DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA FAMILIA DE NORMAS DE LA SERIE ISO/IEC 27000 PARA UNA ENTIDAD PÚBLICA COLOMBIANA

ARTURO CARDONA LONDOÑO

DIANA LIZETH CARVAJAL PORTILLA

UNIVERSIDAD AUTÓNOMA DE MANIZALES

FACULTAD DE INGENIERÍA

MAESTRÍA EN GESTIÓN Y DESARROLLO DE PROYECTOS DE SOFTWARE

MANIZALES

2018

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA FAMILIA DE NORMAS DE LA SERIE ISO/IEC 27000 PARA UNA ENTIDAD PÚBLICA COLOMBIANA

ARTURO CARDONA LONDOÑO

DIANA LIZETH CARVAJAL PORTILLA

Proyecto de grado para optar al título de Magister en Gestión y Desarrollo de proyectos de Software

Asesor

PhD. FRANCISCO JAVIER VALENCIA DUQUE

UNIVERSIDAD AUTÓNOMA DE MANIZALES

FACULTAD DE INGENIERÍA

MAESTRÍA EN GESTIÓN Y DESARROLLO DE PROYECTOS DE SOFTWARE

MANIZALES

2018

DEDICATORIA

Agradecemos a nuestros padres por su apoyo incondicional.

AGRADECIMIENTOS

Agradecemos al doctor Francisco Valencia por su apoyo incondicional en la realización de este documento, y al doctor Mauricio Alba su acompañamiento y asesoría durante nuestros estudios.

RESUMEN

Los activos de información han adquirido un gran valor para las organizaciones, lo cual ha generado una necesidad legal y organizacional para todas las empresas por medio de la confidencialidad, integridad y disponibilidad de la información. Para poder dar solución a estas necesidades en las entidades públicas, el Gobierno Colombiano ha creado la estrategia de Gobierno en Línea, con un componente de seguridad y privacidad de la información basado en la norma ISO/IEC 27001, que plantea como objetivos el diseño, ejecución, monitoreo y control de un sistema de gestión de seguridad de la información.

Este proyecto plantea como resultado la propuesta del diseño del Sistema de Gestión de seguridad de la información de una entidad pública, basándose en la familia de normas de la ISO 27000 y complementándose con el Modelo de Seguridad y Privacidad de la información propuesto por MinTic.

Palabras clave: Seguridad de la Información, ISO/IEC 27000; SGSI, Riesgos de TI, Metodologías

ABSTRACT

The information assets have acquired a great value for the organizations, which has generated that safeguarding the confidentiality, integrity and availability of the information is a legal and organizational necessity for all the companies, to be able to give solution to these needs in the public entities , the Colombian Government has created the Online Government strategy, with a security and information privacy component based on the ISO / IEC 27001 standard, which sets out as objectives the design, execution, monitoring and control of a management system of information security.

This project has resulted in the proposal for the design of the Information Security Management System of a public entity, based on the family of ISO 27000 standards, complemented by the guidelines of the Security and Privacy Model of the information proposed by MinTic.

Keywords: Information Security, ISO/IEC 27000, ISMS, IT Risks, Methodologies

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

1. PRESENTACIÓN

La información manejada al interior de la entidad pública colombiana debe contar con niveles adecuados de aseguramiento, en términos de confidencialidad, integridad y disponibilidad, en esencia, debido al tipo de información que maneja, la cual se encuentra asociada en una gran proporción a información ciudadana.

De forma adicional, las entidades públicas deben cumplir con la estrategia de Gobierno en línea (GEL) propuesta por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), la cual contempla como uno de sus componentes la seguridad y privacidad de la información.

Para dar respuesta tanto a la seguridad de la información, como al cumplimiento que por ley debe desarrollar la entidad en relación con el tema, este proyecto pretende establecer un marco de seguridad y privacidad de la información y de los sistemas de información en contexto con los procesos de la entidad.

Para dar cumplimiento a esta necesidad se acude al método de caso de estudio, teniendo como alcance los procesos financieros de la entidad, para lo cual se llevará a cabo una revisión sistemática de literatura sobre sistemas de gestión de seguridad de la información (SGSI), seguido del desarrollo del caso de estudio, que incluyen diversas fases, las cuales estarán basadas en la metodología propuesta por Valencia-duque & Orozco-alzate (2017) y utilizando de forma complementaria las guías del modelo de seguridad y privacidad de la información (MSPI) propuestas por MinTIC.

Como resultado de este proyecto se espera diseñar un SGSI ajustado a las necesidades de la entidad y un plan de implementación. Adicional a esto se harán recomendaciones a la entidad sobre cómo implementar el SGSI en otras áreas y un artículo científico que presente los resultados del proyecto.

2. REFERENTE CONTEXTUAL

2.1.Área Problemática

En el año 2016 el 46.7 % de las empresas en Colombia sufrieron algún tipo de incidente relacionado con la seguridad de la información (ESET, 2017), en diferentes modalidades como *phishing, ransomware*, ataques de denegación de servicios, fraudes internos y externos, infección de malware y explotación de diferentes vulnerabilidades. Lo anterior da cuenta de las grandes brechas de seguridad de la información en las entidades colombianas, causando entre otros impactos: la exposición de datos personales, robo de identidades, acceso a cuentas de forma no autorizada, pérdida de credibilidad entre otras.

Las víctimas de estos ataques para el año 2016 en su mayoría son los ciudadanos en un 52%, seguido del sector financiero en un 14%, industria tecnológica con el 8% y el sector gobierno con un 4%. Para este último, en los servicios de Gobierno electrónico el malware se ha convertido en la principal amenaza, los atacantes utilizan correos falsos de entidades públicas para difundir y capturar la información de sus víctimas (Centro cibernético, 2017).

En el caso de las entidades del orden territorial como Gobernaciones y Alcaldías se deben procurar por salvaguardar la información en términos de disponibilidad, integridad y la confidencialidad, para así proteger los derechos de los ciudadanos, la integridad del estado y la industria; en cuanto a la vida, la salud y la seguridad (artículo 31 de la Ley 1448 de 2011), la defensa y la seguridad nacional (artículo 8 de la Ley 1621 de 2013), las relaciones internacionales (artículo 4 de la Ley 68 de 1993), entre otros.

La entidad no cuenta con un modelo de seguridad y privacidad de la información plenamente consolidado y tan solo se cuenta con medidas de seguridad informática dispersas sin un enfoque integrado y ajustado a las mejores prácticas del mercado, ni a los lineamientos establecidos por el gobierno nacional, de forma tal que sea el pilar de apoyo para la protección de los datos manejados en su interior, algunos de estos datos si no son tratados de forma adecuada y son accedidos, publicados o modificados de forma errónea, pueden afectar gravemente a los ciudadanos, el estado, la industria y la seguridad nacional.

En respuesta a lo anterior, el Gobierno colombiano desarrolla la estrategia de gobierno en línea, a través de la cual, entre otros aspectos, se definen lineamientos para la implementación de un modelo la seguridad de la información con el objetivo de tener un estado más eficiente, transparente, y participativo, asegurando la información de los ciudadanos y del estado.

Para asegurar la información manejada y dar cumplimiento a las normas promulgadas al respecto, la entidad requiere el diseño de un Sistema de gestión de seguridad de la información.

2.1.1 Pregunta de investigación

¿Cómo la entidad pública colombiana podrá asegurar sus activos de información cumpliendo con los requerimientos de la estrategia de gobierno en línea?

2.2. Justificación

La entidad tiene dentro de sus objetivos principales la atención al ciudadano, por ello proporciona mecanismos que faciliten su interacción, conocimiento de necesidades y canales de respuesta eficientes. Dentro de este quehacer surge como necesidad proteger la información tratada y generada al interior de la entidad.

Para dar respuesta a esta necesidad se debe elaborar un plan para la implementación de un sistema de gestión de seguridad de la información (SGSI), que aporte los lineamientos rectores para la protección de datos al interior de la entidad.

Además de lo anterior, la entidad siendo un ente territorial debe ceñirse a los lineamientos estipulados por el Gobierno nacional que buscan la mejora en la prestación de servicios de las entidades públicas al ciudadano, con tal objetivo el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MinTIC) por medio del decreto 1151 del año 2008 lanzó la estrategia GEL, luego fue actualizado por el decreto 1078 del año 2015, la estrategia apunta a:

- Lograr que los ciudadanos cuenten con servicios en línea de muy alta calidad.
- Impulsar el empoderamiento y la colaboración de los ciudadanos con el Gobierno.
- Encontrar diferentes formas para que la gestión en las entidades públicas sea óptima gracias al uso estratégico de la tecnología.
- Garantizar la seguridad y la privacidad de la información.

En torno a esta última estrategia, plantea como objetivo primordial salvaguardar la confidencialidad, integridad y disponibilidad de la información (Pilares fundamentales de la seguridad de la información), por medio de las siguientes actividades:

1. Realizar el diagnóstico de seguridad y privacidad (Definición).
2. Realizar el plan de seguridad y privacidad de la información (Definición).
3. Realizar la gestión de riesgos de seguridad y privacidad de la información.
4. Evaluación del diseño (Monitoreo y mejoramiento continuo).

Por lo anterior es de interés para la entidad promover, plantear y llevar a cabo iniciativas que apunten a cumplir los anteriores objetivos; el presente proyecto busca cumplir los tres primeros y tiene como resultado principal la generación del plan para la implementación del sistema de gestión de seguridad de la información (SGSI), tomando como base la familia de normas de la ISO/IEC 27000 y el MSPI promovido por el MinTIC; que tiene como finalidad garantizar la protección de la información y la privacidad de los datos de los ciudadanos y funcionarios de la entidad que lo aplique (MinTIC, 2015c).

En resumen, este proyecto procura evaluar el estado actual de seguridad de la información en la entidad y posteriormente dejar un plan para la implementación del SGSI, en aras de proteger los datos y la información tanto de la entidad, sus funcionarios y los ciudadanos, además de dar cumplimiento a lo establecido por ley en cuanto a los plazos para la Implementación de la estrategia Gobierno en línea.

2.3.Objetivos

2.3.1. Objetivo general

Definir el marco de seguridad y privacidad de la información y de los sistemas de información bajo el marco de la norma NTC ISO/IEC 27001: 2013 en la entidad.

2.3.2. Objetivos específicos

- Llevar a cabo una revisión sistémica de literatura de los sistemas de gestión seguridad de la información a nivel internacional.
- Establecer el estado actual de la seguridad de la información de la entidad.
- Diseñar el sistema de gestión de seguridad de la información.
- Definir el plan de implementación del sistema de gestión de seguridad de la información.

2.4. Estrategia metodológica

2.4.1. Enfoque

El enfoque de este proyecto es de tipo Gestión, con un tipo de estudio cualitativo

2.4.2. Metodología

Se plantea la realización de un caso de estudio, tomando como referencia el artículo "El método de estudio de caso: Estrategia metodológica de la investigación científica", la cual tiene las siguientes etapas y actividades (Martínez Carazo, 2006):

2.4.2.1. Semblanza del caso de estudio

Para la semblanza del caso de estudio, se realizará una revisión sistémica de literatura, tomando como base los pasos proporcionados por Barbara Kitchenham en el informe técnico "Procedures for Performing Systematic Reviews" (Kitchenham, 2004), la cual tiene las siguientes etapas y actividades:

- Planificación de la revisión:
    - Identificación de la necesidad de una revisión
    - Desarrollo de un protocolo de revisión.
- Ejecución la revisión:
    - Identificación de la investigación
    - Selección de estudios primarios
    - Evaluación de la calidad del estudio
    - Extracción y seguimiento de datos
    - Síntesis de datos.
- Informe de la revisión.

2.4.2.2. Preguntas del caso de estudio

La pregunta del caso de estudio será la misma pregunta de investigación ¿Cómo la entidad podrá asegurar sus activos de información cumpliendo con los requerimientos de la estrategia de gobierno en línea?

2.4.2.3. Procedimientos a ser realizados

En la ejecución del caso de estudio, se utilizará la metodología propuesta en el artículo "Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO / IEC 27000" (Valencia-duque & Orozco-alzate, 2017), la cual contempla los siguientes pasos:

- Fase 1: Aprobación de la dirección para iniciar el proyecto
    - Establecimiento de las prioridades de la organización para desarrollar un SGSI
    - Definir el alcance preliminar del SGSI
    - Creación del plan de proyecto para ser aprobado por la dirección
- Fase 2: Definir el alcance, los límites y la política del SGSI
    - Definir el alcance
    - Definición de la política y objetivos de seguridad
    - Aprobación de la dirección
- Fase 3: Análisis de los requisitos de seguridad de la información
    - Identificar los activos dentro del alcance del SGSI
- Fase 4: Validación de riesgos y planificar el tratamiento de los riesgos
    - Establecimiento del contexto
        - Parámetros de probabilidad
        - Parámetros de impacto
        - Determinación de vulnerabilidad
        - Criterios de aceptabilidad del riesgo
    - Valoración de riesgo
        - Identificación de escenarios de riesgo
        - Estimación del riesgo
        - Evaluación del riesgo

    - Tratamiento del riesgo
- Fase 5: diseñar el SGSI
    - Documentación del sistema

Para el desarrollo de las actividades de cada fase, se tomarán como referencia adicional las guías de implementación propuestas por el MinTic en el MSPI.

2.4.2.4. Guía del reporte del estudio de caso

Cuando se concluya el diseño del SGSI, se compararán las conclusiones tanto de los casos estudiados, como del diseño realizado en la ejecución de este proyecto, y se darán recomendaciones sobre la implementación del plan a la entidad y propuestas de investigación a la comunidad científica.

3. REFERENTE TEÓRICO

3.1. Antecedentes

3.1.1. Implementación de sistemas de gestión de seguridad de la información

El nivel de acogida de estos modelos se puede medir con el número de certificados expedidos por entidades avaladas para tal fin, según las estadísticas ISO consultadas, en los países latinoamericanos el número de empresas certificadas tiende a subir con el paso del tiempo, a continuación, en la tabla 1 se presentan los 3 países con mayor número de certificaciones expedidas:

Tabla 1 Número de certificaciones acumuladas en ISO 27001 por año

País	AÑO									
	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
Brasil	10	25	40	48	41	50	53	82	85	94
Chile	2	3	7	10	13	18	23	24	24	32
Colombia	3	8	11	14	23	27	58	82	78	103

Fuente: (ISO, 2017)

Brasil, Chile y Colombia son los países con mayor tendencia al aumento de certificaciones en esta norma, lo anterior debido a que en cada uno de estos se han desarrollado políticas gubernamentales con miras al fortalecimiento de la industria tecnológica.

El gobierno de Brasil público en el 2011 su Estrategia nacional de Ciencia, tecnología e innovación, esta estrategia dentro de sus objetivos tiene, proporcionar un enfoque sistémico para el apoyo del Estado de la acción y el desarrollo de nuevos métodos e instrumentos de apoyo, colaboración, participación en el riesgo y la coordinación con los segmentos de negocio y sectores prioritarios para la promoción de la innovación (Ministerio de ciencia tecnología e innovación Brasil, 2012).

Para este punto se plantea el fortalecimiento del sector público en normatividad y buenas prácticas que ayuden a la estandarización estatal. En este documento las estrategias son:

- Gestión publica

- Nueva organización y gobiernos
- Promoción de la innovación en las empresas

Donde plantean la adopción de diferentes estándares internacionales en los cuales se encuentran ISO/IEC 27001, reconociendo su pertinencia en cuanto al aseguramiento de la información en entidades públicas del gobierno brasileño.

Por otra parte Chile, considerado el segundo país con mayor penetración de nuevas tecnología (The gA Center Digital Business Transformation, 2013), en su plan de gobierno a cargo de la presidenta Michelle Bachelet, expone como ejes fundamentales para el crecimiento: La formación y fortalecimiento del talento TI, así como la aplicación de buenas prácticas y adopción de estándares internacionales como premisa para ser atractivos internacionalmente; dentro de esta postura entra en juego marcos de trabajo en torno a la seguridad de la información siendo el más representativo para Chile la norma ISO/IEC 27001(Bachelet, 2013) .

Culminado la estadística está Colombia, este país contempla un detallado programa para el fortalecimiento de las tecnologías de la información tanto metodológicamente como jurídicamente, contempla temas como Gobierno abierto, trámites y servicios, gestión TI, seguridad y privacidad de la información, empezando por el CONPES de 1995, Gestión pública orientada a resultados, que tiene como propósito fundamental:

> Generar un cambio paulatino pero radical, en las entidades del estado hacia una nueva cultura de gestión pública orientada a resultados, en la cual el ciudadano sea el eje del desempeño de la administración y persiga permanentemente el mejor aprovechamiento de los recursos (DNP Departamento nacional de planeación., 1995, p. 16).

