Metodología integradora para simplificar la implementación de los componentes de un sistema de gestión de la información (SGSI), en pequeñas y medianas empresas del sector de la información y comunicaciones en la ciudad de Medellín

Cesar Augusto González Durango

Instituto Tecnológico Metropolitano
Facultad de Ingenierías
Ciudad de Medellín, Colombia
2019

Metodología integradora para simplificar la implementación de los componentes de un sistema de gestión de la información (SGSI), en pequeñas y medianas empresas del sector de la información y comunicaciones en la ciudad de Medellín

Cesar Augusto González Durango

Trabajo de Investigación presentado como requisito parcial para optar al título de:
Magister en Seguridad Informática

Directores:
Gloria M. Díaz, PhD.
Leonel Marín, MsC.

Grupo de Investigación:
Automática, Electrónica y Ciencias Computacionales

Instituto Tecnológico Metropolitano
Facultad de Ingenierías
Ciudad de Medellí, Colombia
2019

(Dedicatoria)

A Dios: Fuente de sabiduría
A mi esposa, Adriana.
A mis hijos Isabella y Jose Manuel.
A mis padres. Rosalba y José

A los docentes de la Maestría en Seguridad Informática del ITM, dar gracias por haber tomado la decisión de enseñar, por haber decidido compartir sus conocimientos, por instruir con excelencia y disposición; por decidir ser docentes para compartir sus conocimientos con todo aquel que lo requiera, por creer en la educación y el desarrollo de la sociedad.
Cesar Augusto Gonzalez Durango.

Agradecimientos

Son muchas personas a quienes debo agradecer el inicio y culminación de este proyecto:

Gracias a la PHD. Gloria Mercedes Díaz Cabrera, directora de mi proyecto, por su acompañamiento, conocimiento y por su orientación para finalizar felizmente este proyecto, gracias por darle forma a cada idea y vislumbrar un proyecto no como una propuesta de proyecto sino como una idea de negocio y pensar en grande. Aprendí muchísimo.

Gracias al profesor Leonel Marín Ramírez, asesor técnico, por dar claridad a mis dudas y no dejarme desviar del rumbo señalado desde el inicio del proyecto.

Gracias a los docentes, Andres Gomez y Hector Vargas, por sus agradables charlas, en las cuales me ayudaron a dar claridad sobre temas técnicos y normatividad del proyecto.

Gracias al señor gerente general de E-Global Leonardo Echeverri por brindarme la oportunidad en su compañía de realizar parte de mi proyecto.

Resumen

En la actualidad, existen muchos ataques informáticos cuya tendencia va en ascenso, los cuales afectan, en buena medida, el sector empresarial. Uno de los sectores más vulnerables a estos riesgos es el conformado por las PYMES (Pequeña y mediana empresas. Las cuales, por su tamaño y capacidad financiera, adolecen de mecanismos para la adopción de estándares y normas internacionales en seguridad de la información, que les permita mitigar las amenazas derivadas de los ciberataques, y al mismo tiempo, las convierta en una organización que optimice el recurso humano, hacia unas prácticas que las conduzcan a gestionar los riesgos de una manera más eficiente. Este proyecto propone una metodología basada en estándares internacionales, que busca facilitar el diseño de un sistema de gestión de seguridad de la información (SGSI) en PYMES. Particularmente, para las PYMES del sector de la información y comunicaciones de la ciudad de Medellín. El desarrollo de este proyecto incluyó un diagnóstico del nivel de adopción de SGSIs en estas empresas, el análisis de estándares internacionales, cuyas bases fundamentaron la metodología propuesta, y una evaluación de su aplicabilidad en un caso de estudio en una empresa de este sector.
Palabras clave: Gestión - Seguridad - Información – Riesgo – Control – Pymes - Comunicaciones - Gobierno - Tecnología - Guías - Ciberseguridad.

Abstract

At the recent years, computer attacks increasing importantly. These attacks have affected the business sector. One of the most vulnerable sectors to these risks is that conformed by SMEs (Small and medium enterprises). Which, due to their size and financial capacity, suffer from mechanisms for the adoption of international standards and norms related to information security. Adoption of those standards is important for mitigating threats derived from cyber-attacks, at the same time, allow the transformation into an organization that optimizes human resources, towards practices that lead them to manage risks in a more efficient way. This project proposes a methodology based on international standards, which aims to facilitate the design of an information security management system (ISMS) in SMEs, particularly for those in the information and communications sector of the city of Medellín. The development of this The project included a diagnosis of the level of adoption of ISMS in these companies, the analysis of international standards, whose basis were included in the proposed methodology, and an evaluation of its applicability in a case study in a company in this sector.
Keywords: Management - Security - Information - Risk - Control - SMEs - Communications - Government - Technology - Guides - Cybersecurity.

Contenido

Lista de Figuras

Lista de Tablas

1. Introducción

Los ataques informáticos no discriminan el tipo de empresa, suceden tanto en empresas grandes, medianas y pequeñas. Según la empresa internacional de ciberseguridad Kaspersky Lab [1], por intermedio del director del equipo de investigación y análisis para América Latina (Bestuzhev, 2018), se generan 9 ataques de programas maliciosos malware cada segundo, a eso estuvieron expuestos los latinoamericanos durante los últimos años 2017 y 2018. En Latinoamérica, Brasil, Venezuela, Argentina, Guatemala, Perú, Chile, Ecuador, Bolivia, Panamá, Colombia, México y Costa Rica son las más afectadas, con ataques de malware como virus, gusanos, troyanos, phishing y otros programas maliciosos (Kaspersky Lab, 2018), Colombia ocupa el puesto 10 en la región con el 14 % de intentos de ataque por usuario conectado [1].

Esta compañía también reporta que, para el primer trimestre del año 2019, se registró un total de 847 millones de amenazas cibernéticas en América Latina (Kaspersky Lab, 2019)[2]. Por su parte, según lo revela la firma de ciberseguridad Digiware (2017) [3], el coronel de la policía de Colombia de la unidad del cibercrimen (Bautista, 2018) afirma que fueron denunciados 21.687 casos de ciberdelitos, donde el 55 % de los ataques fueron dirigidos a entidades financieras (2018), mientras que, en el año anterior (2017), Colombia presentó 198 millones de ataques para ese mismo periodo, De acuerdo con la compañía citada, diariamente se registran en promedio 542.465 incidentes, y el impacto de los delitos informáticos ha generado pérdidas por 6.179 millones de dólares en el país, donde los sectores más afectados fueron el financiero, con 214.600 ataques por día, seguido de telecomunicaciones, con 138.329; Gobierno, con 83.756 e industria con 51.263 ciberataques. Por otro lado, según el Centro Cibernético Policial (2017)[4], durante el año 2016 se reportaron ante el Departamento de delitos Informáticos de la Policía Nacional de Colombia 7.118 denuncias de delitos asociados a ciberataques, los cuales sucedieron, en la mayoría de los casos, en las Pymes. Este informe también indica que, a pesar de que estos ataques son periódicos, las empresas los intervienen de una forma reactiva, lo que implica que se asume una gestión de riesgo más con fines curativos y no de prevención, trayendo como consecuencia que al no corregir el problema de raíz, a largo plazo resulta siendo un asunto demasiado oneroso para las empresas [5].

Según la ISO/IEC 27001:2013 [6], los sistemas de gestión de seguridad de la información tienen como base la gestión del riesgo empresarial. Sin embargo, un estudio realizado por la Asociación Colombiana de Ingenieros de sistemas en el 2018 (Almanza y Cano, 2018)[7], en

Colombia, aplicado a 234 encuestado, donde se hace una revisión periódica de la seguridad con el siguiente escenario: El 39 % hace una revisión anual, el 34 % entre 2 y 4 evaluaciones al año, y el 9 % realizan más de 4 evaluaciones en el año y el 18 % no realiza ninguna revisión anual. [7].

