiente de aprobación y ejecución)

Identificación y evaluación de riesgos de seguridad y privacidad de la información.

Identificación y evaluación de riesgos de Tecnología y operativos de procesos.

3ra Fase: (Pendiente de aprobación y ejecución)

Implementación y Comunicación

3. PLAN DE MITIGACION DE DESASTRES TIC

En este se definen los procedimientos de copias de seguridad y plan de respaldo que permitan la continuidad de la plataforma tecnológica en caso de un desastre, acordes con la política seguridad de información. El documento se encuentra en fase de revisión

4. CATALOGO DE APLICACIONES Y SERVICIOS

Incluye la descripción de características e interacción con procesos de los sistemas de información de carácter misional, administrativo y financiero. El documento se encuentra ya aprobado y sin embargo debe ser actualizado.

5. PLAN DE ADOPCIÓN DE IPV6 DEFENSORIA

La Defensoría en acatamiento a las directrices de MinTIC, que mediante la Resolución No. 2710 de 2017, estableció los lineamientos para la adopción del protocolo IPv6 por parte de las entidades que conforman la administración pública, definió el plan de implementación a nivel Central en las sedes Bogotá, y las 38 regionales del territorio nacional. Este plan fue aprobado y ejecutado para la vigencia 2020.

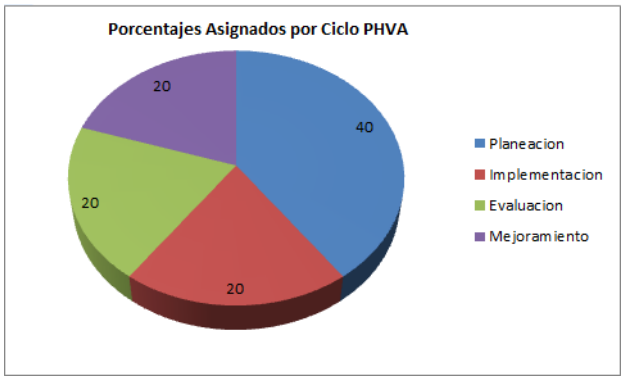
6. REGISTRO Y CALIFICACION DE ACTIVOS DE INFORMACION

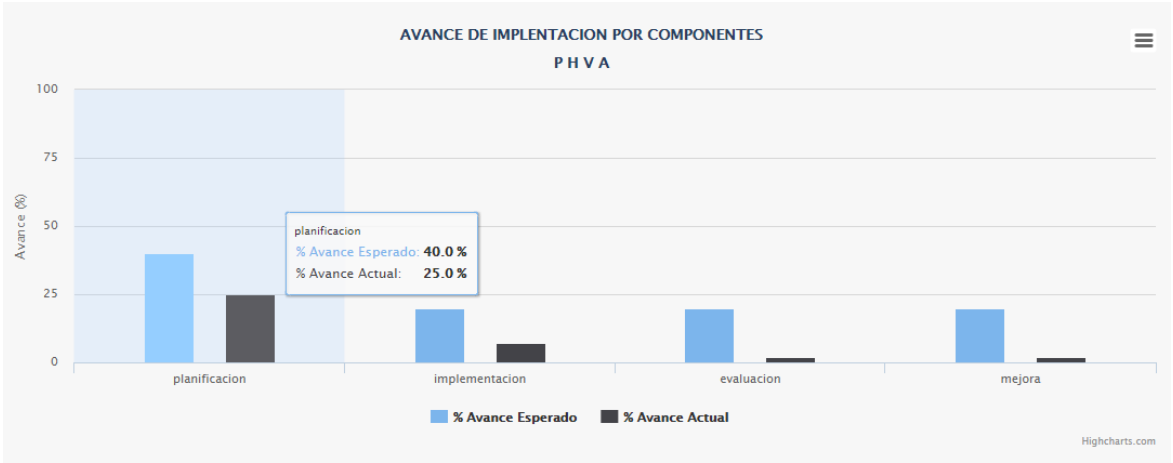
El área de tecnología de la entidad, desarrollo un sistema de información que permite el registro y calificación de la información de acuerdo a lo estipulado en la ley 1712 de2014 en su Artículo 13. Registros de Activos de Información y siguiendo los criterios y lineamientos definidos del Min TIC.

Este aplicativo (RAEI), se encuentra en producción y permite el registro de toda la información que las áreas y sus delegados consideren generadora de valor institucional,

permitiendo a través de la misma herramienta la calificación según los criterios de reserva, clasificación y publicación.

El avance general de la implementación acuerdo a lo evaluado se observa en la siguiente imagen: (Teniendo en cuenta los avances esperados para: planificación de un 40%, implementación 20%, evaluación 20% y mejoramiento 20%)





Glosario.

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controlar en su calidad de tal.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: Se entiende por datos sensibles 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. (Decreto 1377 de 2013, art 3).

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

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 la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

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 la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Responsabilidad Demostrada: Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de

actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Normatividad Aplicable.