A partir de la anterior iniciativa, Colombia ha aunado esfuerzos por fortalecer la industria a través de diferentes programas, políticas e iniciativas, una de ellas fue lanzada en el 2008 conocida como GEL, que presenta dentro de sus estrategias un componente llamado

seguridad y privacidad de la información (MinTIC, 2015b), y el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia proporcionó el MSPI para la implementación del componente en las entidades públicas.

Respecto al nivel de implantación de Gobierno en línea según las estadísticas del MinTIC en el año 2016, en entidades del orden nacional como ministerios, entidades de salud y social en promedio el indicador de definición del plan está en 71%, mientras que la implementación se encuentra en el 56% como se evidencia en la tabla 2

Tabla 2 Índice GEL entes Nacionales año 2016

	Entidad/Indicador	**Definición TOTAL L.14**	**Implementación TOTAL L.15**
Defensa	CAJA DE RETIRO DE LAS FUERZAS MILITARES	37,5	27,5
Minas y Energía	COMISION DE REGULACION DE ENERGIA Y GAS -CREG-	87,5	100,0
Defensa	DIRECCION GENERAL DE LA POLICIA NACIONAL	93,8	56,7
Hacienda y Crédito Público	FINANCIERA DE DESARROLLO TERRITORIAL S.A. FINDETER	97,2	83,3
Defensa	INDUSTRIA MILITAR	100,0	100,0
Cultura	INSTITUTO COLOMBIANO DE ANTROPOLOGIA E HISTORIA	0,0	6,7
Educación	INSTITUTO COLOMBIANO DE CRÉDITO EDUCATIVO Y ESTUDIOS TÉCNICOS EN EL EXTERIOR - ICETEX	87,5	100,0

Estadísticas	INSTITUTO GEOGRAFICO AGUSTIN CODAZZI	39,6	46,7
Transporte	SUPERINTENDENCIA DE PUERTOS Y TRANSPORTE	89,6	100,0
Trabajo	UNIDAD ADMINSITRATIVA ESPECIAL DEL SERVICIO PUBLICO DE EMPLEO	34,7	28,3

Fuente: (MinTIC, 2017b)

En este mismo estudio de medición se clasificaron de la misma forma las entidades territoriales (Gobernaciones y alcaldías) en la tabla 3:

Tabla 3 Índice GEL entes territoriales

Departamento	**Nombre Institución**	**L14 Definición**	**L15 Implementación**
Cauca	Gobernación de Cauca	15	0
Magdalena	Gobernación de Magdalena	9	67
Risaralda	Gobernación de Risaralda	68	67
Chocó	Gobernación de Chocó	19	0
Santander	Gobernación de Santander	24	67
Norte de Santander	Gobernación de Norte de Santander	39	67
Córdoba	Gobernación de Córdoba	76	100
Tolima	Gobernación de Tolima	12	67
Nariño	Gobernación de Nariño	51	100
Cesar	Gobernación de Cesar	84	100
Arauca	Gobernación de Arauca	38	100
Antioquia	Gobernación de Antioquia	91	67

Amazonas	Gobernación de Amazonas	28	33

Fuente: (MinTIC, 2017a)

Según la información anterior se puede apreciar que las entidades de orden territorial y nacional han hecho grandes esfuerzos por poner en marcha los lineamientos presentados por Gobierno en línea, velando por la seguridad y privacidad de la información, la cual es definida como "las acciones transversales tendientes a proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada" (MinTIC, 2015b, p. 34).

Además de dar cumplimiento con lo anterior, las entidades del estado deben aplicar de forma mandataria el Decreto Único Reglamentario 1078 de 2015 (MinTIC, 2015a) por medio del cual se regula el sector de tecnologías de la información y las comunicaciones, en el Título 9. Capítulo 1 se presentan todos los puntos a tener en cuenta en la implementación: los responsables, líderes y presupuestos, en el Artículo 2.2.9.1.3.2 se presentan los plazos, mostrando que para el 2016 y 2017 se espera una ejecución del 80% y para el 2020 un sostenimiento total del sistema.

3.2. Revisión sistémica de literatura

Con el fin de reunir la mayor cantidad de información de forma exhaustiva e imparcial sobre el eje temático del proyecto, se realiza un revisión sistémica de literatura (en adelante SLR) siguiendo las pautas descritas por Barbara Kitchenham en el informe técnico *"Procedures for Performing Systematic Reviews"* (Kitchenham, 2004), en este se exponen diferentes metodologías y se hacen algunas recomendaciones referentes a la aplicación de SLR a diferentes contextos, para el caso que nos ocupa abordaremos los siguientes pasos:

- Planificación de la revisión
- Ejecución la revisión
- Informe de la revisión

3.2.1. Planificación de la revisión

Primero se hace la Identificación de la necesidad de una revisión, dado que uno de los objetivos del proyecto contempla llevar a cabo una revisión sistémica de literatura de los

sistemas de gestión seguridad de la información a nivel internacional, para tal fin se pretende con este ejercicio recopilar de forma juiciosa la información existente en cuanto a:

- Metodologías de diseño e implementación de SGSI en entidades.
- Recomendaciones de anteriores ejercicios en cuanto a diseño e implementación de SGSI.
- Conclusiones dadas en ejercicios pasados.
- Oportunidades de mejora o vacíos en investigación expuestos en anteriores estudios.
- Grados de éxito o fracaso de implementaciones de SGSI en entidades.

Luego, para el desarrollo de un protocolo de revisión se tienen en cuenta los siguientes puntos:

- Pregunta de investigación ¿Cómo se han implementado y diseñado Sistemas de gestión de seguridad de la información en entidades?

  El responder esta pregunta proporciona la base existente en cuanto a la información en el tema que nos ocupa y deja claro en qué punto se puede aportar.

- Revisión del protocolo: La revisión del protocolo es revisada por el asesor de la tesis.

3.2.2. Ejecución de la revisión

Con el objetivo de encontrar la mayor cantidad de estudios primarios relacionados con la pregunta, se pretende que la estrategia de búsqueda sea imparcial y conserve el rigor necesario, para lo cual se desarrollan los puntos contenidos en la tabla 4:

Tabla 4 Puntos de ejecución del SLR

Pregunta a resolver	
	Pregunta de investigación ¿Cómo se han implementado y diseñado Sistemas de gestión de seguridad de la información en entidades? Preguntas de apoyo

	- Variables para la implementación de SGSI - ¿Cuál fue el enfoque metodológico? - Recomendaciones de cómo Implementar un SGSI - ¿Cómo se ha validado el modelo?
Términos y combinaciones de búsqueda	
	Palabras clave (Con base en el título y la temática) **Términos (Las búsquedas se hacen en español e inglés)** - Sistemas de gestión de seguridad de la información - SGSI - Entidades - Empresas - Metodología - MSPI - Implementación - PHVA - Sistemas de gestión - Riesgos TI - Metodologías - Metodologías de riesgos de TI - Seguridad de la información - ISO 2700* (27001-27002- 27003-27005). **Combinaciones** Sistemas de gestión de seguridad de la información and Entidades. Sistemas de gestión de seguridad de la información and Empresas Sistemas de gestión de seguridad de la información and Metodología Implementación and Sistemas de gestión de seguridad de la información Metodología and seguridad de la información ISO 2700* (27001-27002- 27003-27005) and empresas. PHVA (PDCA) and seguridad de la información.

	MSPI and entidades. Seguridad de la información and empresas SGSI and empresas Implementación and SGSI Metodologías de riesgos de TI and empresas Sistemas de gestión and seguridad de la información. Empresas and riesgo TI. Caso de estudio and implementación SGSI. 27000 and empresas o entidades 27000 and implementación practice 27000
Bases de datos / Fuentes	
	- SCIENCE DIRECT - SCOPUS - EBSCO - BDCOL- BIBLIOTECA DIGITAL COLOMBIANA - SCIELO - REDALYC - GOOGLE ACADÉMICO ** Informes técnicos ** Trabajos en curso ** Actas de congresos (Ponencias y experiencias significativas). ** Consulta a expertos (Profesionales con experiencia en implementación de SGSI en entidades públicas).
Rango de fechas	
	Artículos o estudios hecho y/o publicados desde el 2010 al 2017
Proceso de gestión bibliográfica	
	El software para gestionar la bibliografía en centrada en la revisión es Mendeley ya que presenta las siguientes características:

	Extracción automática de metadatos de documentos PDF. Visor de documentos PDF con notas adhesivas, selección de texto y lectura a pantalla completa. Búsqueda completa de texto a través de documentos. Citas y bibliografías en Microsoft Word, OpenOffice y LibreOffice. Compartir y colaborar en grupo, anotaciones en los documentos. Estadísticas sobre los documentos, autores y publicaciones más leídas.
Documentación de la búsqueda.	
	Con el fin de cumplir el objetivo de que la revisión sistemática sea transparente y replicable, se propone la siguiente plantilla la cual se debe alimentar con cada búsqueda. Campos plantilla: Identificador - Fecha de búsqueda (fecha y hora) – Filtro de la BD científica (este campo es opcional) – Base de datos (Nombre de la base de datos o fuente) – Titulo (Titulo del articulo) – Autor (Nombre del autor o autores) – Palabras clave (o su combinación) – Resumen (Abstract) – Aporte (Pequeño resumen que muestra el aporte de este articulo al SLR) – Link/Ubicación (Donde se puede encontrar en el futuro).
Consolidación documentos primarios	
	Total documentos: 24 entre artículos y proyectos de implementación
Criterios de selección	
	Identificar aquellos estudios primarios que proporcionan evidencia directa sobre la pregunta de investigación o las preguntas de apoyo que se plantearon. Para la selección se realizaron las inspecciones a todos los estudios primarios seleccionados utilizando el siguiente método: <u>Primera pasada:</u> Lectura con detenimiento del título, el resumen, y la introducción. Lectura de los encabezados de las secciones y sub secciones ignorando el resto. Ojeada al contenido formal

Lectura de las conclusiones

Ojeada de las referencias.

Se pretende buscar si el artículo podría dar alguna contribución a la pregunta de investigación planteada o si definitivamente tiene otro contexto.

<u>Segunda pasada:</u>

Lectura del artículo con atención

Atención a las figuras y tablas y referencias desconocidas.

Comprensión del artículo en su totalidad.

Identificación de puntos fuertes y puntos débiles

Comprender, evaluar y revisar el artículo.

Se intentan resolver algunas de estas preguntas.

¿Cuáles son los aportes del artículo?

¿Qué es lo nuevo?

¿Una pregunta?

¿Un enfoque?

¿Una metodología?

¿Un algoritmo?

¿Evidencia?

¿Casos de estudio?

¿Cuáles son las conclusiones?

¿Qué se aprendió del artículo?

¿Impacta las prácticas actuales?

¿Son generalizables los resultados?

¿Quedan preguntas abiertas?

El trabajo:

- ¿Permite aplicaciones?
- ¿Profundiza en el conocimiento?
- ¿Explora un nuevo espacio de investigación?

	RESUMEN: Motivación Contribución Metodología/argumentos Conclusiones Dar una calificación de calidad y clasificar los estudios en grupos por calidad.
Validación	
	La validación de los resultados se realiza por medio del asesor de la tesis.

Fuente: Propia

3.2.3. Resultados de la revisión

A partir de la información del Anexo "Artículos encontrados" se tienen 34 Artículos que cumplieron con los criterios de búsqueda, distribuidos en las bases de datos, tal como se puede observar en la tabla 5:

Tabla 5 Artículos encontrados por base de datos

BD	Total
Ebsco	2
Redalyc (Libre Acceso)	1
ScienceDirect	31
Total general	**34**

Fuente: Los autores

Estos artículos fueron analizados y filtrados según un posible aporte al SLR, con lo cual se redujeron los resultados a 19 estudios primarios, a partir de la información del anexo "Estudios primarios"

Para el último filtro, se utilizaron las preguntas a resolver planteadas en la estrategia de búsqueda, con lo cual se encontraron 13 artículos a partir de la información del anexo "Estudios seleccionados", clasificados según su enfoque de investigación en la tabla 6:

Tabla 6 Artículos por enfoque de investigación

Enfoque de investigación	Total
TOPICO: Conciencia empleados - clima organizacional.	6
TOPICO: Implementación de un SGSI	5
TOPICO: Riesgos: evaluación de su inversión.	1
TOPICO: gestión del conocimiento en cuanto a la seguridad de la información.	1
Total general	**13**

Fuente: Los autores

La información más relevante encontrada en la revisión es la siguiente:

El principal tópico tratado dentro de la literatura es la importancia de la consciencia de las personas y el clima organizacional para la implementación de un Sistema de Gestión de Seguridad de la Información en una entidad, para mejorar estos temas se proponen diferentes metodologías que ayudan a clasificar los usuarios y de esta forma realizar planes segmentados según la necesidad de cada cultura, por ejemplo (Chan, Woon, & Kankanhalli, 2005), explica que la supervisión directa y la socialización de compañeros es positivamente relacionada con la percepción de seguridad de la información, con lo cual propone crear un clima organizacional mediante la participación de todos los niveles(gerenciales, intermedios y operativos), por otro lado (Bauer, Bernroider, & Chudzikowski, 2017), proporciona una serie de premisas que se deben respetar para el diseño de programas que incentiven la seguridad de la información:

- Implementar un sistema que se evalúe periódicamente con marcos de referencia conocidos (ej. COBIT)
- Realizar pruebas de penetración de ingeniería social
- Utilizar enfoques creativos que mejoren la participación emocional de los empleados
- Uso de lenguaje común y vocabulario amigable
- Personalizar los programas para grupos de usuarios y áreas

Con respecto a las decisiones de inversión sobre controles de seguridad de la información, (Dor & Elovici, 2016) propone una metodología para tomar decisiones en cuanto a la inversión de seguridad de la información, por medio de la participación de todas las áreas y evaluando las opciones sin verse sesgado por percepciones personales o motivaciones de cada área, con un modelo conceptual con una lista de verificación en 14 fases y aclara conceptos comunes a tener en cuenta.

En cuanto a las implementaciones de un SGSI se contemplan diferentes escenarios, en Taiwán (Ku, Chang, & Yen, 2009) expone la política gubernamental en cuanto a seguridad de la información y da a conocer el caso de una entidad pública que implementó la norma ISO 27001 de forma autónoma, este caso contempla una entidad financiera del estado que decir auto implementar el modelo a partir de las siguientes fortalezas:

- Conocimiento de Sistemas de Gestión, experiencia en certificación ISO 9001
- Evaluación costo/beneficio en cuanto a la contratación de un asesor externo y la curva de aprendizaje de los procesos contra el entrenamiento interno del personal encargado
- Alto nivel de documentación de los procesos y un sistema de gestión de riesgos implementado
- Alto apoyo de la gerencia y cultura organizacional

Otro caso de implementación fue evaluado en Turquía, donde se pretendía evaluar el nivel de implementación de los SGSI (Ozkan & Karabacak, 2010) tomó como base 5 empresas y evaluó mediante encuestas los niveles de implementación y los posibles factores de fracaso de estos proyectos, encontró que sólo una de ellas implementó el sistema con éxito con ayuda de sus procesos bien definidos y su alta autonomía, las otras 4 presentaron problemas principalmente por la legislación vigente y por el bajo apoyo de los niveles directivos.

Por último tenemos a (Said, Abdullah, Uli, & Mohamed, 2014), el cual evaluó la gestión del conocimiento en implementaciones de los SGSI, encontró que la cultura es una barrera importante para la transferencia de conocimiento, también evidenció que las recompensas e incentivos tienen una influencia positiva en el tratamiento de incidentes de seguridad de la información.

3.3. Marco legal

El marco legal se divide entre el marco jurídico de la estrategia de Gobierno en Línea, Gobierno abierto y Gestión de TI

3.3.1. Marco jurídico institucional de la estrategia de Gobierno en Línea

La estrategia de Gobierno en línea inició con la Agenda de conectividad – CONPES 3072 del 2000, la cual establece como objetivo *"*Proveer al estado la conectividad que facilite la gestión en línea de los organismos gubernamentales y apoye su función de servicio al ciudadano*"* (MinTIC, 2000, p. 12), presentó las tecnologías de la información y comunicación para la competitividad de los países en desarrollo, la situación actual en infraestructura de información, computacional y social, así como los objetivos de la agenda que fueron promover un ambiente favorable e impacto en la comunidad, el sector productivo y el estado mediante las estrategias de:

- Acceso a la infraestructura de la información.
- Uso de TI en los procesos educativos y capacitación en el uso de las TI.
- Uso de TI en las empresas.
- Fomento de la industria nacional de TI.
- Generación de contenido
- Gobierno en línea

Luego de esto, se reglamentó el Decreto 1078 de 2015, Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. En su título 9 Políticas y lineamientos de tecnologías de la información, Capitulo 1: Estrategia GEL, presenta como objetivo Definir el ámbito de aplicación, definiciones, principios, fundamentos y propósitos fundamentales:

> "Artículo 2.2.9.1.1.2. Ámbito de aplicación. Serán sujetos obligados de las disposiciones contenidas en el presente capítulo las entidades que conforman la Administración Pública en los términos del artículo 39 de la Ley 489 de 1998 y los particulares que cumplen funciones administrativas" (MinTIC, 2015a, p. 134).