Adicionalmente, se sabe que un componente de los sistemas de gestión de seguridad de la información (SGSI), es gestionar adecuadamente un gobierno de seguridad; sin embargo, según la Asociación Colombiana de Ingenieros de Sistemas - ACIS (2018) [7], para el año 2018 solo el 39 % de las empresas poseen un directivo a cargo de la seguridad , y en el 18 % de las empresas, la seguridad depende del departamento de sistemas y 21 % depende de otras dependencias de la organización y el 1 % es tercerizado ; por lo cual, la falta de gobierno impulsado desde la alta gerencia es notorio y haría difícil la gestión de seguridad si ésta depende de un área en particular. Así mismo, se indica que el 49 % de las empresas tienen ausencia o falta de una cultura de seguridad de la información, lo que conlleva a que las personas o desconozcan los aspectos relacionados con la seguridad o no exista el personal suficiente para su gestión y gobierno. Además, solo el 58 % de las empresas consideran la ISO/IEC 27001:2013 como importante.

A pesar de que en el mercado se cuenta con los avances tecnológicos para mitigar los ciberataques en las pequeñas y medianas empresas, estas siguen siendo las más afectadas, debido, en parte, a la falta de la adopción de estándares y normas internacionales y estándares de seguridad de la información, como la norma ISO/IEC 27001:2013 [6], el marco de referencia de NIST.SP 800-53r4[8], Cobit 5 [9] para seguridad de la información, ITIL Foundation V3 [10] o MAGERIT versión 3 [11]. Diferentes autores (Shojaie, Federrath & Saberi, 2015 [12]; Santos-Olmo, Sánchez, Caballero, Camacho [13] & Fernández-Medina, 2016; Panjwani, Jäntti & Sormunen [14], 2016), han descrito los principales factores que ocasionan la poca adopción de una cultura de la seguridad de la información en las Pymes, entre los que se destacan: el alto costo de dispositivos y aplicaciones, el alto consumo de recursos de los dispositivos necesarios, la falta de adopción del SGSI, la falta de recurso humano con conocimiento especializado en seguridad, la falta de controles de seguridad y el desconocimiento de las ventajas de los SGSI [15].

En Colombia, según la ley 590 de 2000 [16], las empresas se clasifican en micro, pequeñas, medianas, y grandes empresas. Las medianas empresas son aquellas que cuentan con activos totales por valor de entre 5.001 y 15.000 salarios mínimos legales mensuales vigentes y una planta de personal entre 51 y 200 empleados; la pequeña empresa es la que posee un total de activos por valor entre el rango de 501 y 5001 salarios mínimos legales mensuales vigentes y una planta de personal entre 11 y 50 empleados. Según datos de la Cámara de Comercio en Medellín [17] hay 300 pequeña empresas y 52 medianas empresas dedicadas a la actividad económica de “Información y comunicaciones”. la mayoría de estas pymes, están orientadas

a ofrecer servicios de outsourcing en la administración de la tecnología a otras empresas de otros sectores económicos que no cuentan con un área de tecnología constituida. Por lo anterior, el no contar con una cultura de seguridad de información y la no implementación de SGSIs puede afectar no sólo su unidad de negocio, sino la de otras compañías. Más aún, pueden perder capacidad de contratación debido a que otras empresas, en especial las de mayor tamaño, son exigentes con la implementación de un SGSI para sus contratistas (Medina, Castrol y Pulido, 2017) [18].

Ante esta situación, el desarrollo de estrategias en seguridad de la información en pymes del sector de la información y comunicaciones en la ciudad de Medellín, que plantee un diseño de un SGSI de fácil implementación, es un tema de relevancia y de pertinencia que es susceptible de ser investigado, el cual es abordado en el marco de este trabajo, tal como lo reflejan los objetivos planteados, que se presentan a continuación.

1.1. Objetivos

1.1.1. Objetivo general

Proponer una metodología, basado en estándares internacionales, que facilite la implementación de un sistema de gestión de la seguridad de la información en pequeñas y medianas empresas del sector de la información y comunicaciones de la ciudad de Medellín, la cual debe abarcar gobierno seguridad, identificación de activos, análisis de riesgos, plan de tratamiento de riesgos y mejora continua.

1.1.2. Objetivos específicos

- Realizar un diagnóstico que identifique los factores del nivel de adopción de estándares internacionales y la implementación de un sistema de gestión de seguridad de la información en las pequeñas y medianas empresas del sector de la información y comunicaciones de la ciudad de Medellín.

- Analizar los resultados obtenidos en el diagnóstico con el fin de seleccionar la propuesta más adecuada que se acomode a los intereses de las empresas objeto de estudio.

- Evaluar la aplicabilidad de la metodología para la implementación de un sistema de gestión de seguridad de la información en un caso de estudio de una pyme del sector de la información y comunicaciones de Medellín.

- Analizar los resultados obtenidos en la implementación de la metodología del sistema de gestión de seguridad de la información en el caso de estudio, para determinar su aplicabilidad y generar conclusiones generales para otras empresas del sector.

1.2. Estructura del documento

Este documento se estructura de la siguiente manera: en el capítulo 2, se introducen algunos conceptos relevantes para la comprensión general de los aspectos desarrollados en este trabajo, como son la clasificación de las empresas en Colombia, y el concepto de sistema de gestión de seguridad de la información y sus componentes. El capítulo 3, presenta el estudio realizado para determinar el estado actual de adopción de estándares e implementación de SGSIs en las pequeñas y medianas empresas del sector de la información y las comunicaciones de la ciudad de Medellín; se describe tanto el estudio realizado, como los resultados y conclusiones del mismo. El capítulo 4, presenta la propuesta de metodología de implementación de SGSIs para pymes del sector de la información y comunicaciones de la ciudad de Medellín, el cual se compone de dos secciones principales, la primera, un análisis de normas y metodologías aceptadas internacionalmente para SGSIs y gestión de riesgos, y la segunda, la propuesta de SGSI que se soporta tanto en las necesidades identificadas en el estudio presentado en el Capítulo 3, como en los análisis de estándares. El capítulo 5, presenta un caso de estudio de la aplicabilidad de la metodología propuesta en una empresa del sector, el análisis de los resultados y las conclusiones y recomendaciones para su aplicación en otras empresas del sector. Finalmente, el Capítulo 6, presenta las conclusiones generales de este trabajo y propone algunos trabajos futuros que se pueden desarrollar a partir de los resultados obtenidos.

2. Marco conceptual

2.1. Sistema de gestión de la seguridad de la información (SGSI)

Un sistema de gestión de la seguridad de la información (SGSI), definido por la norma ISO/IEC 27001:2013 [6], no sólo debe considerar el contexto de la industria y características culturales de la organización, sino que también debe ser sostenible en el tiempo, con capacidad de incorporar mejoras de forma incremental y continua, con un beneficio comprobable para la organización. Para ello se requiere de una metodología bien definida que acompañe el dinamismo necesario de la empresa/organización y de la industria y a su vez respete las estrategias empresariales y vinculación estructural (Pallas, Corti, 2009 [19])

2.2. Estándares internacionales del SGSI

2.2.1. Norma ISO/IEC 27001:2013

La norma ISO/IEC 27001:2013 [6] (Compendio seguridad de la información marzo 2013) es un estándar que especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de seguridad de la información - SGSI (Parra-Giraldo, 2015) [20], que procura porque los aspectos trabajados dentro del SGSI se ajusten con las necesidades de la organización.
Segun la norma ISO/IEC 27001:2013 plantea que los sistemas de informacion [6] promueve un enfoque basado en procesos, adoptando el modelo de Deming, en el que se plantea un ciclo de mejora continua a través de la repetición de las fases de (Planificar- Hacer - Verificar - Actuar) conocido como PHVA (o PDCA, por sus siglas en inglés "Plan-Do-Check-Act) [21].