Constitución Política de Colombia: Por medio de la cual se promulga el marco jurídico, democrático y participativo que garantiza el orden político, económico y social justo, así como el compromiso a impulsar la integración de la comunidad latinoamericana.

Decreto 612 de 2018: Por el cual se fijan las directrices para la integración de los planes institucionales y estratégicos al plan de acción por parte de las entidades del estado.

Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Ley 527 de 1999: Por la cual se define y regula el uso de los mensajes de texto, comercio electrónico y firmas digitales.

Ley 1341 de 2009: Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

Ley Estatutaria 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.

Decreto 025 de 2014: Por el cual se modifica la estructura orgánica y se establece la organización y funcionamiento de la Defensoría del Pueblo.

Decreto 2573 de 2014: Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

Decreto 943 de 2014: Modelo Estándar de Control Interno (MECÍ)

Resolución 1014 de 2013: Por la cual se adopta el Plan Estratégico de la Defensoría del Pueblo para la vigencia 2013-2016.

Resolución 1296 de 2014: Manual de Supervisión e Interventoría de la Defensoría del Pueblo.

Norma NTC ISO 9001: Sistemas de Gestión de la Calidad.

Norma NTCGP 1000:2009: Norma Técnica de Calidad en la Gestión Pública – ICONTEC.

Norma NTC-ISO-IEC 27001: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos.

Norma NTC-ISO-IEC 27002: Tecnología de la información. Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información.

Bibliografía

Organización Internacional de Estandarización. ISO 27000. [En Línea] https://www.iso.org/obp/ui#iso:std:iso-iec:27000:ed-5:v1:en

Organización Internacional de Estandarización. ISO 27001. [En Línea] https://www.iso.org/obp/ui#iso:std:iso-iec:27001:ed-2:v1:en

Organización Internacional de Estandarización. ISO 27002. [En Línea] https://www.iso.org/obp/ui#iso:std:iso-iec:27002:ed-2:v1:en

Organización Internacional de Estandarización. ISO 27005. [En Línea] https://www.iso.org/obp/ui#iso:std:iso-iec:27005:ed-2:v1:en

Organización Internacional de Estandarización. ISO 31000. [En Línea] https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es.

El portal de ISO 27001. ISO 27000.es. [En Línea] https://www.iso27000.es/sgsi.

MinTIC. Modelo de Seguridad y Privacidad de la Información MSPI. [En línea] https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

MinTIC. Gobierno Digital. [En línea] https://www.estrategia.gobiernoenlinea.gov.co/

MinTIC. Instrumento de Evaluación MSPI. [En línea] https://www.mintic.gov.co/gestionti/615/articles-5482_Instrumento_Evaluacion_MSPI.xlsx

MinTIC. Modelo de Gestión de Riesgos de Seguridad Digital - MinTIC. [En línea] https://www.mintic.gov.co/portal/604/articles-61854_documento.docx

1.4 Anexo D. Acta de reunión

Modelo GRC enfocado a la administración de Tecnologías de la Información y las Comunicaciones para mejorar los procesos empresariales de la defensoría del pueblo.

1.4.1 Acta de Reunión

Proyecto: MODELO GRC	Lugar de la Reunión: Fecha: 20/06/2023

Versión:
0100Fecha:
20/11//2023

Proyecto	Modelo GRC		
Entregable	Acta de Reunión		
Autor	Jorge Eliecer Zúñiga Barros		
Versión/Edición	0100	**Fecha Version**	20/11/2023
		Nº Total de Páginas	

- ÍNDICE

1 LISTA DE CONVOCADOS

Nombre y Apellidos	Organismo	ASISTE (S/N)
ORLANDO BURGOS	DPC	
VIVIANA PINILLA	DPC	
LIZET ALVAREZ	DPC	

1 AGENDA DE LA REUNIÓN

1.1 Orden del Día

Nº	Asunto	Tiempo Estimado	Responsable
1	ESTADO ACTUAL DE LA DEFENSORIA DEL PUEBLO	30 MIN	Jorge Eliecer Zúñiga Barros
2	POSIBLES REMEDIACIONES	30 MIN	Jorge Eliecer Zúñiga Barros

2.2 Objetivos Principales

Identificar el estado actual de la Defensoría del Pueblo en Gobierno, Riesgo y Cumplimiento y las posibles remediaciones que se le puede dar para mitigar riesgos.

3 REUNION

Durante la reunión se habló del estado actual del GRC en la Defensoría del Pueblo y cómo podemos aportar de acuerdo a nuestra experiencia para remediar los estados críticos encontrados durante nuestra investigación.

Establecimos las fechas de entrega y los parámetros a tener en cuenta.

Se tuvo en cuenta las recomendaciones del oficial de seguridad de la Defensoría del Pueblo.

Se establecieron los compromisos.

4 ACUERDOS Y TAREAS

Acuerdo	Responsables	Fecha Prevista	Estado
Evaluar la entidad	Jorge Eliecer Zúñiga Barros	30 de noviembre 2023	Pendiente
Entregar modelo GRC	Jorge Eliecer Zúñiga Barros	30 de noviembre 2023	Pendiente