Sus fases de cumplimiento contemplan información en línea, interacción, transacción, transformación y democracia en línea con los siguientes componentes: Tics para servicios, gobierno abierto, para gestión y seguridad y privacidad de la información.

Los plazos contemplados para entes nacionales y territoriales se encuentran en la tabla 7 y tabla 8 respectivamente:

Tabla 7 Plazos de implementación GEL entes nacionales

Componente / Año	2015	2016	2017	2018	2019	2010
TIC para servicios	90%	100%	Mantener 100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para gobierno abierto	90%	100%	Mantener 100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para gestión	25%	50%	80%	100%	Mantener 100%	Mantener 100%
Seguridad y privacidad para la información	40%	60%	80%	100%	Mantener 100%	Mantener 100%

Fuente: (MinTIC, 2015a, p. 138)

Tabla 8 Plazos de implementación GEL entes territoriales

Componente/ año	Entidades A (%)						Entidades B (%)						Entidades C (%)					
	2015	2016	2017	2018	2019	2020	2015	2016	2017	2018	2019	2020	2015	2016	2017	2018	2019	2020
TIC para servicios	70	90	100	100	100	100	45	70	100	100	100	100	40	55	70	100	100	100
TIC para gobierno abierto	80	95	100	100	100	100	65	80	100	100	100	100	65	75	85	100	100	100
TIC para gestión	20	45	80	100	100	100	10	30	50	65	80	100	10	30	50	65	80	100
Seguridad y privacidad de la información	35	50	80	100	100	100	10	30	50	85	80	100	10	30	50	65	80	100

Fuente: (MinTIC, 2015a, p. 139)

3.3.2. Gobierno abierto

El Gobierno abierto comenzó con la Ley 1712 de 2014, también conocida como Ley de transparencia y del derecho de acceso a la información política nacional, la cual tiene como objetivo:

> *"Regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información"* (Congreso de la República, 2014, p. 1)

Esta ley define los principios de transparencia y acceso a la información, algunos de ellos son: transparencia, buena fe, facilitación, gratuidad, eficiencia, calidad de la información y Principio de divulgación proactiva de la información: Obligación de respuesta a las solicitudes de la sociedad y la publicación de información correspondiente a la actividad estatal de forma rutinaria y proactiva (Congreso de la República, 2014).

Los funcionarios públicos están en la obligación de publicar las actividades y resultados de su gestión con fin de cuidar la transparencia pública y el conocimiento por parte del

ciudadano, por ejemplo: informes de gestión, procedimientos internos y externos, mecanismos de control, etc.

Se deben proporcionar los medios para esta actividad como sistema de información, adopción de metodologías de manejo documental y archivo.

3.3.3. Gestión Ti

La Ley 1581 de 2012 contempla las disposiciones generales de habeas data y se regula el manejo de la información, en conjunto con los decretos 1377 del año 2013 y el 886 del año 2014, su objetivo es:

> Desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países (Congrerso de Colombia, 2012)

Para su aplicabilidad se deben respetar los siguientes principios de forma integral:

- Principio de veracidad o calidad de los registros o datos
- Principio de finalidad.
- Principio de circulación restringida
- Principio de temporalidad de la información
- Principio de interpretación integral de derechos constitucionales
- Principio de seguridad

Los titulares de la información tendrán derecho a:

- Restringir el acceso
- Solicitar cambios, actualizaciones y eliminación.
- Solicitar pruebas de su autorización de divulgación o compartimiento

3.4. Marco referencial

Para el desarrollo de este proyecto, tomaremos como base la documentación contenida en la familia de normas de la ISO 27000, puntualmente la ISO 27001, ISO 27002, ISO 27003 e ISO 27005. Adicional a esto, también se tendrá en cuenta la información ofrecida por el MINTIC para el componente de seguridad de la información por medio del MSPI

3.4.1. ISO 27001

La norma ISO 27001 (ISO/IEC, 2013b) contiene los requisitos que se deben tener en cuenta para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (en adelante SGSI), para ello define los siguientes componentes:

- Contexto de la organización
- Liderazgo
- Planificación
- Soporte
- Operación
- Evaluación del desempeño
- Mejora

3.4.2. ISO 27002

La guía ISO 27002 (ISO/IEC, 2013a) proporciona directrices para la seguridad de la información organizacional y las prácticas de gestión de seguridad de la información en las actividades de selección, implementación y gestión de controles. La guía contiene 14 numerales de control que contiene 35 categorías de seguridad y 114 controles. Los numerales y categorías se muestran en la tabla 9:

Tabla 9 Controles de la norma ISO 27002

Numerales	Categorías
Políticas de seguridad de la información	directrices establecidas por la dirección para la seguridad de la información
Organización de la seguridad de la información	organización interna
	dispositivos móviles y teletrabajo
Seguridad del recurso humano	antes de asumir el empleo
	durante la ejecución del empleo
	terminación y cambio de empleo
Gestión de activos	responsabilidad por los activos
	clasificación de la información
	manejo de medios
Control de acceso	requisitos del negocio para control de acceso
	gestión de acceso de usuarios
	responsabilidades de los usuarios
	control de acceso a sistemas y aplicaciones
Criptografía	controles criptográficos
Seguridad física y del entorno	áreas seguras
	Equipos
seguridad de las operaciones	procedimientos operacionales y responsabilidades
	protección contra códigos maliciosos
	copias de respaldo
	registro (logging) y seguimiento
	control de software operacional
	gestión de la vulnerabilidad técnica
	consideraciones sobre auditorías de sistemas de información
Seguridad de las comunicaciones	gestión de la seguridad de las redes
	transferencia de información
Adquisición, desarrollo y mantenimiento de sistemas	requisitos de seguridad de los sistemas de información
	seguridad en los procesos de desarrollo y soporte

	datos de prueba
Relaciones con los proveedores	seguridad de la información en las relaciones con los proveedores
	gestión de la prestación de servicios de proveedores
Gestión de incidentes de seguridad de la información	gestión de incidentes y mejoras de la seguridad de la información
Aspectos de seguridad de la información de la gestión de continuidad del negocio	continuidad de seguridad de la información
	Redundancias
Cumplimiento	cumplimiento de requisitos legales y contractuales
	revisiones de seguridad de la información

Fuente: (ISO/IEC, 2013a)

3.4.3. ISO 27003

La norma ISO 27003 (ISO/IEC, 2007) Contiene las actividades necesarias para el diseño e implementación de un SGSI a partir de los requisitos de la norma ISO 27001. La norma está organizada con los siguientes numerales y sus respectivas actividades:

- **Obtener aprobación de la dirección para iniciar el proyecto de SGSI:** Está compuesto por el panorama general para la obtención de la aprobación de la dirección para iniciar el proyecto SGSI, aclaración de las prioridades de la organización para desarrollar un SGSI, definir el alcance preliminar del SGSI, crear el caso de negocio y el plan de proyecto para la aprobación por la dirección (ISO/IEC, 2007).
- **Definir el alcance del SGSI y la política del SGSI:** Está compuesto por el panorama general de la definición del alcance, los límites y la política del SGSI, definir el alcance y los límites de la organización, definir el alcance y los límites de las tecnologías de la información y las comunicaciones(en adelante TIC), definir el alcance y los límites físicos, desarrollar la política del SGSI y obtener la aprobación de la dirección (ISO/IEC, 2007).
- **Realizar un análisis de la organización:** Comprende el panorama general de la realización del análisis de los requisitos de seguridad de la información, definir los requisitos de seguridad de la información para el proceso del SGSI, identificar los

activos dentro del alcance del SGSI y realizar una evaluación de la seguridad de la información (ISO/IEC, 2007).

- **Llevar a cabo la evaluación de riesgos y el plan de tratamiento de los riesgos:** Se compone por el panorama general de la realización de la valoración de riesgos y la planificación del tratamiento de riesgos, realizar la valoración de riesgos, seleccionar los objetivos de control y los controles y obtener la autorización de la dirección para implementar y operar un SGSI (ISO/IEC, 2007).
- **Diseñar el SGSI:** Está compuesto por el panorama general del diseño del SGSI, diseñar la seguridad de la información de la organización, diseñar la seguridad de información física y de las TIC, diseñar la seguridad de la información específica de un SGSI y producir el plan del proyecto final de SGSI (ISO/IEC, 2007).

3.4.4. ISO 27005

La norma ISO 27005 (ISO/IEC, 2008) contiene las directrices a utilizar para la gestión de riesgos de la seguridad de la información, está compuesta por las siguientes actividades:

- **Establecimiento del contexto:** Está compuesto por las consideraciones generales, los criterios básicos, el alcance, los límites y la organización para la gestión del riesgo en la seguridad de la información (ISO/IEC, 2008).
- **Valoración del riesgo en la seguridad de la información:** Para el desarrollo de esta actividad primero se realiza la identificación de los activos de información, luego la Identificación de las amenazas, posteriormente la identificación de controles existentes y planificados, luego la identificación de las vulnerabilidades, la estimación del riesgo, la evaluación de las consecuencias, evaluación de la probabilidad de incidentes, definir el nivel de estimación del riesgo y por último realizar la evaluación del riesgo, la cual consiste en comparar los niveles de riesgo frente a los criterios de evaluación y sus criterios de aceptación, con las cuales se priorizan los riesgos y se ordenan a partir de su valor respectivo (ISO/IEC, 2008).
- **Tratamiento del riesgo de la seguridad de la información:** Para el tratamiento de los riesgos, la norma ISO 27005 (ISO/IEC, 2008) menciona cuatro opciones para el tratamiento del riesgo, las cuales son reducir el riesgo, retenerlo, evitarlo y transferirlo, descritos a continuación:

- ✓ Reducir el riesgo: Consiste en seleccionar controles que permitan disminuir la probabilidad de ocurrencia o el impacto que pueden llegar a generar en caso de materializarse (ISO/IEC, 2008). Los controles pueden ser consultados en la norma ISO 27002.
- ✓ Retener el riesgo: También llamado como aceptar del riesgo, consiste en la decisión de mantener el riesgo sin ninguna acción, la cual debe ser comparada con la evaluación del riesgo(ISO/IEC, 2008).
- ✓ Evitar el riesgo: Esta opción corresponde a evitar la actividad o acción que da origen al riesgo, normalmente se utiliza cuando la evaluación del riesgo es muy alta, o los costos para implementar los controles exceden los beneficios de su implementación (ISO/IEC, 2008).
- ✓ Transferir el riesgo: Consiste en delegar el riesgo a otra de las partes de la organización, para que pueda gestionarlo de manera más eficaz (ISO/IEC, 2008).

- **Aceptación de los riesgos de la seguridad de la información:** Consiste en la revisión del plan de tratamiento de los riesgos y la evaluación del riesgo residual, para que sea aceptado por la dirección de la organización de manera formal (ISO/IEC, 2008).
- **Comunicación de los riesgos para la seguridad de la información:** La información obtenida sobre los riesgos debe ser intercambiada entre la persona que toma las decisiones y las demás partes involucradas, esto se hace con el fin de brindar seguridad del resultado de la gestión del riesgo, recolectar información, compartir los resultados, evitar o reducir la ocurrencia e impacto de las brechas de seguridad de la información, brindar soporte para la toma de decisiones, coordinar y planificar acciones, y dar un sentido de responsabilidad acerca de los riesgos (ISO/IEC, 2008).
- **Monitoreo y revisión del riesgo en la seguridad de la información:** Está compuesta por el monitoreo y revisión de los factores de riesgo y el monitoreo, revisión y mejora de la gestión del riesgo (ISO/IEC, 2008).

3.4.5. Modelo de seguridad y privacidad de la información de MinTIC

El Modelo de seguridad y privacidad de la información (MSPI) es un documento elaborado para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo de la seguridad de la información (MinTIC, 2015c), alineado con la estrategia de GEL

Este modelo incluye un conjunto de guías en cada una de sus fases, para tener claridad sobre los resultados a obtener y cómo lograrlos, teniendo como su objetivo principal generar un documento de lineamientos de buenas prácticas en un SGSI para las entidades del estado, apuntando al componente de seguridad y privacidad de la información de Gobierno en Línea (MinTIC, 2015c).

El MSPI está compuesto por cinco fases, las cuales permiten que las entidades puedan gestionar la seguridad y privacidad de los activos de información (MinTIC, 2015c). Las fases son:

- Diagnóstico
- Planeación
- Implementación
- Evaluación de Desempeño
- Mejora continua

Para efectos de este proyecto se profundizará en el alcance de las fases de diagnóstico y planificación.

3.4.5.1. Fase de Diagnóstico

En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del MSPI, con las siguientes metas:

- Estado actual de la entidad
- Identificación del nivel de madurez
- Levantamiento de información

3.4.5.2. Fase de Planificación

Consiste en elaborar el plan de seguridad y privacidad de la información alineada con el objetivo misional de la entidad, definiendo las acciones a implementar a nivel de seguridad y privacidad de la información a través de una metodología del riesgo, está compuesta por las siguientes secciones (MinTIC, 2015c):

- Contexto de la entidad: Corresponde a entender la entidad, necesidades y expectativas de las partes interesadas y determinar el alcance del MSPI.
- Liderazgo: Se compone del liderazgo y compromiso de la alta dirección, la política de seguridad, roles de la entidad, responsabilidades y autoridad.
- Planeación: Comprende las acciones para abordar los riesgos, oportunidades, objetivos y planes para lograrlos.
- Soporte: Se compone por los recursos, competencias, sensibilización, comunicación y documentación.

Por medio de la fase de Planeación, se tiene como objetivo cumplir con los siguientes ítems (MinTIC, 2015c):

- Política de seguridad y privacidad de la información
- Procedimientos de seguridad y privacidad de la información
- Roles y responsabilidades de seguridad y privacidad de la información
- Inventario de activos de información
- Integración del MSPI con el sistema de gestión documental
- Identificación, valoración y tratamiento de riesgos
- Plan de comunicaciones
- Plan de transición de Ipv4 a IPv6

Para el desarrollo de la fase de planificación, el MinTIC proporciona el apoyo de las siguientes guías (MinTIC, 2015c):

- Guía N° 2 - Política General del MSPI
- Guía N° 3 - Procedimientos de seguridad y privacidad de la información
- Guía N° 4 - Roles y responsabilidades de seguridad y privacidad de la información
- Guía N° 5 - Gestión de activos
- Guía N° 7 - Gestión de riesgos
- Guía N° 8 - Controles de seguridad

3.5. Marco conceptual

A efectos de dar claridad en torno a los diversos conceptos desarrollados en el proyecto, se tomará como base aquellos términos establecidos en las normas de la familia ISO 27000.

Acción correctiva: Es la acción que se ejecuta para eliminar la causa de una no conformidad y evitar que se repita (ISO/IEC, 2016).

Amenaza: Posible causa de un incidente no deseado, que puede dañar un sistema u organización (ISO/IEC, 2016).

Ataque: Consiste en un Intento de inhabilitar, robar, destruir, exponer, alterar, obtener acceso no autorizado o hacer uso no autorizado de un activo (ISO/IEC, 2016).

Atributo: Propiedad o característica de un objeto, que puede distinguirse cualitativa o cuantitativamente por medios automatizados o humanos (ISO/IEC, 2016).

Auditoría: Proceso documentado, independiente y sistemático para obtener evidencias y evaluar en qué medida se cumplen los criterios de manera objetiva (ISO/IEC, 2016).

Autenticación: Garantía de que una característica solicitada por una entidad es correcta(ISO/IEC, 2016).

Confidencialidad: Propiedad que determina que la información sólo esté disponible y sea mostrada a entidades, individuos o procesos autorizados (ISO/IEC, 2016).

Confiabilidad: Propiedad que expresa el nivel de consistencia de un comportamiento y los resultados esperados (ISO/IEC, 2016).

Control: Consiste en procesos, políticas, dispositivos, prácticas u otras acciones para modificar un riesgo (ISO/IEC, 2016).

Control de acceso: Corresponde a los medios utilizados para que el acceso a los activos esté restringido y autorizado en función a los requisitos (ISO/IEC, 2016).

Corrección: Es la acción para eliminar una no conformidad detectada en una auditoría (ISO/IEC, 2016).

Criterios de decisión: Umbrales utilizados para describir el nivel de confianza de un resultado dado, o para determinar la necesidad de actuar con respecto a una situación (ISO/IEC, 2016).

Criterios de riesgo: Se definen como los términos de referencia para evaluar y determinar la importancia de un riesgo (ISO/IEC, 2016).