2.2.2. Nist.SP800-53r4 - Guía de controles de seguridad para los sistemas de información federales

Según lo planteado por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos la guía NIST.SP 800-53r4 es un marco de referencia, el cual contiene una serie de

publicaciones, en el cual se recomienda controles de seguridad para sistemas de información federales, organizaciones y documenta controles de seguridad para todos los sistemas federales de información, excepto los diseñados para la seguridad nacional, (2013) [22]

2.2.3. ISM3

ISM3 es un modelo de madurez de administración de la seguridad de la información publicado por The Open Group [23], líder en el desarrollo de estándares y certificaciones de TI abiertas. Como indica (Vicente, 2011) gerente de sistemas informáticos abiertos y director del consorcio ISM3 de The Open Group, El estándar O-ISM3 define los procesos de seguridad para administrar el Sistema de gestión de la seguridad de la información de una empresa. El estándar O-ISM3 (por las siglas en inglés de Information Security Management) asigna la responsabilidad del negocio para definir sus objetivos de seguridad empresarial requeridos en su política de seguridad, y luego ofrece un conjunto de procesos de administración de seguridad, desde los cuales el negocio selecciona cuáles implementar en un ISMS coherente. Cada proceso de control de seguridad en el ISMS luego devuelve métricas para indicar qué tan bien está contribuyendo ese proceso para alcanzar los objetivos de seguridad del negocio. La retroalimentación de métricas estándar O-ISM3 es una característica diferenciadora importante en comparación con otros sistemas ISMS [23].

2.2.4. COBIT ver5

Cobit ver5 [9], proporciona un marco integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de los activos de información y tecnología, definido y actualizado por ISACA (Asociación de Auditoría y Control de Sistemas de Información), ayudando a las empresas a crear un valor óptimo de TI manteniendo un equilibrio entre la obtención de beneficios y la optimización de los niveles de riesgo y el uso de los recursos. COBIT 5 [9] permite que las TI sean gobernadas y administradas de manera holística, abarcando las áreas de responsabilidad funcional y de TI de extremo a extremo, considerando los intereses relacionados con TI de los interesados internos y externos. COBIT 5 es genérico y útil para empresas de todos los tamaños, ya sean comerciales, sin fines de lucro o en el sector público.

2.3. Metodologías de riesgos

El comité nacional para el conocimiento del riesgo SNGRD en Colombia en su terminología sobre gestión del riesgo de desastres y fenómenos amenazantes define el riesgo [24] como la

probabilidad que ocurra una desastre o daño de forma negativa. Así, un riesgo está compuesto por dos factores, el primero son las vulnerabilidades o una ausencia de control (Físico o Lógico), la segunda son las amenazas. Por separado no representan un peligro peros si se juntan se convierten en un riesgo (2017)[25] y (Ley 1523 de 2012).

2.3.1. Gestion de riesgos

Como indica la organización internacional de normalización ISO en su norma ISO 31000:2018 gestión de riesgos es el proceso de preparación en el cual se planifica, y se organiza los recursos humanos, tecnológicos y materiales de la organización, para el desarrollo de las actividades de la gestión de riesgos [26] (identificación, análisis, evaluación y tratamiento del riesgo) [27], con el objetivo de prevenir desastres, reducir al mínimo los riesgos e incertidumbres a los que están expuestos las organizaciones.

2.3.2. DAFP versión 4

El departamento administrativo de la función pública de la República de Colombia DAFP define y actualiza la guía para la administración de gestión del riesgo, la cual se encuentra en su versión 4 de (2018) [28] y a través del Decreto 1537 de 2001 [29]. Esta es determinada como una metodología de gestión del riesgo organizacional para las entidades públicas las cuales deben contar con una política de gestión de riesgos apuntando a los riesgos de corrupción y seguridad digital (2018).

2.3.3. Nist 800-30 Rev.1 - Guía de gestión de riesgos para sistemas de tecnología de la información

Esta es una guía [5] para realizar evaluaciones de riesgos de los sistemas de información y organizaciones federales de los Estados Unidos. De acuerdo a esta guía, las evaluaciones de riesgos, realizadas en los tres niveles en la jerarquía de gestión de riesgos, son parte de un proceso general de gestión de riesgos, que proporciona a los líderes / ejecutivos senior la información necesaria para determinar los cursos de acción adecuados en respuesta a los riesgos identificados. Esta guía brinda información sobre la selección de controles de seguridad rentables, los cuales pueden ser usados para mitigar el riesgo, para una mejor protección de la información de misión crítica y los sistemas de TI que procesan, almacenan y transportan esta información (Publicada por la Nist en el 2012).

2.3.4. OCTAVE

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), es una metodología desarrollada por la empresa Computer Emergency Response Team (CERT) desde el (2001) [30], que corresponde a una método de planificación y consultoría estratégica en seguridad de la información basada en riesgo, la cual realiza una verificación y validación a los riesgos que afectan a la seguridad de la información, incluyendo los aspectos organizaciones y técnicos.

Para cualquier iniciativa de mejora frente a la seguridad de la información, se requiere un análisis previo que permita ver de forma transversal a la organización y los riesgos potenciales, con esto se obtiene una base para entender e implementar dichas mejoras.

A diferencia de metodologías tradicionales, Octave se enfoca en los riesgos tecnológicos y temas tácticos pasando por la estrategia y practica organizacional, dando peso a la gobernabilidad de las TIC en las organizaciones.

2.3.5. MAGERIT

Magerit es una metodología de análisis y gestión de riesgos de los sistemas de información[11], la entidad responsable de las actualizaciones y publicaciones es el Ministerio de Hacienda y Administraciones Públicas de España, secretaria de estado y administraciones públicas, la cual es emplea el método de gestión de riesgo dentro de un marco de trabajo para que las unidades de gobierno realicen dictámenes teniendo en cuenta los riesgos derivados de las tecnologías de información.

Los objetivos que persigue esta metodología se enfocan en sensibilizar a los responsables de la información con la existencia de los riesgos y que es imperativo gestionarlos, presentar un método sistemático para analizar los riesgos resultantes del uso de la TIC y ayuda a describir y planificar el tratamiento para mantener el riesgo controlado.

El Ministerio de Hacienda y Administraciones Públicas de España, secretaria de estado y administraciones públicas indica que la versión de Magerit v3 liberada en (octubre de 2012), los derechos de uso de la metodología son de uso libre y no requiere autorización previa. En cualquier explotación de la obra se hará constar la autoría original de (2012) [11]
.

2.3.6. ISO 27005:2018

ISO27005:2018 [31] proporciona directrices para la gestión de riesgos de seguridad de la información, elaborada y actualizada por la organización internacional de normalización ISO dicha publicación en (julio de 2018). Es compatible con los conceptos generales especificados en ISO / IEC 27001 [6] y está diseñado para ayudar a la implementación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

El conocimiento de los conceptos, modelos, procesos y terminologías descritos en ISO / IEC 27001 e ISO/IEC 27002 [32] es importante para una comprensión completa de ISO/IEC 27005:2018.

ISO/IEC 27005:2018 es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que pretenden gestionar los riesgos que podrían comprometer la seguridad de la información de la organización.

2.3.7. ISO 31000

ISO 3100:2018 [26] es una técnica de gestión del riesgo - directrices, proporciona principios, marco y un proceso para gestionar el riesgo, dada por la organización internacional de normalización ISO dicha publicación en (febrero de 2018). La cual puede ser aplicada por cualquier organización, independientemente de su tamaño, actividad o sector.

El uso de ISO 31000 puede ayudar a las organizaciones a aumentar la probabilidad de lograr objetivos, mejorar la identificación de oportunidades y amenazas, y asignar y utilizar de manera efectiva recursos para el tratamiento de riesgos.

Sin embargo, ISO 31000 no se puede utilizar con fines de certificación, pero proporciona una guía para los programas de auditoría internos o externos. Las organizaciones que lo utilizan pueden comparar sus prácticas de gestión de riesgos con un punto de referencia reconocido internacionalmente, proporcionando principios sólidos para la gestión eficaz y el gobierno corporativo.

2.4. Clasificación de las empresas en Colombia

En Colombia, según la ley 590 de 2000 [16], las empresas se clasifican en microempresas, Pymes, compuestas por pequeñas y medianas empresas, y grandes empresas; esta clasificación se define según el número de trabajadores y el total de activos valorados sobre el salario

mínimo mensual legal vigente (SMMLV), como se muestra en la Tabla **2-1**

Clasificación	**Número de trabajadores**	**Valoración de activos Totales SMMLV**
Microempresa	Menores a 10	Inferior a quinientos uno (501) SMMLV.
Pyme (Pequeña Empresa)	Entre 11 y 50	Entre quinientos uno (501) y menos de cinco mil (5.001) SMMLV.
Pyme (Mediana Empresa)	Entre 51 y 200	Entre cinco mil uno (5.001) y quince mil (15.000) SMMLV.
Grandes Empresas	Mayor a 200	Mayor o igual a quinientos un mil (15.001) SMMLV.

Tabla 2-1.: Fuente: Ley 590 del 2000. Marco de acción para la pequeña y mediana empresa

2.5. Sector económico

La CIIU [33] es la clasificación industrial internacional uniforme elaborada y divulgada por el departamento de asuntos económicos y sociales en conjunto con la división de estadística de la Organización de las Naciones Unidas (ONU) (Rev. 4 del 2009)[34]; La CIIU tiene por finalidad establecer una clasificación uniforme de las actividades económicas productivas agrupadas en (categorías y actividad sector económico) la cual se encuentra adoptada por los países desde el año 1948, para el caso de Colombia la (Rev. 4 del 2009) liberada por la ONU es aplicada por el Departamento Administrativo Nacional de Estadística (DANE) [35] en (marzo de 2012) brindando esta clasificación con el ánimo de que sea utilizada como estándar para la recolección, la codificación y el análisis de la información estadística en materia de actividades económicas, para las diferentes investigaciones, cuentas nacionales, encuestas, censos, registros administrativos y estudios sectoriales. Así se podrá disponer de una información estadística confiable y oportuna, en las regines es adoptada por las Camara de Comercio [17] donde cada empresa realiza y actualiza su certificado de industria y comercio.

3. Estado de la implementación de SGSIs en PyMEs del sector de la información y comunicaciones de la cuidad de Medellín

En este capítulo se presenta el estudio realizado para establecer el nivel de adopción de estándares e implementación de sistemas de gestión de seguridad de la información en pequeñas y medianas empresas del sector de las tecnologías de información y comunicaciones de la ciudad de Medellín (Colombia). Este estudio se llevó a cabo mediante una encuesta, realizada a un conjunto de empresas de este sector, según registro de la Cámara de Comercio de Medellín para Antioquia. La encuesta fue realizada vía formulario electrónico. Con el fin de tener una muestra significativa, se envió invitación a todas las empresas de las que se obtuvó información de contacto. Sin embargo, sólo 45 de ellas dieron respuesta a la invitación, y 40 diligenciaron el formulario completo.

3.1. Identificación y selección de empresas participantes

Para este estudio, se realizó una encuesta en las PyMEs del sector de la información y las comunicaciones en la ciudad de Medellín, registradas en la Cámara de Comercio de Medellín para Antioquia, cuyas activiades, según CIIU [33], se enumeran en la Tabla **3-1**. Para este caso, se considerarón las actividades de las divisiones 61, 62 y 63.

Div.	Grupo	Clase	Descripción Sector (información y comunicaciones)
58			Actividades de edición
	581		Edición de libros, publicaciones periódicas y otras actividades de edición
		5811	Edición de libros
		5812	Edición de directorios y listas de correo
		5813	Edición de periódicos, revistas y otras publicaciones periódicas
		5819	Otros trabajos de edición
	582	5820	Edición de programas de informática (software)

59			Actividades cinematográficas, de video y producción de programas de televisión, grabación de sonido y edición de música
	591		Actividades de producción de películas cinematográficas, video y producción de programas, anuncios y comerciales de televisión
		5911	Actividades de producción de películas cinematográficas, videos, programas, anuncios y comerciales de televisión
		5912	Actividades de posproducción de películas cinematográficas, videos, programas, anuncios y comerciales de televisión
		5913	Actividades de distribución de películas cinematográficas, videos, programas, anuncios y comerciales de televisión
		5914	Actividades de exhibición de películas cinematográficas y videos
	592	5920	Actividades de grabación de sonido y edición de música
61			Telecomunicaciones
	611	6110	Actividades de telecomunicaciones alámbricas
	612	6120	Actividades de telecomunicaciones inalámbricas
	613	6130	Actividades de telecomunicación satelital
	619	6190	Otras actividades de telecomunicaciones
62			Actividades de programación, transmisión y/o difusión
	620		Desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas), consultoría informática y actividades relacionadas
		6201	Actividades de desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas)
		6202	Actividades de consultoría informática y actividades de administración de instalaciones informáticas
		6209	Otras actividades de tecnologías de información y actividades de servicios informáticos
63			Actividades de servicios de información
	631		Procesamiento de datos, alojamiento (hosting) y actividades relacionadas; portales web
		6311	Procesamiento de datos, alojamiento (hosting) y actividades relacionadas
		6312	Portales web
	639		Otras actividades de servicio de información
		6391	Actividades de agencias de noticias
		6399	Otras actividades de servicio de información n.c.p.

Tabla 3-1.: Estructura detallada CIIU (Sector información y comunicaciones sección J)

Como se detalla en la Tabla **3-2**, de acuerdo a la Cámara de Comercio de Medellín para Antioquia, para el año 2017 se encuentran registradas 304 empresas, las cuales fueron invitadas a participar en el estudio.

Código CIIU	**Descripción Actividad Económica**	**Cantidad**
6110	Actividades de telecomunicaciones alámbricas	6
6120	Actividades de telecomunicaciones inalámbricas	1
6190	Otras actividades de telecomunicaciones	33
6201	Actividades de desarrollo de sistemas informáticos planificación, análisis, diseño, programación, pruebas	126
6202	Actividades de consultoría informática y actividades de administración de instalaciones informáticas	57
6209	Otras actividades de tecnologías de información y actividades de servicios informáticos	43
6311	Procesamiento de datos, alojamiento hosting y actividades relacionadas	12
6312	Portales web	4
6399	Otras actividades de servicio de información n.c.p.	22
	Total	304

Tabla 3-2.: Cantidad de PyMEs registradas ante la Cámara de Comercio de Medellín para Antioquia en el sector de información y comunicaciones - Fuente: Base de datos de los registros mercantiles registrados ante Cámara de Comercio de Medellín

3.2. Diseño del instrumento

Se diseñó una encuesta con preguntas que permitieran identificar tanto el nivel de adopción de SGSIs, como la percepción de riesgo e importancia que estas empresas dan a la seguridad de la información. Se realizó un diseño inicial del instrumento, el cual fue sometido a un proceso de validación inicial, por estudiantes y profesores de la Maestría en Seguridad Informática del Instituto Tecnológico Metropolitano de Medellín. El propósito de esta evaluación inicial fue validar que las preguntas del instrumento propuesto fueran comprensibles, además de obtener sugerencias de mejora por personas conocedoras del tema y con posible experiencia en implementación de SGSIs.

La encuesta se elaboró en un formulario electrónico y se envió invitación a 10 personas, 5 profesores y 5 estudiantes de último semestre de la Maestría en Seguridad Informática, obteniéndose respuesta de nueve de ellos. Además de las preguntas establecidas, se les pidió diligenciar un campo de comentarios, que permitió obtener una valiosa retroalimentación, la cual se tradujo en una versión mejorada del instrumento (Ver Anexo de Resultado de la

Encuesta Docentes y Estudiantes.pdf).