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada cuando ésta la solicite (ISO/IEC, 2016).

Evaluación del riesgo: Proceso de comparación entre el análisis de riesgos y el criterio de riesgos para determinar si el riesgo o su magnitud son aceptables (ISO/IEC, 2016).

Evento de seguridad de la información: Se define como un posible incumplimiento en la política de seguridad de la información o falla de un control de un sistema, servicio o estado de la red (ISO/IEC, 2016).

Gestión del riesgo: Conjunto de actividades coordinadas para dirigir y controlar los riesgos de una organización (ISO/IEC, 2016).

Identificación de riesgos: Proceso para encontrar, reconocer y describir los riesgos (ISO/IEC, 2016).

Impacto del riesgo: Resultado de un evento que afecta los objetivos (ISO/IEC, 2016).

Incidente de seguridad de la información: Evento o eventos no deseados o inesperados de seguridad de la información que puedan amenazar la seguridad de la información y con probabilidad de comprometer las operaciones comerciales (ISO/IEC, 2016).

Indicador: Medida que evalúa atributos especificados para controlar los objetivos, riesgos y problemas de una organización (ISO/IEC, 2016).

Integridad: propiedad de salvaguardar la exactitud y estado completo de la información (ISO/IEC, 2016).

Mejora continua: Actividad periódica para mejorar el rendimiento (ISO/IEC, 2016).

Nivel de riesgo: Magnitud de un riesgo en términos de la combinación de probabilidad e impacto (ISO/IEC, 2016).

No conformidad: Incumplimiento de un requisitos (ISO/IEC, 2016).

Objetivo: Se define como el resultado propuesto a ser alcanzado (ISO/IEC, 2016).

Objetivo de control: Corresponde a la descripción de los resultados que se esperan lograr con la implementación de controles (ISO/IEC, 2016).

Organización: Grupo de personas con funciones, responsabilidades, autoridades e interrelaciones que buscan alcanzar unos objetivos organizacionales (ISO/IEC, 2016).

Política: Conjunto de expectativas y lineamientos expresados formalmente por la alta dirección de una organización (ISO/IEC, 2016).

Proceso: Conjunto de actividades que interactúan entre sí para convertir los insumos en productos (ISO/IEC, 2016).

Probabilidad: Posibilidad de que algo suceda (ISO/IEC, 2016).

Proceso de gestión del riesgo: Se define como la aplicación sistemática de las políticas de gestión, procedimientos y prácticas a las actividades de comunicar, consultar, establecer e identificar el contexto, analizar, evaluar, tratar, monitorear y revisar los riesgos (ISO/IEC, 2016).

Propietario del riesgo: Persona, área o entidad con la responsabilidad y autoridad para manejar un riesgo (ISO/IEC, 2016).

Requerimiento: Son las necesidades o expectativas que deben ser alcanzadas, de manera implícita o de obligatorio cumplimiento (ISO/IEC, 2016).

Riesgo: Efecto de la incertidumbre de una situación sobre los objetivos (ISO/IEC, 2016).

Riesgo residual: Riesgo restante generado por el resultado del tratamiento de riesgo (ISO/IEC, 2016).

Seguridad de la información: Consiste principalmente en salvaguardar la confidencialidad, disponibilidad e integridad de la información (ISO/IEC, 2016)

Sistema de gestión: Se define como un conjunto de elementos organizacionales (tales como la estructura, roles, responsabilidades, etc.) relacionados entre sí, para establecer políticas, objetivos y procesos para alcanzar los objetivos (ISO/IEC, 2016).

Sistema de gestión de seguridad de la información: La norma ISO/IEC 27000 (ISO/IEC, 2016) lo define como el conjunto de políticas, procedimientos, directrices, recursos y actividades de una organización, para proteger sus activos de información a través del ciclo de monitorear, revisar, mantener y mejorar continuamente la seguridad de la información para alcanzar los objetivos de negocio

Stakeholder: Persona u organización que puede afectar o verse afectada por una decisión o actividad (ISO/IEC, 2016).

Tratamiento del riesgo: Proceso para modificar el riesgo (ISO/IEC, 2016).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas (ISO/IEC, 2016).

4. PROPUESTA DEL DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA ENTIDAD

Con el objetivo de mantener la confidencialidad de la información de la entidad, el detalle de los resultados se encuentra en los anexos, y en el informe se mostrará el resumen de cada uno de los resultados objetivos en este proyecto.

4.1. Alcance, límites y política del SGSI

4.1.1. Alcance y límites del SGSI

Para determinar el alcance del Sistema de Gestión de Seguridad de la Información, inicialmente se realizó una revisión de los procesos de la entidad, posteriormente se recibió una inducción sobre la estructura documental de los procesos del Sistema Integrado de Gestión por parte de un funcionario.

Posteriormente, se hizo un análisis de los procesos para determinar el alcance de los procesos del SGSI enfocados en la misión de la entidad, por medio de una reunión con el Director, Para la definición del alcance se planteó la siguiente pregunta: ¿Cuál es la información más crítica manejada en la entidad?

Para dar respuesta se tomaron en cuenta los criterios de disponibilidad, integridad, y confidencialidad, para lo cual el representante de la Dirección por parte de la entidad decide que la información financiera es la que se considera más crítica.

4.1.2. Política de seguridad y privacidad de la información

Para la definición de la política de seguridad y privacidad de la información de la entidad se tomó como base la "Guía para la elaboración de la política general de seguridad y privacidad de la información" (MinTIC, 2016) la cual tiene los aspectos más importantes a tener en cuenta, la Política para la entidad se encuentra en el anexo "Política de seguridad y privacidad de la información de la entidad"

4.2. Análisis de los requisitos de seguridad de la información

4.2.1. Activos de información

Para la identificación y clasificación de los activos de información se tomó como base la "Guía para la Gestión y Clasificación de Activos de Información" del MinTic, con la cual se recolectaron los siguientes datos para cada activo (MinTic, 2016):

- Identificador
- Proceso
- Nombre de Activo
- Descripción/observaciones
- Tipo (Información, Software, Recurso Humano, Servicio, Hardware, Otros)
- Ubicación
- Clasificación de la Confidencialidad, Integridad y Disponibilidad
- Criticidad (Alta, Media o Baja)
- Propietario
- Custodio
- Usuarios con Acceso
- Fecha ingreso del activo
- Fecha salida del activo

Los criterios de clasificación usados se encuentran en la figura 1, la clasificación de activos de acuerdo a la confidencialidad se realizó a partir de los tres (3) niveles alineados con los tipos de información declarados en la ley 1712 del 2014 (MinTic, 2016) de la figura 2

Figura 1 Criterios de Clasificación General

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

Fuente: (MinTic, 2016, p. 7)

Figura 2 Esquema de Clasificación por confidencialidad

INFORMACION PUBLICA RESERVADA	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
INFORMACION PUBCLCA CLASIFICADA	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
INFORMACION PÚBLICA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA.

Fuente: (MinTic, 2016, p. 16)

La clasificación de activos de acuerdo a su Integridad se realizó bajo el esquema de la figura 3.

Figura 3 Esquema de clasificación por integridad

A (ALTA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
M (MEDIA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.
B (BAJA)	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.

Fuente: (MinTic, 2016, p. 17)

La clasificación de activos de acuerdo a su disponibilidad se realizó bajo el esquema de la figura 4

Figura 4 Esquema de clasificación por disponibilidad

1 (ALTA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
2 (MEDIA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
3 (BAJA)	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.

Fuente: (MinTic, 2016, p. 18)

Para calcular la criticidad de los activos de información se utilizaron las reglas definidas por MinTic en la figura 5.

Figura 5 Criterios de Criticidad de los activos de Información

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

Fuente: (MinTic, 2016, p. 7)

Luego de tener definida la información a recolectar y los criterios de clasificación de Confidencialidad, Integridad y Disponibilidad a aplicar, se realizaron reuniones con los

representantes de los procesos para determinar los activos de información, se tomó como punto de partida los activos de tipo información física con ayuda de las tablas de retención documental de la entidad, con las cuales se obtuvieron los resultados de la figura 6, figura 7 y tabla 10 a partir del anexo de los activos de información:

Figura 6 Criticidad de Activos de Información

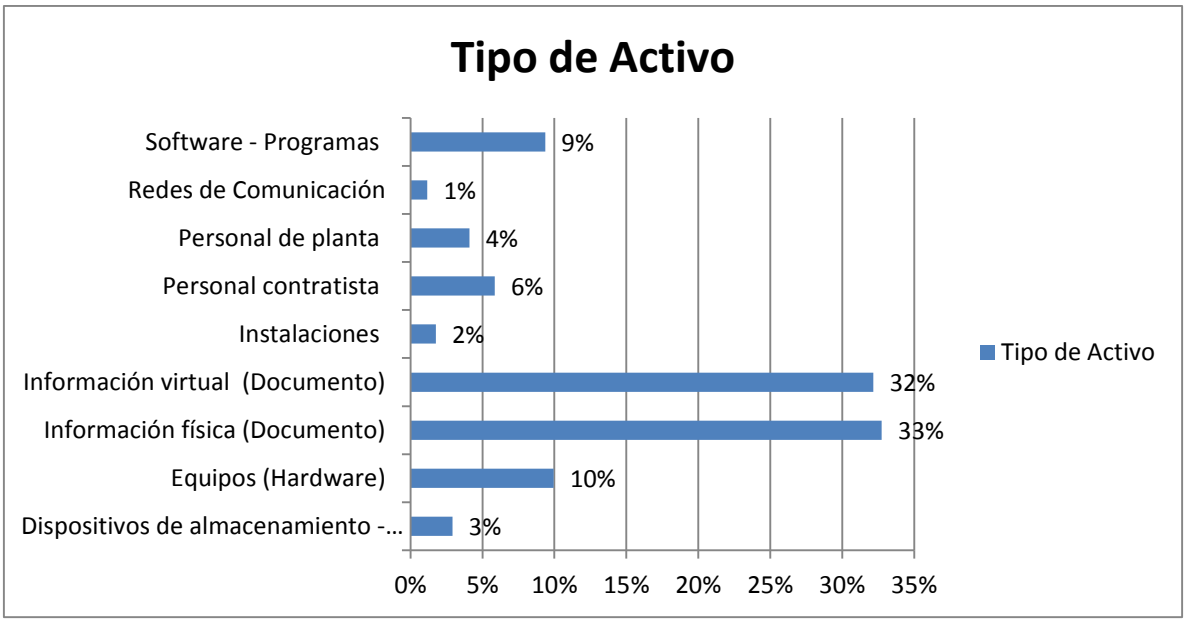
Fuente: Propia

Tabla 10 Activos de Información por Proceso

Proceso	Total
proceso 1	26
proceso 2	20
proceso 3	1
proceso 4	20
proceso 5	1
proceso 6	1
proceso 7	25
proceso 8	1
proceso 9	14
proceso 10	18
proceso 11	43
proceso 12	1
Total general	**171**

Fuente: Propia

Figura 7 Clasificación de Activos de Información



Fuente: Propia

4.2.2. Diagnóstico

4.2.2.1. Requisitos de la norma

Para el diagnóstico del cumplimiento de la norma ISO/IEC 27001 se creó un instrumento para evaluar cada uno de los numerales por medio de 167 preguntas distribuidas de la tabla 11:

Tabla 11 Cantidad de preguntas por numeral de la norma

Numeral	**Preguntas**
4. CONTEXTO DE LA ORGANIZACIÓN	15
5 LIDERAZGO	23
6. PLANIFICACIÓN	41
7. SOPORTE	29
8. OPERACIÓN	12
9 EVALUACIÓN DEL DESEMPEÑO	35
10. MEJORA	12
TOTAL	**167**

Fuente: Los autores.

Para cada una de las preguntas se midió el % de cumplimiento a partir de los siguientes criterios, por parte de la persona encargada de la seguridad de la información de la entidad como se encuentra en la tabla 12:

Tabla 12 Criterios de evaluación por pregunta

%	DESCRIPCIÒN
0%	No documentado/No existente
25%	Se aplica, pero no está documentado
50%	Está documentado, pero no se aplica
75%	Se aplica y está documentado
100%	Se aplica, está documentado y se realiza medición, control y seguimiento
N/A	No aplica

Fuente: Los autores

Los resultados del diagnóstico del cumplimiento de los debes de la norma fueron consignados en el anexo "Diagnostico ISO/IEC 27001", el cual arroja los resultados promediados por numeral y a nivel general en la tabla 13:

Tabla 13 Resultados diagnostico ISO/IEC 27001

Numeral	Cumplimiento x Numeral
4. CONTEXTO DE LA ORGANIZACIÓN	78,33%
5 LIDERAZGO	48,91%
6. PLANIFICACIÓN	68,90%
7. SOPORTE	71,55%
8. OPERACIÓN	81,25%
9 EVALUACIÓN DEL DESEMPEÑO	12,86%
10. MEJORA	64,58%
TOTAL CUMPLIMIENTO GENERAL	**56,29%**

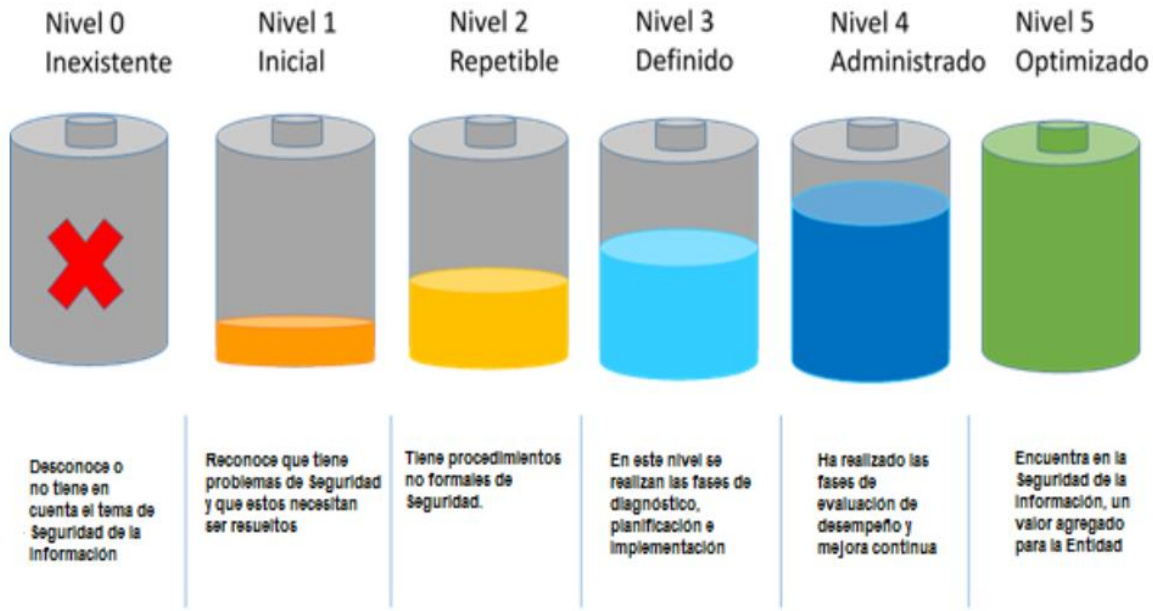
Fuente: Propia

Podemos evidenciar que la mayor fortaleza se encuentra en los numerales “Operación, contexto y soporte”, mientras que los de menor calificación fueron “Evaluación y liderazgo”, a nivel general se tiene un cumplimiento del 56 %.

4.2.2.2. Controles de la norma

Para la realización del diagnóstico del cumplimiento de la norma ISO/IEC 27002, se tomó como base el instrumento de Evaluación del MSPI (MINTIC, 2017), el cual busca evaluar el Nivel de madurez de la entidad a partir de la figura 8:

Figura 8 Niveles de Madurez de las entidades según el MSPI



Fuente: (MinTIC, 2015c, p. 36)

Esta actividad se realizó con el apoyo de los integrantes del área de sistemas de la entidad a partir del concurso del MinTic llamado “Máxima Velocidad Digital”, para lo cual se realizaron entrevistas a los encargados de los procesos, con la cual la entidad obtuvo la puntuación por el reto como se evidencia en la figura 9:

Figura 9 Puntaje reto Diagnóstico

Fuente: (MinTic, 2017)

Los resultados fueron consignados en el Anexo "Diagnóstico ISO/IEC 27002", el resumen es el siguiente:

Los Dominios de controles con mayor puntuación fueron las "políticas de seguridad de la información", "gestión de activos", "control de acceso", "seguridad física y del entorno" y "cumplimiento", los cuales muestran una calificación actual por encima del 50%, mientras que los Dominios de controles con puntuaciones menores o iguales al 20% fueron "Relaciones con los proveedores", "Gestión de incidentes de seguridad de la información", "Adquisición, desarrollo y mantenimiento de sistemas" y "Seguridad de los recursos humanos", el promedio total de la evaluación de controles nos da un 36% lo cual se encuentra muy por debajo de la meta del 60% planeada para el 2017 como se evidencia en la tabla 14 y figura 10.