A partir de las observaciones realizadas por los nueve participantes, se estableció la estructura final de la encuesta a aplicar a las empresas identificadas, la cual se presenta en el Anexo A. Esta encuesta está conformada por preguntas cerradas y de selección múltiple, agrupadas por secciones, abarcando los datos de las empresas, los componentes del sistema de seguridad de la información y los factores que impiden la adopción de un SGSI. Su gestión fue vía Web a través de la plataforma de formularios de Google. La invitación fue enviada a la información de contacto de cada una de las empresas, sin embargo se solicito que fuera diligenciada por la persona que pudiera informar sobre la gestión de seguridad de la información o en su defecto sobre los sistemas de TI de la empresa.

La encuesta estuvo dividida en las siguientes secciones:

1. Consentimiento Informado de la encuesta.
2. Información de la empresa.
3. Activos de información.
4. Amenazas informáticas.
5. Incidentes informáticos.
6. Sistema de gestión de la información "SGSI".
7. Administración del riesgo.
8. Políticas de seguridad de la información.
9. Controles de seguridad informática.
10. Factores que afectan la implementación del sistema de seguridad de la información en la compañía.

Los participantes fueron notificados vía correo electrónico institucional. La información para el envío de los correos fue suministrada por la Cámara de Comercio de Medellín para Antioquia, obteniendo los siguientes datos: Matrícula, Tipo de sociedad, Codigo CIIU, Descripción Actividad Económica, NIT / Cédula, Nombre / Razón Social, SIGLA, Cédula Rep. Legal, Representante Legal, Teléfono 1, Teléfono 2, Fax, E-mail 1, Dirección, Municipio, Comuna, Barrio, Fecha Inicio, Fecha Ultima Renovación, No. Personas, No. Establ., Valor Activos Renovación, NIT importador, NIT exportador, tamaño, antigüedad, actividad económica, grupo actividad económica, Descripción Tipo de Sociedad, Estado del Correo 06 abril, Correos alternos y Notas, Observaciones del segundo informe, llamada, Numero.

3.3. Resultados

A continuación, se presenta el informe correspondiente a los resultados de la encuesta de diagnóstico sobre la adopción e implementación del sistema de gestión de la seguridad de la información en las PyMEs del sector de la información y las comunicaciones de la ciudad de Medellín, la cual fue lanzada el día 06 de abril de 2018 y se cerró el día 24 de abril de 2018.

3.3.1. Consentimiento informado

Se realizó invitación para participación en la encuesta a 304 empresas del sector de la información y comunicaciones de la ciudad de Medellín, al realizar el cierre se obtienen 45 resultados, 5 de estas empresas decidieron no contestar la encuesta, y 40 empresas diligenciaron la encuesta en su totalidad (Tabla **3-3**). De acuerdo a lo anterior, los resultados de esta encuesta presentan un nivel de confianza del 85 %, con un margen de error del 10 %, suponiendo una distribución normal y con un nivel de implementación en el 50 % de los casos, dado que no se encuentran reportes previos que permitan establecer una distribución más ajustada [36].

Opción de respuesta	**No.Cantidad de respuestas**	**Porcentaje**
No responderé el cuestionario	5	11 %
NSí responderé el cuestionario	40	89 %
Total General	45	100 %

Tabla 3-3.: Resultado de concentimiento informado

3.3.2. Información de la empresa

Tamaño de la empresa

Con el fin de confirmar que la empresa participante correspondía a una PyME, se solicitó al encuestado indicar el tamaño de su empresa, según el número de empleados que laboran en ella. En Colombia, según la ley para el fomento de la micro, pequeña y mediana empresa, la ley 590, las PYMES se clasifican así:

- Microempresa: Personal no superior a 10 trabajadores. Activos totales inferior a 501 salarios mínimos mensuales legales vigentes.
- Pequeña Empresa: Personal entre 11 y 50 trabajadores. Activos totales mayores a 501 y menores a 5.001 salarios mínimos mensuales legales vigentes.
- Mediana: Personal entre 51 y 200 trabajadores. Activos totales entre 5.001 y 15.000 salarios mínimos mensuales legales vigentes.

Como lo muetra la Tabla **3-4**, la mayoría de las empresas que respondieron la encuesta (55 %) corresponden a pequeñas empresas, un 30 % corresponde a empresas medianas y un 15 % a microempresas. Se confirmó que todoas las empresas participantes pertenecían al grupo de las PyMEs.

Opción de respuesta	No. Empleados	Porcentaje
Menos de 10 empleados	6	15 %
Entre 11 a 50 empleados	22	55 %
Entre 51 y 200	12	30 %
Más de 200	0	0 %
Total General	40	100 %

Tabla 3-4.: Número de empleados de las PyMEs participantes en la encuesta

Actividad económica de la empresa

Con el fin de confirmar que las empreas participantes se encontraban en el sector de la información y las comunicaciones, se le solicitó al encuestado indicar la actividad económica de la empresa, mostrando como opción todas aquellas actividades que hacen parte de este sector, según la Camara de Comercio de Medellín para Antioquía (Ver Tabla **3-1**).

Como se observa en la Tabla **3-5**, un mayor número de las PyMEs participantes se dedican al desarrollo de sistemas informáticos, planificación, análisis, diseño, programación y pruebas (7); las demás actividades tienen una participación dispersa de empresas (1 a 3).

Actividad económica	Empresas
Desarrollo de sistemas informáticos planificación, análisis, diseño, programación, pruebas	7
Actividades de tecnologías de información y actividades de servicios informáticos	3
Consultoría informática y actividades de administración de instalaciones informáticas	3
Consultoría informática y actividades de administración de instalaciones informáticas, Desarrollo de sistemas informáticos planificación, análisis, diseño, programación, pruebas, Actividades de servicio de información, Actividades de tecnologías de información y actividades de servicios informáticos	2

Consultoría informática y actividades de administración de instalaciones informáticas, Desarrollo de sistemas informáticos planificación, análisis, diseño, programación, pruebas, Actividades de tecnologías de información y actividades de servicios informáticos	2
Consultoría informática y actividades de administración de instalaciones informáticas, Actividades de tecnologías de información y actividades de servicios informáticos, Actividades de telecomunicaciones, Telecomunicaciones alámbricas, Telecomunicaciones inalámbricas	1
Desarrollo de sistemas informáticos planificación, análisis, diseño, programación, pruebas, Actividades de tecnologías de información y actividades de servicios informáticos, Portales web, Procesamiento de datos, alojamiento hosting y actividades relacionadas	1
Desarrollo de sistemas informáticos planificación, análisis, diseño, programación, pruebas, Actividades de tecnologías de información y actividades de servicios informáticos	1
Consultoría informática y actividades de administración de instalaciones informáticas, Actividades de tecnologías de información y actividades de servicios informáticos, Telecomunicaciones alámbricas, Telecomunicaciones inalámbricas	1
Desarrollo de sistemas informáticos planificación, análisis, diseño, programación, pruebas, Procesamiento de datos, alojamiento hosting y actividades relacionadas	1
Actividades de telecomunicaciones	1
Desarrollo de sistemas informáticos planificación, análisis, diseño, programación, pruebas, Actividades de servicio de información, Portales web, Procesamiento de datos, alojamiento hosting y actividades relacionadas	1
Consultoría informática y actividades de administración de instalaciones informáticas, Desarrollo de sistemas informáticos planificación, análisis, diseño, programación, pruebas, Actividades de servicio de información, Actividades de tecnologías de información y actividades de servicios informáticos, Procesamiento de datos, alojamiento hosting y actividades relacionadas, Otra Actividad	1
Desarrollo de sistemas informáticos planificación, análisis, diseño, programación, pruebas, Actividades de tecnologías de información y actividades de servicios informáticos, Otra Actividad	1
Telecomunicaciones alámbricas	1