Tabla 14 Resultados del Diagnóstico de seguridad de la información

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	60	60	EFECTIVO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	20	60	INICIAL
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	27	60	REPETIBLE
A.8	GESTIÓN DE ACTIVOS	60	60	EFECTIVO
A.9	CONTROL DE ACCESO	54	60	EFECTIVO
A.10	CRIPTOGRAFÍA	30	60	REPETIBLE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	50	60	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	39	60	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	35	60	REPETIBLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	19	60	INICIAL
A.15	RELACIONES CON LOS PROVEEDORES	0	60	INEXISTENTE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	6	60	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	47	60	EFECTIVO
A.18	CUMPLIMIENTO	56	60	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		**36**	**60**	REPETIBLE

Fuente: Resultados Anexo “Diagnóstico ISO/IEC 27002”.

Figura 10 Brechas del Diagnóstico

Fuente: Resultados Anexo “Diagnóstico ISO/IEC 27002”.

4.3.Validación de riesgos y planificar el tratamiento de los riesgos

4.3.1. Establecimiento del contexto

4.3.1.1. Parámetros de probabilidad

Los parámetros de probabilidad utilizados para la evaluar los riesgos están en el rango de 1 a 5, a partir de la descripción y frecuencia indicadas en la tabla 15, la cual corresponde a la información que utiliza la entidad en su tratamiento de riesgos organizacionales en la tabla 15.

Tabla 15 Parámetros de Probabilidad:

Probabilidad del Riesgo	
NIVEL	DESCRIPTOR
1	Raro
2	Improbable
3	Posible
4	Probable
5	Casi Seguro

Fuente: Tratamiento de Riesgos de la entidad

4.3.1.2 Parámetros de impacto

Los parámetros de impacto utilizados para la evaluar los riesgos están en el rango de 1 a 5, a partir de la descripción indicada en la tabla 16, 17 o 18 dependiendo de la dimensión del riesgo (confidencialidad, integridad o disponibilidad), la cual corresponde a la información que utiliza la entidad en su tratamiento de riesgos organizacionales combinada con los parámetros de impacto que se tienen definida para la Confidencialidad, Integridad y Disponibilidad de la información (Valencia Duque, Marulanda, & López Trujillo, 2016)

Tabla 16 Parámetros de Impacto de Confidencialidad

Confidencialidad	
nivel	descriptor
1	Insignificante
2	Menor
3	Moderado
4	Mayor
5	Catastrófico

Fuente: Propia

Tabla 17 Parámetros de Impacto de Integridad

Integridad	
nivel	descriptor
1	Insignificante
2	Menor
3	Moderado
4	Mayor
5	Catastrófico

Fuente: Propia

Tabla 18 Parámetros de Impacto de Disponibilidad

Disponibilidad	
nivel	descriptor
1	Insignificante
2	Menor
3	Moderado
4	Mayor
5	Catastrófico

Fuente: Propia

4.3.1.3 Determinación de vulnerabilidad

La vulnerabilidad de los riesgos corresponde al valor de la probabilidad, multiplicado por el valor del impacto, tal como se realiza en los riesgos organizacionales de la entidad.

4.3.1.4 Criterios de aceptabilidad del riesgo

Para la aceptación de los riesgos, se revisó la tabla de aceptación de riesgos de la entidad, se realizaron algunos ajustes y se acordó que para este proyecto se utilizarían los valores de la tabla 19 para el mapa de temperatura y la tabla 20 para la aceptabilidad del riesgo:

Tabla 19 Mapa de temperatura

probabilidad	impacto				
	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Fuente: Propia

Tabla 20 Aceptabilidad del riesgo

Identificación	Criterio	Calificación
	B: Zona de riesgo baja, asumir el riesgo	<=3
	M: Zona de riesgo moderada, asumir/ reducir el riesgo	>3 y <=6
	A: Zona de riesgo alta, reducir, evitar, compartir o transferir el riesgo	>6 y <=10
	E: Zona de riesgo extrema, , reducir, evitar, compartir o transferir el riesgo	>10 y <=25

Fuente: Propia

4.3.2 Valoración de riesgo

4.3.2.1 Identificación de escenarios de riesgo

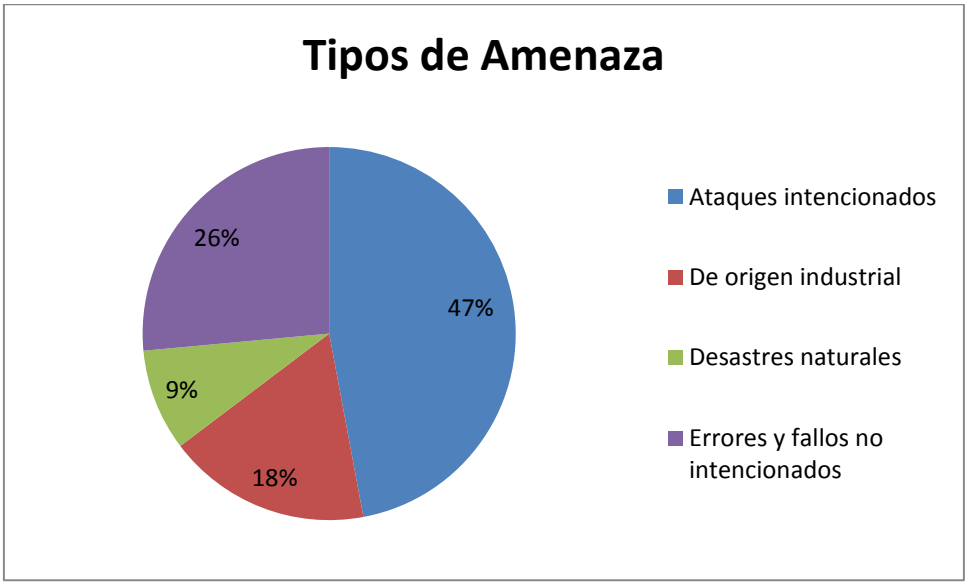
Para la identificación de los escenarios de riesgos de seguridad de la información se tomó como base el catálogo de amenazas de la metodología de Análisis y Gestión de riesgos de los sistemas de información del Ministerio de Hacienda y Administraciones públicas de

España, la cual cuenta con 43 amenazas dependiendo del tipo de activo (Amutio Gómez, 2012):

- Software
- Hardware
- Archivos físicos
- Archivos electrónicos
- Instalaciones
- Redes de comunicación
- Personal

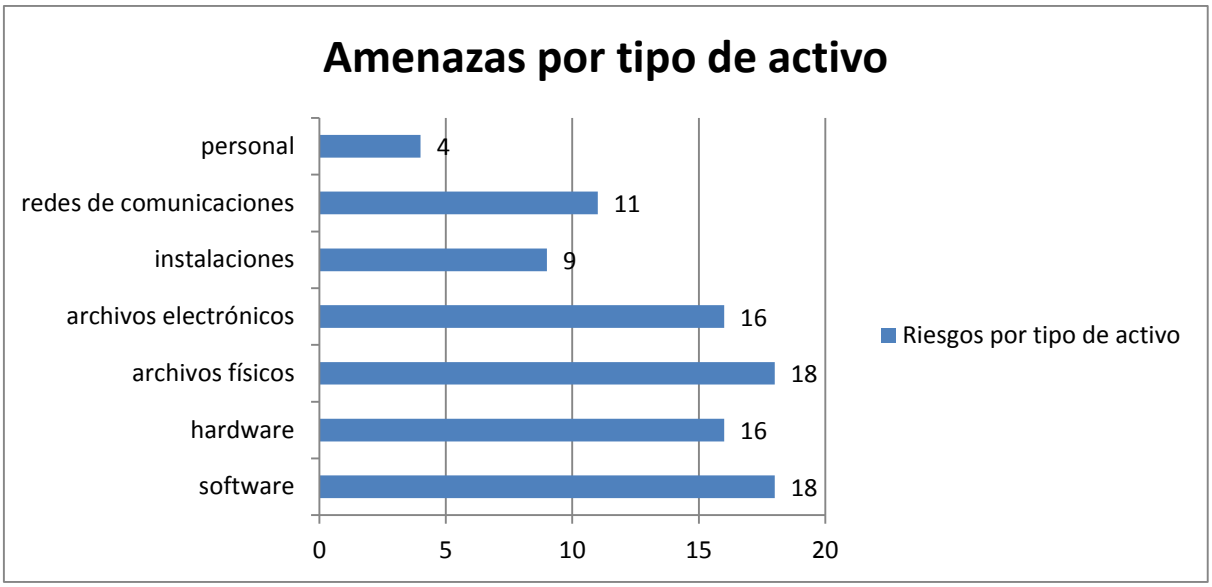
Se revisó el listado de amenazas con la persona encargada de la seguridad de la información de la entidad, y se definieron que para el contexto de la organización aplicaban 34 amenazas en la figura 11 y figura 12:

Figura 11 Tipos de Amenaza



Fuente: Propia

Figura 12 Amenazas por tipo de activo



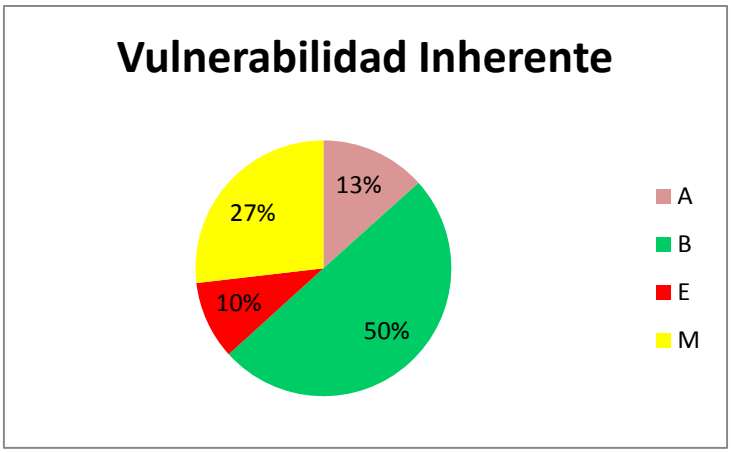
Fuente: Propia

Para la Estimación y Evaluación del riesgo, se realizaron internamente en la vulnerabilidad inherente y vulnerabilidad residual:

4.3.2.2.Vulnerabilidad Inherente

Luego de tener definidos los escenarios y los parámetros de evaluación de los riesgos, se cruzaron los escenarios de riesgo, con los activos de criticidad alta dependiendo del tipo de activo, con lo cual se generó un conjunto de riesgos, se realizaron entrevistas con los representantes de los procesos y se registraron los valores de probabilidad e impacto, los cuales se encuentran detallados en el Anexo “Matriz de riesgo inherente”, el resumen de los datos es el siguiente:

Figura 13 Vulnerabilidad Inherente

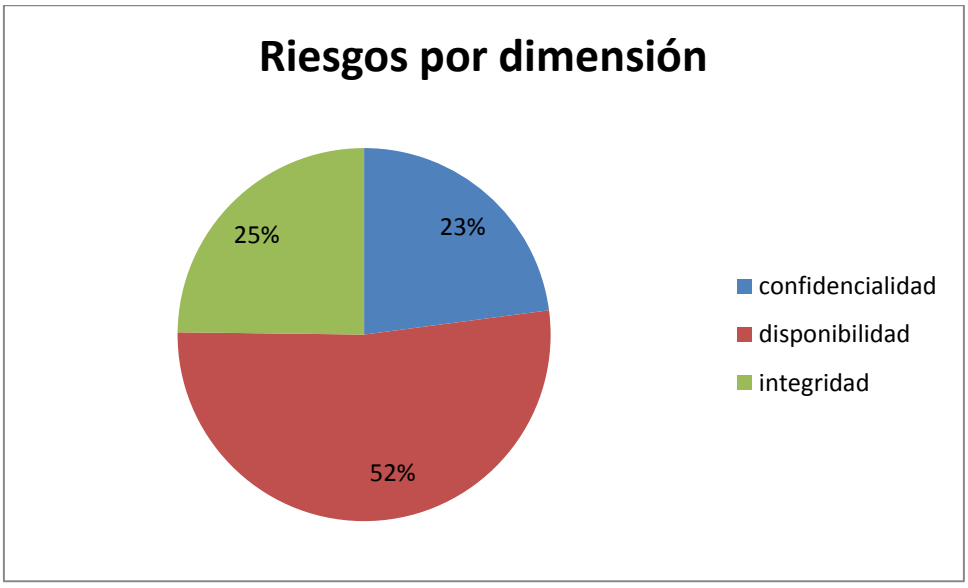


Fuente: Propia

Como podemos ver en la imagen anterior, el 50% de los riesgos tiene una vulnerabilidad baja, seguida por el 27% con vulnerabilidad media, 13% Alta y 10% Extrema.

En la siguiente imagen podemos ver que la mayoría de riesgos se refieren a la disponibilidad de la información con un 52%, y lo que corresponde a la integridad y confidencialidad cada uno tiene aproximadamente el 25% de los riesgos.

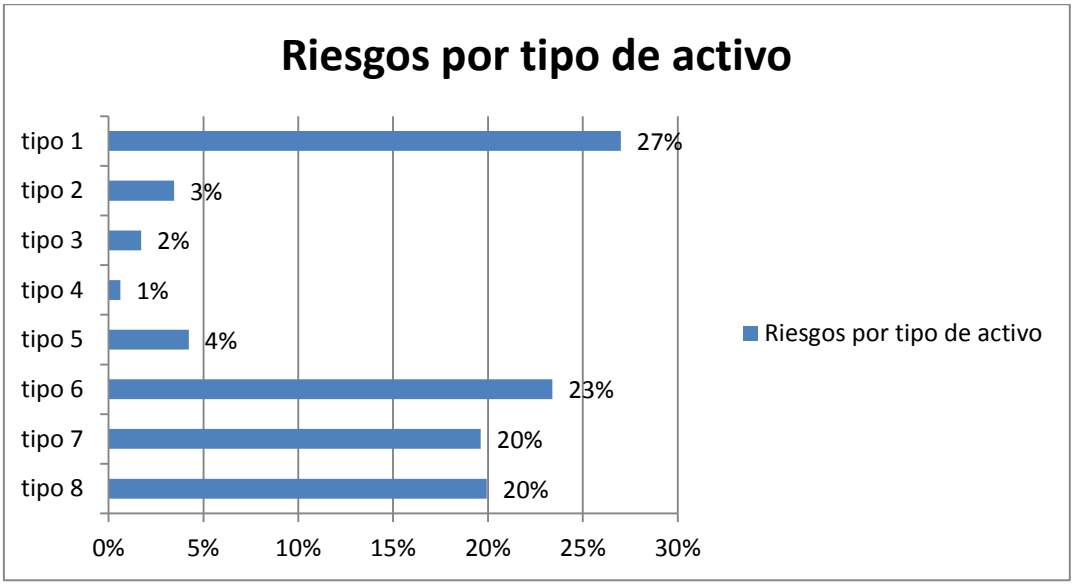
Figura 14 Riesgos por dimensión



Fuente: Propia

En el siguiente gráfico se puede visualizar la cantidad de riesgos que se tiene por tipo de activo, siendo los más representativos el tipo 1, 6, 7 y 8, y con menor cantidad los de tipo 2, 3, 4, y 5.

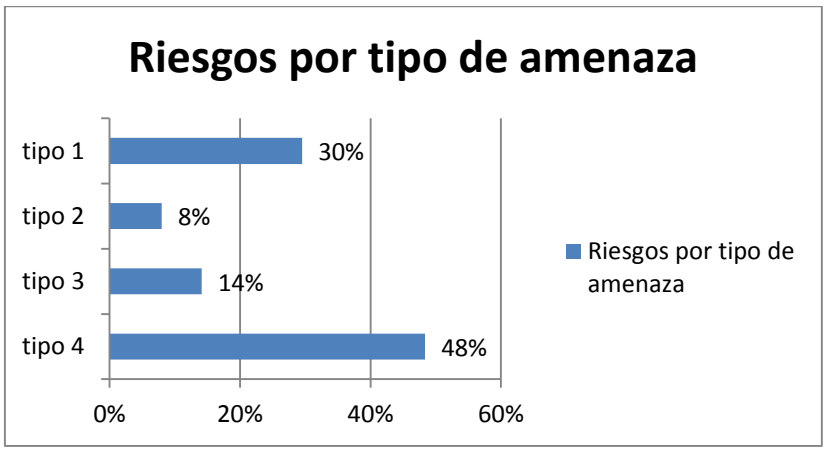
Figura 15 Riesgos por tipo de activo



Fuente: Propia

En la siguiente imagen se evidencia que la mayor cantidad de riesgos se refiere a amenazas de tipo 4, y la menor cantidad para las de tipo 2.