Desarrollo de sistemas informáticos planificación, análisis, diseño, programación, pruebas, Actividades de telecomunicaciones, Portales web, Procesamiento de datos, alojamiento hosting y actividades relacionadas, Telecomunicaciones alámbricas, Telecomunicaciones inalámbricas	1
Actividades de servicio de información, Actividades de tecnologías de información y actividades de servicios informáticos	1
Desarrollo de sistemas informáticos planificación, análisis, diseño, programación, pruebas, Telecomunicaciones inalámbricas	1
Consultoría informática y actividades de administración de instalaciones informáticas, Actividades de tecnologías de información y actividades de servicios informáticos	1
Consultoría informática y actividades de administración de instalaciones informáticas, Actividades de tecnologías de información y actividades de servicios informáticos	1
Desarrollo de sistemas informáticos planificación, análisis, diseño, programación, pruebas, Actividades de servicio de información, Actividades de tecnologías de información y actividades de servicios informáticos, Portales web, Procesamiento de datos, alojamiento hosting y actividades relacionadas	1
Consultoría informática y actividades de administración de instalaciones informáticas, Desarrollo de sistemas informáticos planificación, análisis, diseño, programación, pruebas, Actividades de tecnologías de información y actividades de servicios informáticos, Actividades de telecomunicaciones, Telecomunicaciones alámbricas, Telecomunicaciones inalámbricas	1
Otra Actividad	6
Total general	40

Tabla 3-5.: Actividad económica de las empresas participantes en la encuesta, según la clasificación CIIU

Seis empresas indicaron dedicarse a otra actividad económicas. En este caso se solicitó a los encuestados especificar la actividad. La Tabla **3-6**, indica las respuestas en estos casos, las cuales, como se puede observar, también corresponden al sector económico de la información y comunicaciones.

Provisión de servicios de SOC, CI y NOC
Consultorías para el diagnóstico, modelado, diseño y mejora de procesos de negocio
Asesoría, consultoría, análisis, diseño, implantación, capacitación en soluciones tecnológicas basadas en ingeniería de procesos, software, hardware, servicios y telecomunicaciones.
Network Marketing
Servicios de comunicación estratégica
Solucions de software
Prestación de servicios de implementación de normas y modelos de calidad

Tabla 3-6.: Otras actividades económicas a que se dedican las empresas encuestadas

Pérfil de los encuestados

Los encuestados que diligenciaron la encuesta fueron en su gran mayoría Gerentes(17), seguido de directores de diferentes ares, como operaciones, proyectos, financieras, I+D, entre otros (7), Coordinadores de diferentes áreas, como gestión humana, contabilidad, tecnología de la información, entre otras (6), los otros 10 se distribuyerón entre ingenieros, líderes de área, auxiliares, jefes y consultores, todos estos correspondientes a las áreas de tecnologías de la información y comunicaciones, como se refleja en la tabla **3-7** (rol de los participantes de la encuesta). Es importante mencionar que, al realizar la invitación para responder la encuesta, se le indicó a quien la recibía, el objetivo de la misma y se le solicitó enviar a quien ellos considerarán era la persona idónea para responder. En este sentido, es relevante resaltar la importancia que le dan los gerentes, directores y encargados del área de las tecnologías de la información y comunicaciones al contestar la encuesta, lo que indica un interés de estos por el tema.

3.3.3. Activos de información

Nivel de importancia que le da la empresa a los activos de información

Los encuestados les dan una alta importancia a los activos de información de sus organizaciones (85 %), mientras que el 15 % consideran que estos tienen una importancia media, esto incluye un gerente general, un consultor de procesos, un coordinador de contabilidad, un coordinador de calidad y talento humano, un jefe de sistemas y un coordinador de TI . Ninguno de los encuestados asignó una importancia baja, lo que indica que los activos de información son relevantes para las pymes para la toma de daciones y para su operación y funcionamiento.

Rol	Encuestados
Gerente, gerente general, gerente de línea - gestión de procesos y servicios, gerente de servicios de tecnología	17
Directora de proyectos y calidad, director de operaciones, director financiero, director general, director I+D, CEO (Director operativo)	7
Coordinador de calidad y talento humano, coordinador de contabilidad, coordinadora de gestión humana	4
Coordinador de TI, coordinador aseguramiento calidad de software	2
Ingeniero de soporte, ingeniero de servicios	3
Líder TI	2
Auxiliar de soporte, auxiliar administrativo	2
Administrador de sistemas de información	1
Jefe de sistemas	1
Consultor de procesos	1
Total general	40

Tabla 3-7.: Rol de los participantes de la encuesta

Opción de respuesta	Cantidad de respuestas	Porcentaje
Alta	34	85 %
Media	6	15 %
Baja	0	0 %
Total General	40	100 %

Tabla 3-8.: Nivel de importancia que da la empresa a los activos de información

Nivel de importancia que dan los empleados a la información que manejan

En este punto la percepción de los encuestados sobre la importancia que le dan los empleados a la información que manejan en las empresas está entre alta, con 48 %, y media, con 47 %; tan sólo el 5 % de los encuestados consideran que estos le dan una importancia baja a la información. Cabe aclarar, que esta respuesta corresponde a la percepción del encuestado y no a la realidad de las empresas, para tener una percepción más realista al respecto, se requeriría realizar una encuesta a una muestra de estos empleados, lo cual estaba fuera del alcance de este estudio. Resulta en todo caso inquietante, que dado el sector económico de las empresas, más de la mitad de los encuestados consideren que sus empleados no le dan una importancia alta a la información que manejan.

Opción de respuesta	Cantidad de respuestas	Porcentaje
Alta	19	48 %
Media	19	47 %
Baja	2	5 %
Total General	40	100 %

Tabla 3-9.: Nivel de importancia le dan sus empleados a la información que estos manejan

Personal dedicado a la seguridad de la información y su formación

Se indagó sobre si la empresa contaba con una persona responsable de la seguridad de la información. 21 empresas, que corresponde al 52 % de los encuestados, indicarón que cuentan con un responsable de la seguridad de la información y un 48 % no (tabla **3-10**). Estos resultados contrastan con los de la pregunta ¿la persona encargada de la seguridad de la información tiene formación especializada en el área? (tabla **3-11**), pues en tan sólo 12 de ellas, la persona tiene formación especializada. Lo que implica que aún cuando se asignan responsables, estos no cuentan con la formación requerida para cumplir esta función.

Opción de respuesta	Cantidad de respuestas	Porcentaje
Si	21	52 %
No	19	48 %
Total General	40	100 %

Tabla 3-10.: Empresas que cuentas con un responsable de la seguridad de la información

Opción de respuesta	Cantidad de respuestas	Porcentaje
No	23	58 %
Si	12	30 %
No Sabe	5	13 %
Total General	40	100 %

Tabla 3-11.: Formación especializada del responsable de la seguridad de la información

3.3.4. Amenazas informáticas

Conocimiento sobre los tipos de amenazas informáticas que pueden afectar la empresa

El 90 % de los encuestados declaran que conocen los tipos de amenazas informáticas a los cuales se enfrentan las empresas, que ponen en riesgo la información (**3-12**). De nuevo, es

preocupantes que un 10 % de los encuestados, ni siquiera considere tener conocimiento de estas amenazas, dado el sector al que pertenecen las empresas.

Opción de respuesta	Cantidad de respuestas	Porcentaje
Si	36	90 %
No	4	10 %
Total General	40	100 %

Tabla 3-12.: Conocimiento de los encuestados sobre los diferentes tipos de amenazas informáticas que pueden afectar la empresa

Percepción de riesgo sobre amenazas informáticas

Los encuestados reconocen que existen amenazas informáticas que ponen en riesgo la información de las empresas. De acuerdo a los resultados, los 36 encuestados que declararon tener conocimiento sobre las amenazas informáticas que pueden afectar la empresa, reconocen los Virús informáticos o código malicioso, como una amenaza para su empresa, le siguen robo y pérdida de información con 34 y 31 empresas, respectivamente.

La Tabla **3-13** presenta, en forma descendente, el número de empresas que considera que las amenazas listadas pueden llegar a afectar la empresa. Cabe mencionar que en este pregunta se permitía indicar otras amenazas, obteniéndose como respuestas *phishing* y *cracking*. Para el caso del *phishing*, se considera que hace referenica al término informático para referirse a la suplantación de identidad, mientras que el caso de *cracking*, se asume que el encuestado hace referencia al hecho de quebrar la seguridad del software que la empresa distribuye.
En este punto, cuestiona que sólo el 55.5 % de las empresas reconozca como amenaza la suplantación de identidad, una amenaza bastante frecuente en la actualidad; o que tan sólo el 42.5 %, reconozca la posible amenaza de los desastres naturales. Así mismo, llama la atención que tan sólo 12 empresas reconozcan la amenaza de denegación de servicio, cuando 11 de ellas han sufrido este tipo de incidente, como se verá más adelante.

3.3.5. Incidentes informáticos

Incidentes informáticos en empresas participantes

Aunque 16 de las empresas declararón no haber sufrido ningún ataque informático, 26 de ellas si han sufrido uno o más de ellos. El incidente de seguridad que más se ha presentado es la infección por malware (virus o malware de tipo ransonware), con 12 empresas, seguido por indisponibilidad del servicio, la pérdida de información, la suplantación del sitio Web,

Amenazas	Respuestas
Virús informáticos o código malicioso	36
Robo de información	34
Pérdida de información	31
Divulgacón de información	28
Fuga de información	28
Uso no autorizado de sistemas informáticos	27
Suplantación del sitio Web de la empresa	22
Alteración de la información	22
Indisponibilidad de servicio	22
Suplantación de identidad	20
Fráudes basados en el uso de computadores	19
Desastres naturales	17
Sabotaje, vandalismo	17
Espionaje	15
Ataques de fuerza bruta	14
Denegación de servicio	12
Phishing	1
Cracking	1

Tabla 3-13.: Percepción sobre amenazas informáticas que podrían afectar la información de las empresas

accesos no autorizados y la fuga de información. En este caso, aunque se permitía informar otro tipo de incidente, no se indicó ningún otro.

3.3.6. Sistema de gestión de la información - SGSI

Importancia de la seguridad de la información

El 90 % de los encuestados consideran que la seguridad de la información en sus empresas es muy importante, y el 10 % consideran que es medianamente importante. Si bien estos resultados demuestran que la seguridad de la información no es indiferente para las empresas. De nuevo, se esperaría que, dado el sector económico en estudio, todas las empresas considerarán este como un factor muy importante. Este resultado, sin embargo, se explica en el posible desconocimiento sobre las amenazas informáticas que pueden afectar las empresas.

Tipo de Incidentes Informáticos sufridos	Cantidad
No he sufrido ataque informático	16
Infecciones de Malware (Virus o Malware de tipo Ransonware)	12
Indisponibilidad del servicio	11
Perdida de información	7
Suplantación a su sitio Web	4
Accesos no autorizados a la información	4
Fuga de información	3

Tabla 3-14.: Incidente informático sufridos

Opción de respuesta	Cantidad de respuestas	Porcentaje
Muy importante	36	90 %
Medianamente importante	4	10 %
De importancia baja	0	0 %
Total General	40	100 %

Tabla 3-15.: Importancia de la seguridad de la información en las empresas

Conocimiento del concepto de Sistema de Gestión de Seguridad de la Información

De acuerdo a la encuesta realizada (Tabla 3.3.6, el 63 % de los participantes conocen qué es un sistema de gestión de seguridad de la información SGSI. Esto implica que un 37 % no conocen ni siquiera el concepto. Este desconocimiento puede ser uno de los principales factores que impiden que las empresas implementen este tipo de sistemas.

Opción de respuesta	Cantidad de respuestas	Porcentaje
Si	25	63 %
No	15	37 %
Total General	40	100 %

Tabla 3-16.: De conocimiento de sistemas de gestión de seguridad de la información SGSI en las empresas

Implementación de sistemas de gestión de seguridad de la información - SGSI

De los 25 encuestados que declararón conocer qué es un SGSI, sólo 8 indicarón que su empresa tiene uno implementado. Los demás, así como los 15 que declararón no conocer el concepto, no cuentas con implementación de un SGSI (Tabla **3-17**). Esto significa que sólo el 20 % de los encuestados manifiesta que su empresa cuenta con un sistema de seguridad de la información implementado y en operación.

Opción de respuesta	Empresas	Porcentaje
Si	8	20 %
No	32	80 %
Total General	40	100 %

Tabla 3-17.: Empresas que cuentan con implementación de un sistema de gestión de seguridad de la información SGSI

Implementación de procesos y procedimientos basados de normas internacionales

El 67 % de los encuestados indican no tener normas o procedimientos implementados sobre normas internacionales. El 25 % cuenta con procedimientos basados en la norma ISO 27001:2013, mientras que otro 8 % de los encuestados indican que aplican metodologías de buenas prácticas como ITIL y metodologías de seguridad la información COBIT fusionada con la familia de ISO 27000. Las otras metodologías de seguridad de la información, como NIST.SP 800-53r4, COBIT ver 5 y ISM3 no son implementadas en ninguna empresa. Estos resultados reflejan que los encuestados conocen la norma más común que es ISO 27001:2013, pero desconocen otras metodologías de seguridad de la información como NIST.SP 800-53r4, COBIT ver 5 y ISM3, que se encuentran disponibles para la industria.

En este punto es importante hacer notar que, aunque sólo 8 empresas cuentan con implementaciones de SGSIs, 3 más han implementado procesos o procedimientos basados en normas internacionales, aún cuando no han implementado un SGSI completo.

3.3.7. Administración del riesgo

Implementación de procedimientos para la gestión de riesgos informáticos

Con relación a la implementación de procedimientos de gestión del riesgos informáticos, sólo el 30 % de los encuestados indicaron contar con uno en sus empresas (Tabla **3-19**). Notése que aun siendo un número bajo, este es mayor a la implementación de SGSIs.

Opción de respuesta	Respuestas	Porcentaje
ISO 27001:2013	9	25 %
NIST.SP 800-53r4	0	0 %
COBIT ver 5	0	0 %
ISM3	0	0 %
Otra norma internacional de seguridad (ITIL, porciones de Cobit y ISO27000)	3	8 %
Ninguna de las anteriores normas internacionales de seguridad	24	67 %
Total General	40	100 %

Tabla 3-18.: Procesos y procedimientos de seguridad implementados, basados en normas internaciones

Opción de respuesta	Cantidad de respuestas	Porcentaje
No	28	70 %
Si	12	30 %
Total General	40	100 %

Tabla 3-19.: Empresas que implementan procedimientos de gestión de riesgos informáticos

Implementación de metodologías para la gestión de riesgos

El 70 % de los encuestados indican que no cuentan con metodología de riesgos, el 15 % manejan metodología de riesgos basada en ISO27005 enfocada a los riesgos operacional orientada a la seguridad de la información, el 9 % indican que manejan otra metodología de riesgos como (CMMI Servicios Nivel 3, PMI-RMP y propias de la empresa), el 6 % metodología de riesgos basada en ISO3100 el cual es una metodología de riesgos enfocada a la organización, no se mencionan las otras metodologías de riesgos que se formularon en la pregunta como (DAFP, NIST. 800-30 ver 54 y MAGERIT).