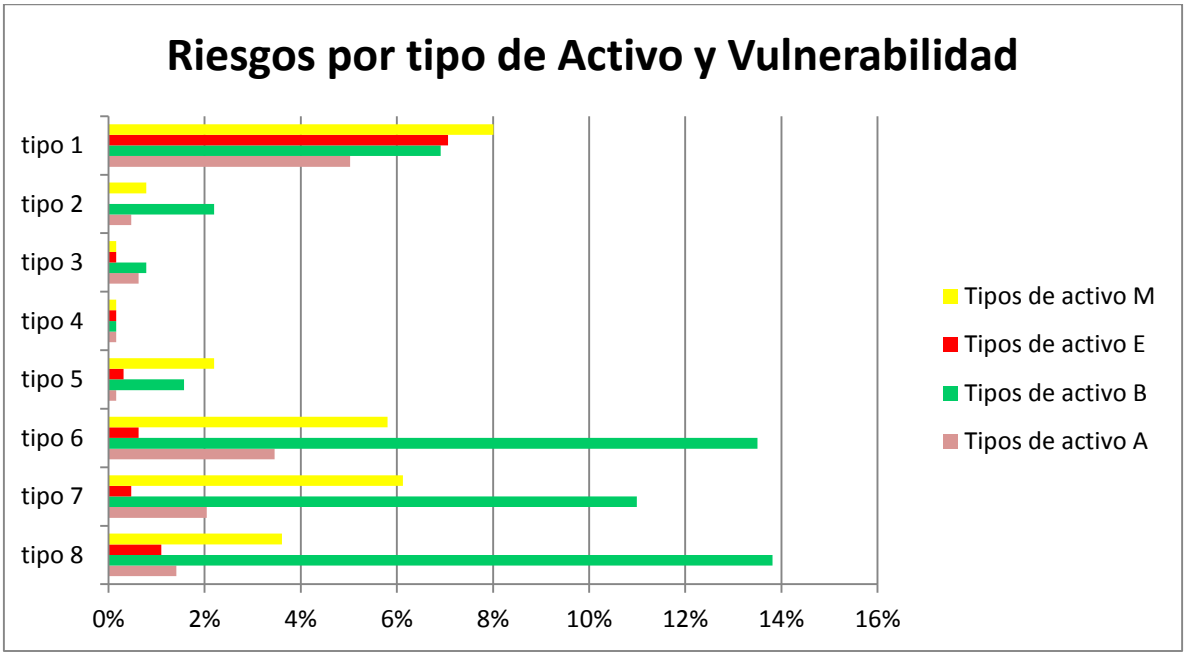
Figura 16 Riesgos por tipo de amenaza



Fuente: Propia

En la imagen de vulnerabilidad de los riesgos por tipo de activo se tiene que el tipo de activo con mayor cantidad de riesgos con vulnerabilidad Alta y Extrema se encuentra en el tipo 1, seguido por la de tipo 6.

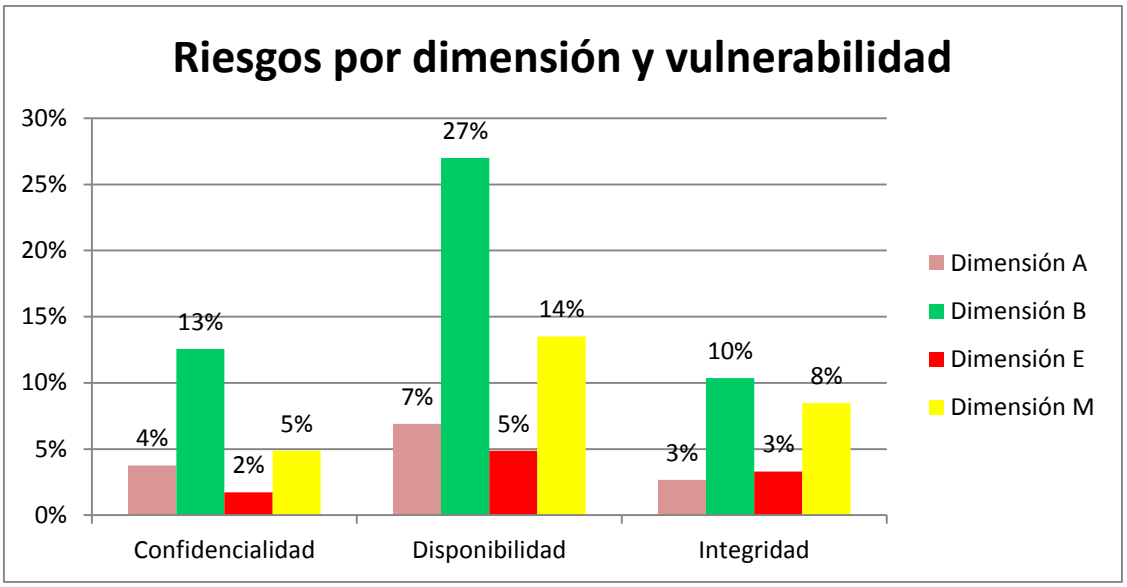
Figura 17 Vulnerabilidad de los riesgos por tipo de activo



Fuente: Propia

En la figura 18 se puede observar que la disponibilidad es la dimensión con mayor cantidad de riesgos de tipo Alto y Extremo, seguido por la Integridad y por último la confidencialidad.

Figura 18 Vulnerabilidad de los riesgos por dimensión de seguridad de la información



Fuente: Propia

4.3.2.3.Vulnerabilidad Residual

La vulnerabilidad residual se determinó a partir de los resultados de la vulnerabilidad inherente, la identificación de los controles actuales, evaluación de controles actuales y por último con la nueva estimación y evaluación de los riesgos.

4.3.2.3.1. Controles Actuales

Para la revisión de los controles actuales de la entidad se hicieron entrevistas con los representantes de los procesos para definir las medidas que se toman actualmente para reducir la probabilidad o el impacto de la materialización de los riesgos, se hizo un listado y luego se procedió a evaluar los controles a partir de la guía de administración del riesgo del Departamento Administrativo de la Función Pública (en adelante DAFP) a partir de los siguientes parámetros (Departamento Administrativo de la Función Pública, 2011) en la tabla 21 y 22:

Tabla 21 parámetros de evaluación de controles

PÁRAMETROS	CRITERIOS	TIPO DE CONTROL		PUNTAJES
		Probabilidad	Impacto	
Herramientas para ejercer el control	Posee una herramienta para ejercer el control.			15
	Existen manuales instructivos o procedimientos para el manejo de la herramienta			15
	En el tiempo que lleva la herramienta ha demostrado ser efectiva.			30
Seguimiento al control	Están definidos los responsables de la ejecución del control y del seguimiento.			15
	La frecuencia de la ejecución del control y seguimiento es adecuada.			25
	TOTAL			100

Fuente: (Departamento Administrativo de la Función Pública, 2011, p. 35)

Tabla 22 Rangos de calificación

RANGOS DE CALIFICACIÓN DE LOS CONTROLES	DEPENDIENDO SI EL CONTROL AFECTA PROBABILIDAD O IMPACTO DESPLAZA EN LA MATRIZ DE CALIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS	
	CUADRANTES A DISMINUIR EN LA PROBABILIDAD	CUADRANTES A DISMINUIR EN EL IMPACTO
Entre 0-50	0	0
Entre 51-75	1	1
Entre 76-100	2	2

Fuente: (Departamento Administrativo de la Función Pública, 2011, p. 35)

Como se puede ver en las tablas anteriores, se tiene definido un instrumento para la calificación de los controles, a partir de unos parámetros y criterios que debe tener el control, y disminuye el valor de la probabilidad o impacto entre 0 y 2 dependiendo de su puntaje, para este proyecto no se tendrán en cuenta los criterios “En el tiempo que lleva la herramienta ha demostrado ser efectiva” y “La frecuencia de la ejecución del control es adecuada”, dado que corresponden a labores de auditoría, por lo tanto se cambiarán los rangos para disminución de los valores de probabilidad e impacto del control de la siguiente manera:

Tabla 23 Puntajes posibles de los controles

Puntajes	Criterio
15	posee una herramienta para ejercer el control
15	existen manuales instructivos o procedimientos para el manejo de la herramienta
15	están definidos los responsables de la ejecución del control y seguimiento

Fuente: Propia

Tabla 24 Rangos de calificación actualizados

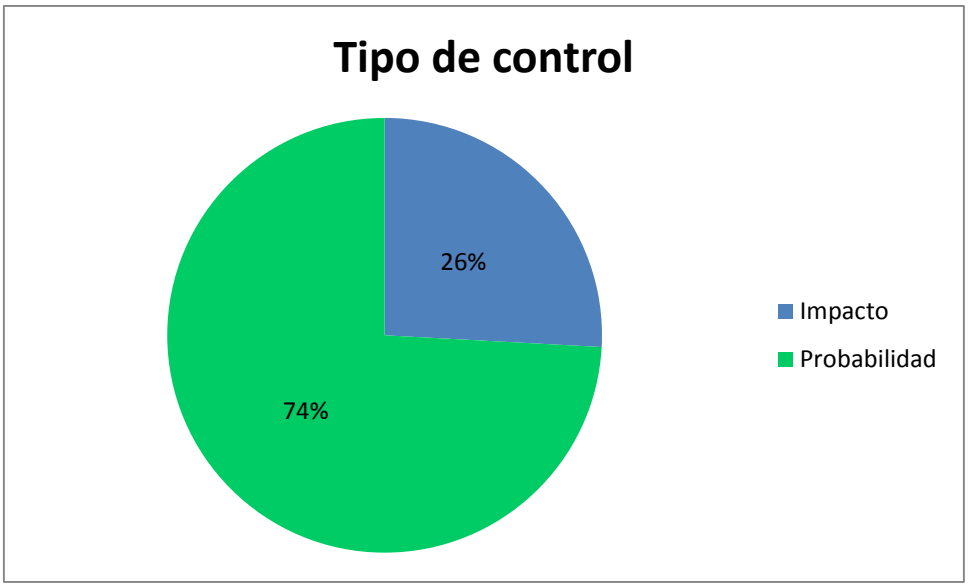
Rangos de calificación	disminuir en probabilidad o impacto
0-15	0
16-30	1
31-45	2

Fuente: Propia

A partir de los datos recolectados y la evaluación de los controles se realizó el Anexo "Controles Actuales" con el detalle de la información.

El tipo de control por probabilidad e impacto de los controles queda distribuido en la figura 19:

Figura 19 Distribución de la afectación del riesgo inherente por tipo de control

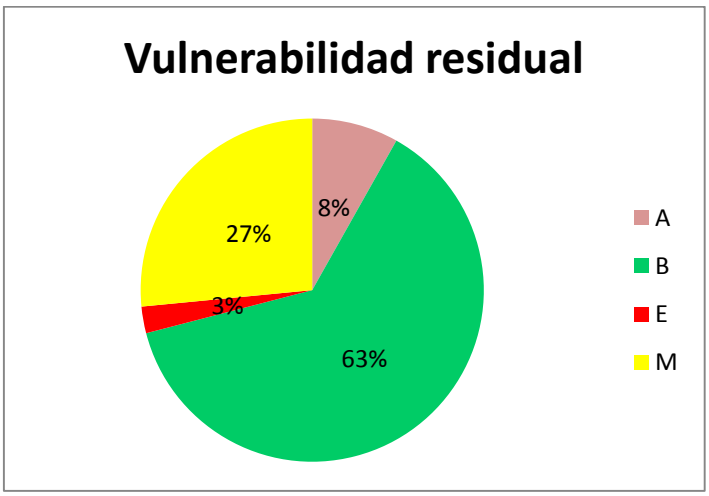


Fuente: Propia

4.3.2.3.2. Valoración y evaluación de los riesgos residual

Se realizó el cruce de los controles con los riesgos, y se aplicaron los valores de disminución dependiendo de la evaluación de los controles, los resultados fueron diligenciados en el Anexo "Matriz de Riesgo Residual", de manera resumida se tienen los datos en la figura 20:

Figura 20 Vulnerabilidad residual

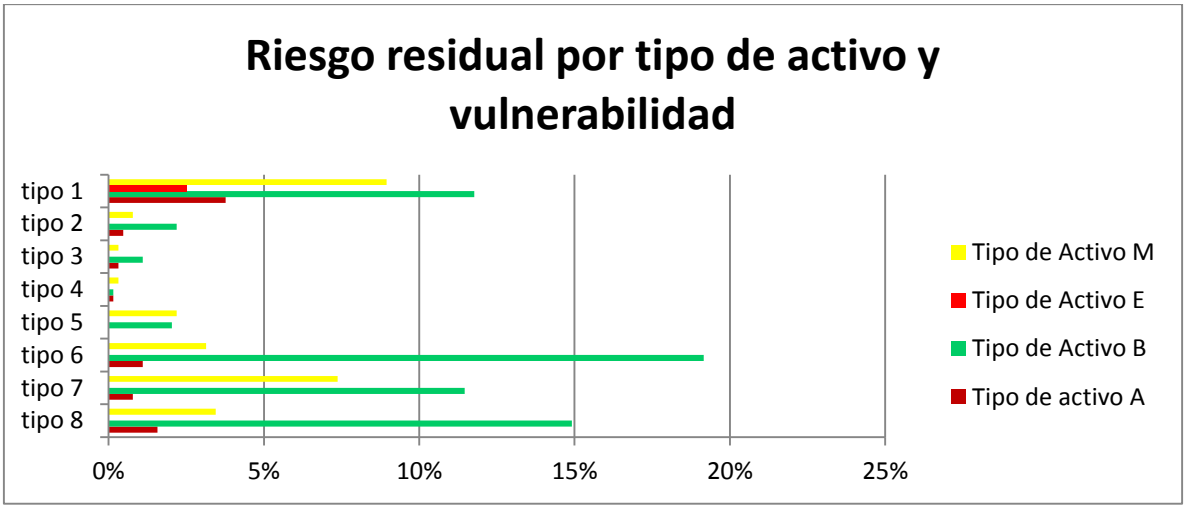


Fuente: Propia

Los resultados de la imagen anterior muestran que los riesgos de categoría baja representan ahora el 63%, categoría media el 27%, categoría alta el 8% y categoría extrema el 2%.

La figura 21 del riesgo residual por tipo de activo y vulnerabilidad permite observar que los tipos de activo con mayor vulnerabilidad son de tipo 1, seguido por los de tipo 6 y 8:

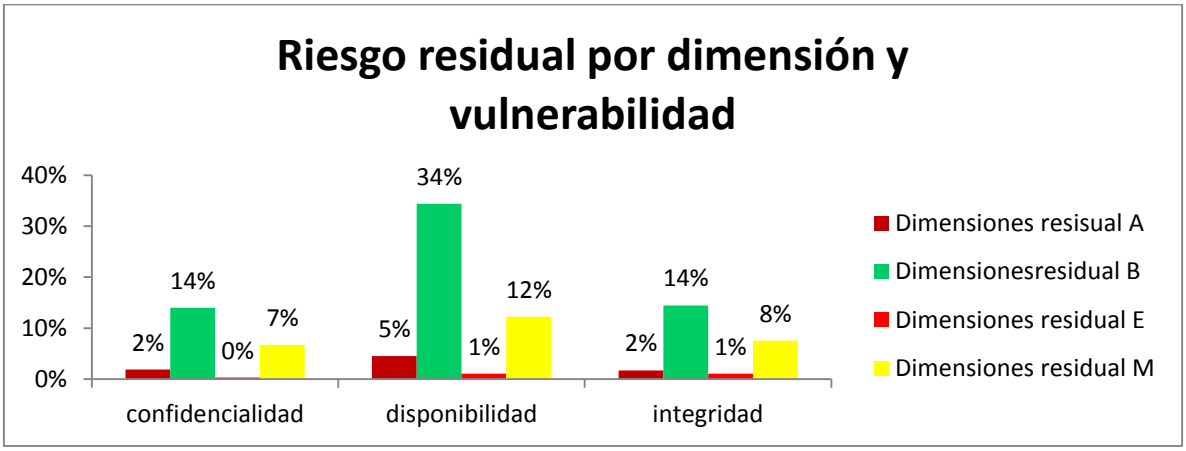
Figura 21 Riesgo residual por tipo de activo y vulnerabilidad



Fuente: Propia

Con respecto a las dimensiones de la seguridad de la información, se puede percibir que la que la mayor vulnerabilidad es de la disponibilidad de la información como muestra la figura 22:

Figura 22 Riesgo residual por dimensión y vulnerabilidad



Fuente: Propia

4.3.3. Tratamiento del riesgo

Al finalizar la matriz de riesgo residual, se cruzaron los controles actuales con los 114 controles de la norma ISO 27002, lo cual dio como resultado que la entidad tiene implementados la mayoría de ellos, luego de analizar los resultados obtenidos en la matriz de riesgo residual y los controles actuales contra los controles de la norma ISO, se plantearon controles adicionales en el anexo "Plan de tratamiento de riesgos" con los siguientes campos:

- Descripción
- Controles propuestos
- Responsable
- Valor
- Fecha Inicio
- Fecha Fin

4.4. Diseño del SGSI

4.4.1. Documentación del sistema

La documentación del Sistema de Gestión de Seguridad de la Información queda definida en la tabla 25

Tabla 25 Documentación del SGSI

Numeral ISO/IEC 27001:2013	Documentación
4,3 Determinación del alcance del SGSI	El alcance debe estar disponible como información documentada.
5,2 Política de seguridad	e) La política de seguridad debe estar disponible como información documentada.

6,1,2 Valoración de riesgos de seguridad de la información	Información documentada acerca del proceso de valoración de la seguridad de la información
6,1,3 Tratamiento de riesgos de seguridad de la información	Información documentada a cerca del proceso de tratamiento de los riesgos de seguridad de la información.
6,1,3 Declaración de aplicabilidad	d) Declaración de aplicabilidad
6,2 Objetivos de seguridad de la información y planes para lograrlo	Objetivos de seguridad de la información
7,2 Competencia	Evidencia de la competencia de las personas relacionadas con la seguridad de la información
7,5 Información documentada	b) La que la empresa ha determinado que es necesaria para la eficiencia del SGSI
7,5,3 Control de la información documentada	La información documentada de origen externo
8,1 Planificación y control operacional	Información documentada para tener confianza de que los procesos se han llevado a cabo de acuerdo a lo planificado
8,2 Valoración de la seguridad de la información	Resultados de las valoraciones de riesgos de la seguridad de la información.
8,3 Tratamiento de riesgos de	Resultado de los tratamientos de riesgos

seguridad de la información	de la seguridad de la información
9,1 Seguimiento, medición, análisis y evaluación.	Evidencia de los resultados del monitoreo y de medición
9,2 Auditoria interna,	g) Conservar la información documentada como evidencia de la implementación del programa de auditoria y los resultados de esta.
9,3 Revisión por la dirección	Evidencia de los resultados de la revisión por la dirección
10,1 No conformidades y acciones correctivas.	Naturaleza de las no conformidades y cualquier acción posterior tomada.

Fuente: Propia, basada en (Valencia-duque & Orozco-alzate, 2017)

4.4.2. Declaración de aplicabilidad

A partir de los controles actuales y los controles propuestos, se detalla a continuación la declaración de aplicabilidad para el diseño del Sistema de Gestión de Seguridad de la Información de la entidad, la cual no se establece como anexo debido a la importancia que representa dentro del SGSI, pero por la confidencialidad de la entidad se muestra sólo el resumen en la tabla 26:

Tabla 26 Declaración de aplicabilidad

Código	Resumen	Objetivo	Código de control existente	Código de control propuesto	observaciones
A.5.1.1	Políticas de la seguridad de la información	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes	57		

A.5.1.2	Revisión de las políticas para la seguridad de la información	Las políticas para la seguridad de la información se debe revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas		59	
A.6.1.1	Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar todas las responsabilidades de seguridad de la información	58	60	
A.6.1.2	Separación de deberes	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de activos de la		61	

		organización			
A.6.1.3	Contacto con las autoridades	Se deben mantener contactos apropiados con las autoridades pertinentes		62	
A.6.1.4	Contacto con grupos de interés especial	Se deben mantener contactos apropiados con grupos de interés especial y otros foros y asociaciones profesionales especializadas en seguridad			no aplica para el contexto de la organización
A.6.1.5	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe tratar en la gestión de proyectos, independiente del tipo de proyecto		63	
A.6.2.1	Política para dispositivos móviles	Se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos		64	

		introducidos por el uso de dispositivos móviles			
A.6.2.2	Teletrabajo	Se debe implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo			no aplica para el contexto de la organización
A.7.1.1	Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a		65	

		tener acceso, y a los riesgos percibidos			
A.7.1.2	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información		66	
A.7.2.1	Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la	2,22,45,46,55, 58	67	

		organización			
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre políticas y procedimientos de la organización pertinentes para su cargo	2,22,45,46,55, 58		
A.7.2.3	Proceso disciplinario	Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la		68	

		información			
A.7.3.1	Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir		66	
A.8.1.1	Inventario de activos	Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos	5,11,12		
A.8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario deben tener un propietario		61	

A.8.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información	14,19		
A.8.1.4	Devolución de activos	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo		69	
A.8.2.1	Clasificación de la información	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada		70	

A.8.2.2	Etiquetado de la información	Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización	5		
A.8.2.3	Manejo de activos	Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización	5,11,12,35,36,37, 41		
A.8.3.1	Gestión de medios removibles	Se deben implementar procedimientos para la gestión de medios	25,39		

		removibles, de acuerdo con el esquema de clasificación adoptado por la organización			
A.8.3.2	Disposición de los medios	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales		71	
A.8.3.3	Transferencia de medios físicos	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte			no aplica para el contexto de la organización
A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la	6,20, 29		

		información			
A.12.1.1	Procedimientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que lo necesiten	7,56		
A.12.1.2	Gestión de cambios	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información	13,42,56		
A.12.1.3	Gestión de capacidad	Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad		78	

		futura, para asegurar el desempeño requerido del sistema			
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación		79	
A.12.2.1	Controles contra códigos maliciosos	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos	23,25		
A.12.3.1	Respaldo de la información	Se deben hacer copias de respaldo de la información, software e imágenes de los	9,15,16,17,31,32,38,48		

		sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas			
A.12.4.1	Registro de eventos	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades de usuario, excepciones, fallas y eventos de seguridad de la información	21,23,24	80	
A.12.4.2	Protección de la información de registro	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado	1,26,27,52		
A.12.4.3	Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se deben registrar, y los		81	

		registros se deben proteger y revisar con regularidad			
A.12.4.4	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo		82	
A.12.5.1	Instalación de software en sistemas operativos	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos	25,39		
A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen;		83	

		evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado			
A.12.6.2	Restricciones sobre la instalación de software	Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios	25,39		
A.12.7.1	Controles de auditorías de sistemas de información	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio		84	
A.13.1.1	Controles de redes	Las redes se deben gestionar y controlar para	23		

		proteger al información en sistemas y aplicaciones			
A.13.1.2	Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente	23		
A.13.1.3	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes	23		
A.13.2.1	Políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de	4		

		información mediante el uso de todo tipo de instalaciones de comunicaciones			
A.13.2.2	Acuerdos sobre transferencia de información	Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas	4		
A.13.2.3	Mensajería electrónica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica	29		
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la	4	66	

		protección de la información			
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar	4,8,10		
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para	3,4,8,10,30,54		

		la información de la organización			
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación	3,4,8,30		
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios con los proveedores		90	

A.15.2.2	Gestión de cambios en los servicios de los proveedores	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos	30	91	

Fuente: Propia

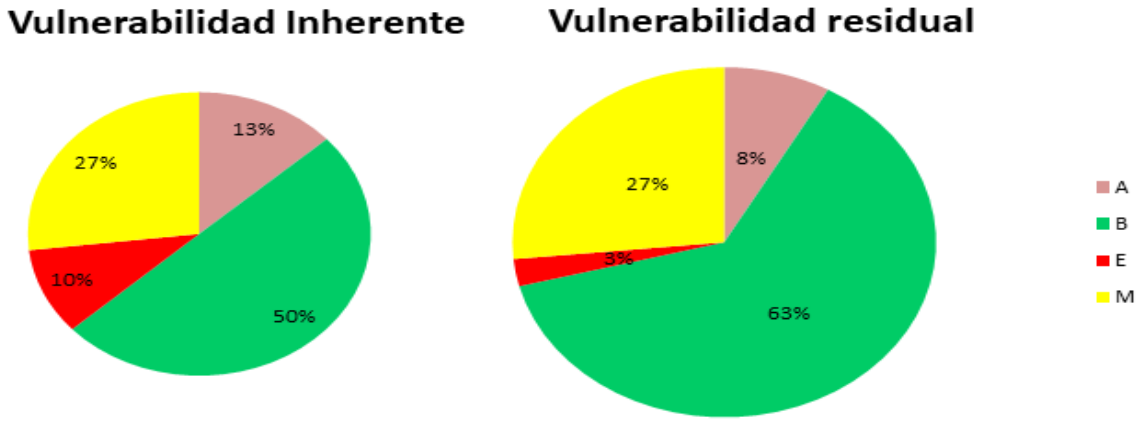
5. DISCUSIÓN DE LOS RESULTADOS

A partir de la información de la revisión sistemática de literatura se comparan las causas variables de la implementación de los SGSI en las entidades, encontrando que entre las más importantes se encuentran la consciencia de los colaboradores, el compromiso de la alta dirección y la cultura organizacional, ya que las personas son un factor clave para el éxito o fracaso de estos proyectos.

La Evaluación de la vulnerabilidad de los riesgos ha disminuido sustancialmente al evaluar los riesgos teniendo en cuenta los controles actuales, de la siguiente manera:

- Riesgos con vulnerabilidad Extrema disminuyeron de 10% a 3%
- Riesgos con vulnerabilidad Alta disminuyeron de 13% a 8%
- Riesgos con vulnerabilidad Media se mantienen en 27%
- Riesgos con vulnerabilidad Baja aumentaron de 50% a 63%

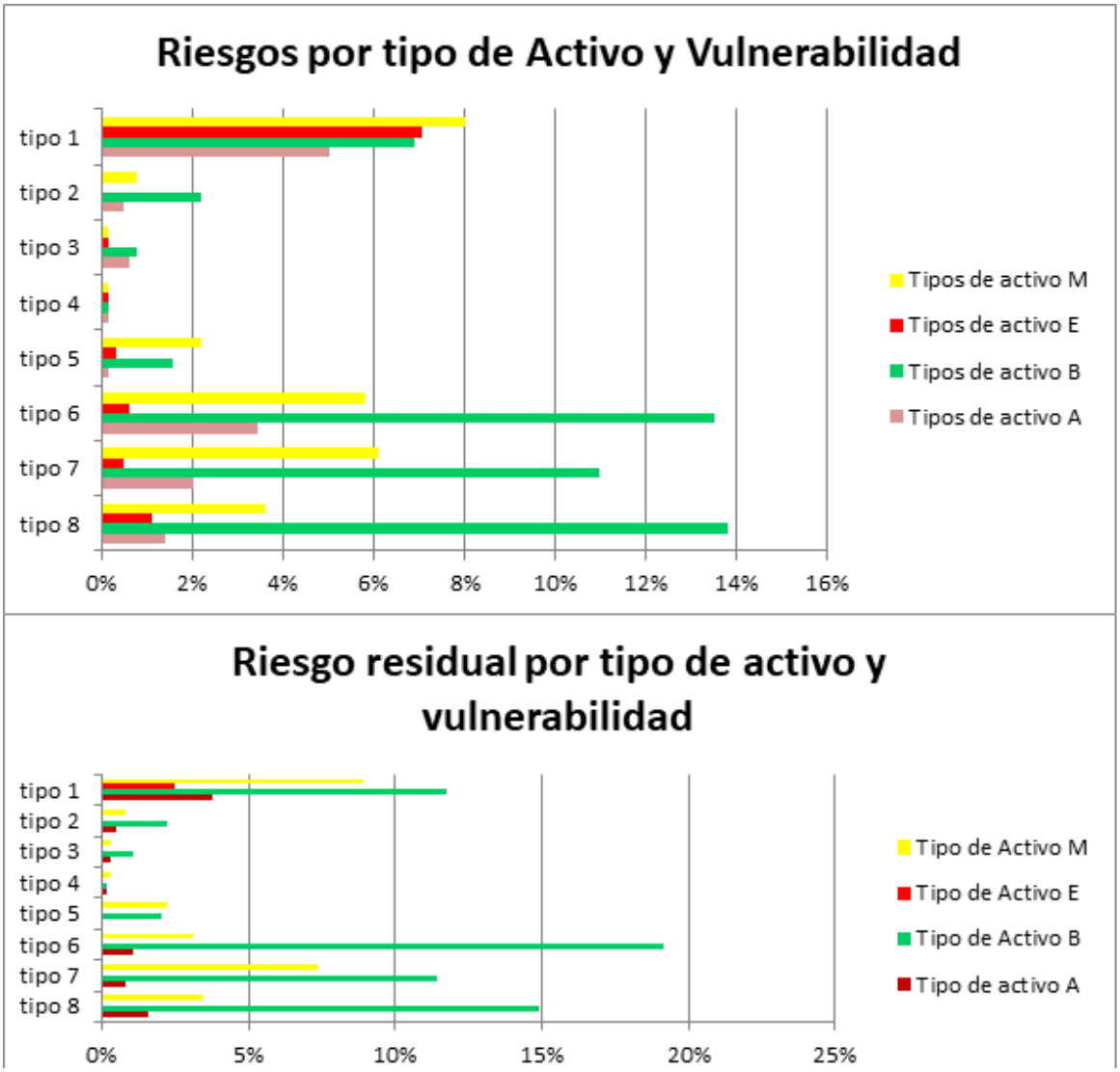
Figura 23 Vulnerabilidad Inherente Vs Vulnerabilidad Residual



Fuente: Propia

Con respecto a la vulnerabilidad en los tipos de Activo, se evidencia que la clasificación con las vulnerabilidades más altas es la de tipo 1, como se puede observar en la figura 24:

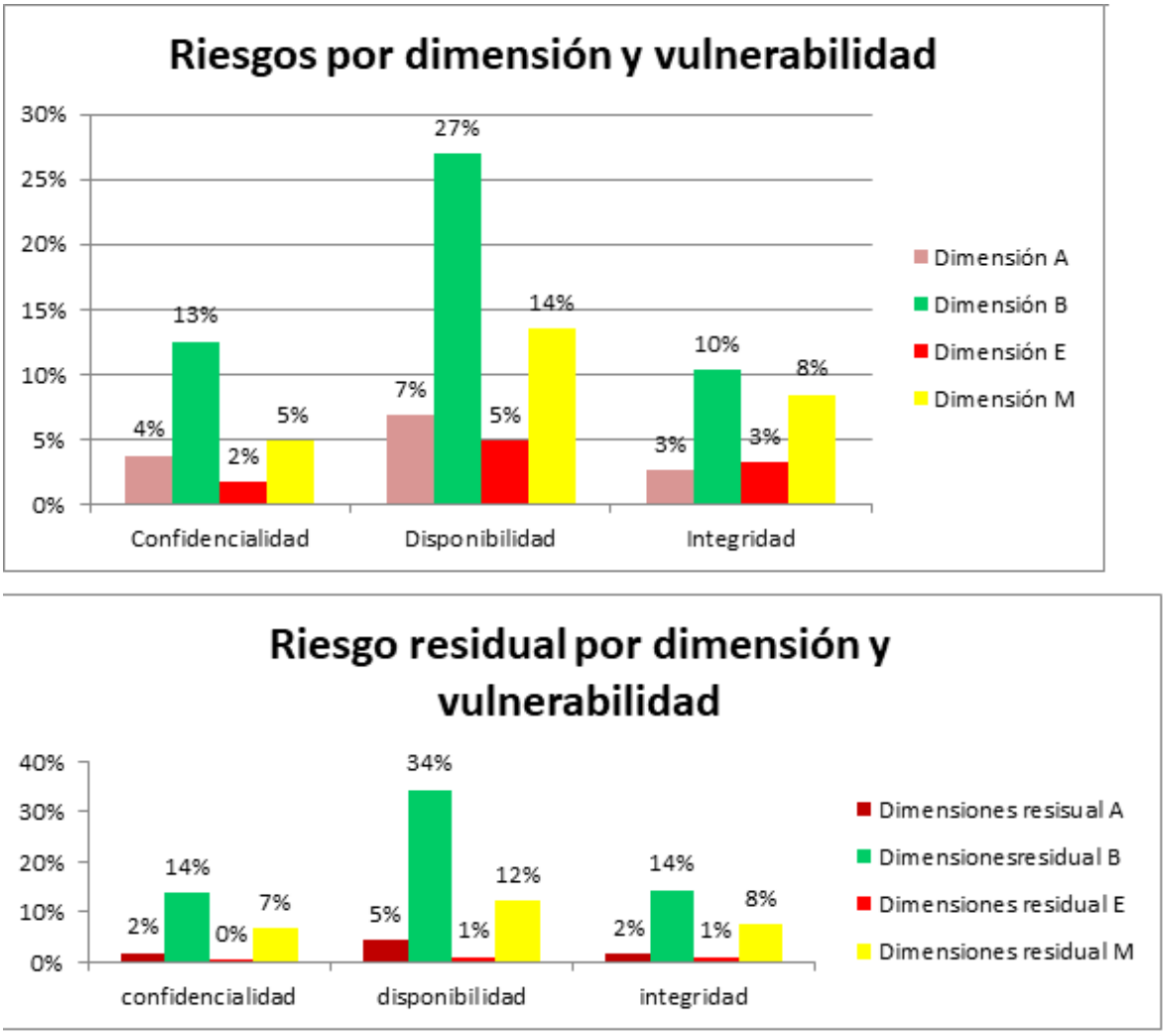
Figura 24 Tipos de Activo con Vulnerabilidad Inherente y Residual



Fuente: Propia

Evaluando las dimensiones de la seguridad de la información, se observa que la dimensión de la Disponibilidad es la que presenta mayor cantidad de vulnerabilidades en la evaluación de riesgos iniciales y en la vulnerabilidad residual, como podemos ver en la figura 25:

Figura 25 Vulnerabilidad de las dimensiones de seguridad de la información



Fuente: Propia

6. CONCLUSIONES Y RECOMENDACIONES

6.1.Conclusiones

La revisión sistémica de literatura muestra que para poder implementar exitosamente un Sistema de Gestión de Seguridad de la Información en una entidad se deben tener en cuenta factores como legales, sociales, culturales y organizacionales, en el contexto de la entidad se tiene una fortaleza en la parte legal con el apoyo del MinTic y la estrategia de Gobierno en Línea, y organizacionalmente tienen una gran capacidad de poder llevar a cabo las actividades para la implementación, seguimiento y control del SGSI, teniendo en cuenta que se deben analizar los factores culturales y sociales para garantizar la implementación de manera exitosa.

Los resultados del diagnóstico de seguridad de la información de las normas ISO 27001 y 27002 muestran un grado de avance por debajo de la meta planteada por el MinTic para el año 2017, con los cuales se evidencia la importancia del diseño e implementación del Sistema de Gestión de Seguridad de la Información.

La entidad viene trabajando continuamente con el tema de seguridad de la información, lo que se puede evidenciar en los resultados obtenidos entre la vulnerabilidad inherente y la vulnerabilidad residual, la cual tuvo una disminución muy significativa en los valores de los riesgos, y cuando apliquen los controles propuestos podrán mejorar aún más sus resultados en cuanto a seguridad de la información

Entre las dimensiones de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad), los resultados muestran que la Disponibilidad es la que representa las vulnerabilidades más altas, debido a que tiene la mayor cantidad de escenarios de riesgo.

6.2.Recomendaciones

Para la entidad:

- Tener un sistema de recompensas e incentivos para la culturización de la seguridad de la información con sus colaboradores
- Realizar una segmentación de usuarios a partir del nivel de consciencia y conocimiento en cuanto a la seguridad de la información, para convertirlos en multiplicadores del conocimiento y de la buena cultura organizacional
- Mantener capacitado al personal encargado de la seguridad de la información en temas normativos.
- Realizar seguimiento y control a la implementación de seguridad de la información, de los incidentes que se presenten y los resultados, con el fin mejorar continuamente el SGSI.
- Manejar un vocabulario adecuado con respecto a los términos de seguridad de la información para mejorar el entendimiento y la consciencia de todos los funcionarios.

Para la comunidad científica:

- Desarrollar metodologías para selección de controles de seguridad de la información y priorización de los mismos en los planes de implementación de un SGSI.
- Validar modelos expuestos en el SLR acerca de la toma de consciencia de las personas en cuanto a seguridad de la información.
- Evaluar más implementaciones de los SGSI en las entidades públicas para validar el Modelo de Seguridad y Privacidad de la Información del MinTic y permita mejorarlo continuamente.

7. EVIDENCIA DE RESULTADOS EN GENERACIÓN DE CONOCIMIENTO, FORTALECIMIENTO DE LA CAPACIDAD CIENTÍFICA Y APROPIACIÓN SOCIAL DEL CONOCIMIENTO, FORMACIÓN

Tabla 27 Resultados/Productos esperados

Aspecto	Resultado/Producto esperado	Indicador	Beneficiario
Fortalecimiento de la comunidad científica	Identificación del cumplimiento actual de la entidad con respecto a la norma ISO 27001	Anexo "Diagnóstico"	Entidad pública colombiana
	Identificación de activos de información	Anexo "Activos de información"	Entidad pública colombiana
	Identificación y valoración de riesgos de seguridad de la información	Anexo "Matriz de riesgo Inherente"	Entidad pública colombiana
Apropiación social del conocimiento	Informe final con los resultados del Diseño del Sistema de gestión de seguridad de la información	Sustentación y Publicación del informe final	Autores, comunidad académica, Talento Digital
Apropiación social del conocimiento	Artículo para revista indexada con los resultados del proyecto y del caso de estudio	Artículo en proceso de construcción para su posterior publicación	Autores, comunidad académica, Talento Digital

Fuente: Propia

8. IMPACTOS LOGRADOS

Tabla 28 Cuadro de Impactos Esperados

Impacto Esperado	Plazo (años)	Indicador Verificable	Supuestos
Implementación de la norma ISO 27001 en el proceso de gestión y finanzas públicas de la entidad	1	Cumplimiento del logro "Implementación del plan de seguridad y privacidad de la información y de los sistemas de información"	La entidad gestionará los recursos necesarios para ejecutar el plan de implementación
Aumento en el nivel de seguridad de la información	3	Disminución en un 50% de incidentes reportados que afecten la seguridad de la información	Se efectuaron todos los controles de seguridad del plan de implementación, y se realiza monitoreo y control al SGSI
Mejora continua sobre el SGSI	6	Nivel de madurez del SGSI	Se realizan acciones de mejora sobre el SGSI

Fuente: Propia

9. ANEXOS

La mayoría de los anexos se encuentran en archivos independientes, debido en primera instancia a la dimensión en su diseño y en segundo lugar por aspectos de reserva de información solicitado por la entidad.

Anexo A. Cronograma

CRONOGRAMA		MESES											
N°	Actividades	1	2	3	4	5	6	7	8	9	10	11	12
1	Presentación y aprobación de la propuesta												
2	Realizar la revisión sistemática de literatura de los sistemas de gestión de seguridad de la información en una entidad												
3	Realizar diagnóstico para determinar estado actual de seguridad con la iso 27001												
4	Definir el alcance de los procesos a ser analizados												
5	Valoración de los riesgos de seguridad de la información												
6	Planificación del tratamiento de riesgos												
7	Diseñar el Sistema de Gestión de Seguridad de la Información												
8	Definir la Política del Sistema de Gestión de Seguridad de la Información												
9	Realizar el plan de proyecto para la implementación del Sistema de Gestión de Seguridad de la Información												
10	Elaboración del caso de estudio												
11	Formación al personal encargado de la institución												
12	Elaboración del informe final												
13	Elaboración de artículo												
14	Entrega informe final, artículo y cesión de derechos												

Anexo B. Presupuesto

Detalle	**Descripción**	**Valor hora**	**Cantidad horas**	**Valor (COP)**
Personal	Estudiantes	20.000	1.400	$ 28.000.000
	Personal de la entidad	30.000	300	$ 9.000.000
	Consultor seguridad de la información	50.000	8	$ 400.000
	Asesor del proyecto	50.000	100	$5.000.000
Equipos de Cómputo	Portátiles			$2.400.000
Bibliografía	Libros y normas			$600.000
	Fotocopias			$100.000
Viajes y viáticos	Desplazamiento a la entidad en la ciudad de Pereira			$1.600.000
Documento final	Impresión			$200.000
	Empastes			$50.000
Subtotal				$ 47.350.000
Imprevistos	10% del total del proyecto			$4.735.000
Total				$ 52.085.000

Anexo C Diagnóstico ISO/IEC 27001

Archivo: “INSTRUMENTOS DE DIAGNOSTICO_27001.xlsx”

Anexo D. Diagnóstico ISO/IEC 27002

Archivo “diagnostico SGSI V2.xlsx”

Anexo E. Activos de Información

Archivo “Consolidado de Activos.xlsx”

Anexo F. Matriz de riesgo Inherente

Archivo “matriz de riesgo inherente.xlsx”

Anexo G. Controles Actuales

Archivo “controles actuales.xlsx”

Anexo H. Matriz de Riesgo Residual

Archivo “Matriz de riesgo residual.xslx”

Anexo I. Acta de Definición del Alcance del SGSI

Archivo “ACTA 02.docx”

Anexo J. Tablas de retención documental

Archivo “Tablas de Retención Documental.xls”

Anexo K. Catálogo de amenazas

Archivo “catálogo de amenazasV2.xlsx”

Anexo L. Política de seguridad y privacidad de la información de la entidad

Archivo “Política de Seguridad y Privacidad de la Información VI.docx”

Anexo M. Plan de tratamiento de riesgos

Archivo “Plan de tratamiento de riesgos.xlsx”

Anexo N Artículos encontrados

Archivo: “Artículos encontrados SLR.xslx”

Anexo O. Estudios primarios

Archivo “Estudios primarios SLR.xlsx”

Anexo P Estudios Seleccionados

Archivo “Estudios seleccionados SLR.xslx”

Anexo Q ANEXO AL CONTRATO DE TRABAJO ACUERDO DE CONFIDENCIALIDAD

Archivo” ANEXO AL CONTRATO DE TRABAJO ACUERDO DE CONFIDENCIALIDAD.docx”

Anexo R Acta de seguimiento por parte de la dirección

Archivo “Acta de seguimiento por parte de la dirección.docx”

Anexo S PROCEDIMIENTO GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Archivo “PR- PROCEDIMIENTO GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.docx”

Anexo T FORMATO DE REGISTRO PRUEBAS SISTEMAS DE CONTINGENCIAS

Archivo “F - FORMATO DE REGISTRO PRUEBAS SISTEMAS DE CONTINGENCIAS.xlsx”

Anexo U REPORTE INCIDENTES SEGURIDAD DE LA INFORMACIÓN

Archivo “F- REPORTE INCIDENTES SEGURIDAD DE LA INFORMACIÓN.xlsx”

Anexo V SEGUIMIENTO DE INDICADOR SGSI

Archivo “SEGUIMIENTO DE INDICADOR SGSI.xlsx”

10. BIBLIOGRAFÍA

Amutio Gómez, M. A. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Retrieved from http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Bachelet, M. (2013). *Programa de Gobierno Michelle Bachelet PRUEBA*. Santiago de Chile. Retrieved from http://www.onar.gob.cl/wp-content/upLoads/2014/05/ProgramaMB.pdf

Bauer, S., Bernroider, E. W. N., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers and Security*, *68*, 145–159. https://doi.org/10.1016/j.cose.2017.04.009

Centro cibernético, P. (2017). *CIBERCRIMEN*. Bogota: Centro cibernetico Policial. Retrieved from https://caivirtual.policia.gov.co/contenido/informe-amenazas-del-cibercrimen-en-colombia-2016-2017

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of Information Security at the Workplace : Linking Information Security Climate to Compliant Behavior Mark Chan National University of Singapore Irene Woon School of Computing , National University of Singapore Atreyi Kankanhalli School of Com. *Journal of Information Privacy and Security*, *1*(3), 18–41. https://doi.org/10.2307/3151312

Congrerso de Colombia. LEY ESTATUTARIA 1581 PROTECCÓN DE DATOS PERSONALES, Pub. L. No. 1581, 301 (2012). Colombia.

Congreso de la República. Ley de Transparencia y del Derecho al Acceso a la Información Pública Nacional [Ley 1712 de 2014], Pub. L. No. 1712, 2014 (2014). Colombia: Congreso de la República. Retrieved from http://www.centrodememoriahistorica.gov.co/descargas/transparencia/Ley1712-transparencia-acceso-informacion.pdf

Departamento Administrativo de la Función Pública. (2011). *Guía para la administración del riesgo*. Retrieved from https://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba

DNP Departamento nacional de planeación. CONPES 2790, Pub. L. No. CONPES 2799, 16 (1995). Colombia: DNP Departamento nacional de planeación. Retrieved from https://www.armada.mil.co/sites/default/files/conpes_2790-gestion_publica_resultados.pdf

Dor, D., & Elovici, Y. (2016). A model of the information security investment decision-making process. *Computers & Security*, *63*, 1–13. https://doi.org/10.1016/j.cose.2016.09.006

ESET. (2017). *ESET Security Report Latinoamérica*. Retrieved from https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

ISO. (2017). 9. ISO Survey of certifications to management system standards - Full results. Retrieved June 11, 2017, from http://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

ISO/IEC. (2007). GUÍA TÉCNICA COLOMBIANA GTC-ISO-IEC 27003. Geneva.

ISO/IEC. (2008). NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27005. Geneva.

ISO/IEC. (2013a). GUÍA TÉCNICA COLOMBIANA GTC-ISO-IEC 27002. Geneva.

ISO/IEC. (2013b). NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27001. Geneva.

ISO/IEC. (2016). ISO/IEC 27000:2016 Information technology — Security techniques — Information security management systems — Overview and vocabulary. *ISO.org [Online]*. Retrieved from http://standards.iso.org/ittf/PubliclyAvailableStandards/c066435_ISO_IEC_27000_2016(E).zip

Kitchenham, B. (2004). *Procedures for performing systematic reviews*. *Keele, UK, Keele University* (Vol. 33). https://doi.org/10.1.1.122.3308

Ku, C.-Y., Chang, Y.-W., & Yen, D. C. (2009). National information security policy and its implementation: A case study in Taiwan. *Telecommunications Policy*, *33*(7), 371–384. https://doi.org/10.1016/j.telpol.2009.03.002

Martínez Carazo, P. C. (2006). El método de estudio de caso: Estrategia metodológica de la investigación científica. *Pensamiento Y Gestión*, *20*, 165–193. https://doi.org/10.1055/s-0029-1217568

Ministerio de ciencia tecnología e innovación, B. (2012). Estratégia Nacional de Ciência, Tecnologia e Inovação 2012 - 2015. Ministerio de ciencia, tecnologia e inovación (MCTI). Retrieved from http://bibspi.planejamento.gov.br/handle/iditem/384

MinTic. (2016). Guía para la Gestión y Clasificación de Activos de Información.

MinTic. (2017). puntuaciones máxima velocidad de la entidad. Retrieved December 9, 2017, from http://maximavelocidad.gov.co/663/w3-propertyvalue-33424.html

MinTIC. Conpes 3072, Pub. L. No. CONPES 3072, 23 (2000). Santa Fe de Bogotá, Colombia: Ministerio de Comunicaciones. Retrieved from http://www.mintic.gov.co/portal/604/articles-3498_documento.pdf

MinTIC. Decreto 1078, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones (2015). Bogota, Colombia. Retrieved from http://www.mintic.gov.co/portal/604/w3-article-13657.html

MinTIC. (2015b). Estrategia de Gobierno en Línea. Bogota, Colombia: MIN TIC. Retrieved from http://estrategia.gobiernoenlinea.gov.co/623/articles-7941_manualGEL.pdf

MinTIC. (2015c). Modelo de Seguridad y Privacidad de la Información. Retrieved from http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_Seguridad.pdf

MinTIC. (2016). Elaboración de la política general de seguridad y privacidad de la

información.

MinTIC. (2017a). índice Nacional GEL. Retrieved June 11, 2016, from http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-14713.html

MinTIC. (2017b). Indice Territorial GEL. Retrieved June 11, 2017, from http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-14714.html

MINTIC. (2017). Instructivo para el Diligenciamiento de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información.

Ozkan, S., & Karabacak, B. (2010). Collaborative risk method for information security management practices: A case context within Turkey. *International Journal of Information Management*, *30*(6), 567–572. https://doi.org/10.1016/j.ijinfomgt.2010.08.007

Said, A. R., Abdullah, H., Uli, J., & Mohamed, Z. A. (2014). Relationship between Organizational Characteristics and Information Security Knowledge Management Implementation. *Procedia - Social and Behavioral Sciences*, *123*, 433–443. https://doi.org/10.1016/j.sbspro.2014.01.1442

The gA Center Digital Business Transformation. (2013). Latin America 4.0 The digital transformation in the value chain. Retrieved from http://www.grupoassa.com/informes/Latam-40-dBT-in-the-Value-Chain.pdf

Valencia-duque, F. J., & Orozco-alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO / IEC 27000. *Risti*, *22*, 73–88. https://doi.org/10.17013/risti.22.73

Valencia Duque, F. J., Marulanda, C. E., & López Trujillo, M. (2016). Gobierno y gestión de riesgos de tecnologías de información y aspectos diferenciadores con el riesgo organizacional. *Gerencia Tecnológica Informática*, *15*(2015), 65–77.