Opción de respuesta	Respuestas	Porcentaje
ISO 27005:2011	6	15 %
ISO 31000	2	5 %
COBIT ver 5	0	0 %
DAFP	0	0 %
Nist. 800-30 ver 30	0	0 %
MAGERIT	0	0 %
Otra Metodología de Riesgos (CMMI Servicios Nivel 3, PMI-RMP y propias de la empresa)	4	10 %
Ninguna de las anteriores metodologías de Riesgos	28	70 %
Total General	40	100 %

Tabla 3-20.: Metodologías de riesgos utilizados en las empresas

3.3.8. Políticas de seguridad de la información

Adopción de manuales de políticas de seguridad de la información

Los encuestados indican que el 57 % de sus empresas cuenta con un manual de política de seguridad de la información como decálogo de normas internas para proteger sus activos de la información y un 43 % no cuenta con el manual de política de seguridad de la información.

Opción de respuesta	Cantidad de respuestas	Porcentaje
No	23	43 %
Si	17	57 %
Total General	40	100 %

Tabla 3-21.: Adopción de manual de políticas de seguridad en las empresas

3.3.9. Controles de seguridad informática

Implementación de controles de seguridad informática

En esta pregunta se evidencia que los controles más usados e implementados en las empresas encuestadas son: firewall, control de malware (antivirus), acuerdos de confidencialidad, cultura en seguridad, sistemas de autenticación y autorización (con token, password, biométricos, o similar), y planes de mantenimiento (actualización de sistema operativos, bases de datos y aplicaciones).

Controles como monitoreo de seguridad, detectores de intrusos (IDS/IPS) no son tan aplicados en la mayoría de las empresas, como se muestra en la Tabla **3-22**. Por otro lado, dos

encuestados indican indican tener otros controles, como son: anti-ramsonware y certificados digitales para acceso a los servidores por medio de una VPN.

Opción de respuesta	**Respuestas**
Firewall	33
Control de malware (Antivirus)	30
Acuerdos de confidencialidad	27
Cultura en seguridad	22
Sistemas de autenticación y autorización (con token, password, biométricos, o similar)	16
Planes de mantenimiento (Actualización de sistema operativos, bases de datos y aplicaciones)	16
Monitoreo de seguridad	12
Detectores de intrusos (IDS/IPS)	12
Manejo de incidentes de seguridad	8
Otros controles (Anti-Ramsonware y Certificados digitales para acceso a los servidores por medio de una VPN)	2

Tabla 3-22.: Controles de seguridad implementados en las empresas

Percepción sobre el control de amenazas informáticas

Además de indagar sobre los controles implementados en las empresas, se preguntó a los encuestados, su percepción sobre el tipo de amenazas que, según su conocimiento, estarían controladas. Como se observa en la Tabla **3-23**, para los encuestados, la amenaza más controlada es la de vírus informático o código malicioso (33), seguida del uso no autorizado de sistemas de información (23), lo que se asocia seguramente a la implementación de firewall y de antivirus, incluso más que al uso de sistemas de autenticación, pues sólo 16 empresas declararón contar con este tipo de sistemas (ver Tabla **3-22**). En este mismo sentido, resalta el hecho de que tan sólo en 8 empresas se considera que se tiene controlada la amenaza de suplantación de identidad, lo que supone poca confiabilidad en los sitemas de autenticación. Algo similar sucede con la confiabilidad que aporta el contar con acuerdos de confidencialidad, pues los encuestados de 27 empresas declararón contar con estos acuerdos, pero sólo 7 consideran tener controlada la amenaza de fuga de información y 6 de alteración de la misma.

En esta pregunta destaca el hecho que, excepto para las amenazas de virus informáticos y uso no autorizado de sistemas informáticos, la mayoría de las empresas consideran que no tienen contraladas las demás amenazas informáticas (Tabla 3-14). Más aún, a pesar de que,

por ejemplo, 11 empresas hallan sido afectadas por al menos una indisponibilidad de servicio (Tabla 3-14), tan sólo 6 consideran que tienen controlada esta amenaza.

Amenazas	Respuestas
Virus informáticos o código malicioso	33
Uso no autorizado de sistemas informáticos	23
Pérdida de información	13
Robo de información	12
Suplantación de identidad	8
Ataques de fuerza bruta	8
Fráudes basados en el uso de computadores	8
Desastres naturales	7
Denegación de servicio	7
Divulgacón de información	7
Fuga de información	7
Alteración de la información	6
Indisponibilidad de servicio	6
Sabotaje, vandalismo	5
Suplantación del sitio Web de la empresa	5
Espionaje	2

Tabla 3-23.: Percepción sobre amenazas informáticas controladas en las empresas

3.3.10. Factores que afectan la implementación de un sistema de seguridad de la información

La última sección de la encuesta indagó sobre cuáles son los factores que, según la opinión de los encuestados, impiden la implementación de un SGSI. La Tabla **3-24** presenta los resultados para esta pregunta. Como se puede observar, los factores que, según los participantes, afectan más la implementación de un SGSI en estas empresas son el tiempo y el presupuesto, seguido de la falta de conocimiento especializado, el cual puede también estar asociado a los dos primeros. Aunque no resulta un valor significativo, se debe indicar que 3 de las empresas consideran que este aspecto no es el foco, ni la proyección de la empresa, un factor altamente relacionado con la cultura sobre seguridad de la información.

Al relacionar las respuestas a esta pregunta con las obtenidas para las demás preguntas de la encuesta, se encuentra que el 85 % de los encuestados le da una importancia alta a los activos de información de la organización, pero solo el 52 % cuentan con un responsable de la seguridad de la información; además, el 58 % de los encuestados indican que su personal responsable en seguridad de la información no cuentan con la formación especializada.

Opción de respuesta	Respuesta
Tiempo	26
Presupuesto	25
Conocimiento especializado	21
Desconocimiento	14
Otro factor (Personal dedicado y Decisión a la adopción de estas prácticas)	5
No es el foco ni la proyección de la empresa	3

Tabla 3-24.: Factores que impiden la implementación de un sistema de gestión de seguridad de la información.

Además, el 90 % de los encuestados indican que la organización puede afectarse con algún tipo de amenaza informática conocida por su personal, amenazas como: Virus informático, robo de información, perdida de información , duplicación de información y fuga de información; adicional a sus preocupaciones sobre las amenazas, 12 encuestados han sido afectados por incidentes informáticos como (Virus o Malware de tipo Ransonware), que generan indisponibilidad del servicio, poniendo en riesgo la información, la operación del servicio para la toma de decisiones de estas organizaciones.

Por otro lado, y aunque el 90 % de los encuestados indican que es muy importante que las empresas cuenten con un sistemas de gestión de la seguridad de la información (Tabla 3-16), la mayoría de este 90 % no cuenta con un SGSI implementado (Tabla 3-18). Así mismo, el 70 % no cuenta con la gestión de riesgos implantados(Tabla 3-20), el 43 % no cuenta con una política de seguridad de la información (Tabla 3-23), y las empresas considera que la mayoría de amenazas no están siendo controladas (Tabla 3-14).
Estos resultados corresponden a lo mencionado por (Gutiérrez Amaya, 2017) [15], él menciona siete factores que presentan las PyMEs en Latinoamérica par la adopción de un sistema de gestión de la información, los cuales corresponden a:

1. Las PyMEs no tienen presupuesto dedicado a seguridad, o si lo tienen es muy poco.

2. Las PyMEs no tienen tiempo para dedicar a las actividades de seguridad.

3. Las PyMEs aún no son conscientes de lo que deben hacer.

4. Las PyMEs no cuentan con el personal calificado para realizar las tareas de seguridad de la información.

5. Las PyMEs no son conscientes de qué tan importante es la seguridad, si algo malo llegara a ocurrir.

6. La gerencia no está enterada de los riesgos.

7. Las PyMEs no saben dónde encontrar la información que deberían conocer.

3.4. Conclusiones de la encuesta

La realización de este estudió evidencia que, como se supusó desde la preparación de la propuesta de este trabajo, el nivel de implementación de sistemas de gestión de seguridad de la información es bajo en las pequeñas y medianas empresas del sector de la información y las comunicaciones de la ciudad de Medellín (Tabla 3-5), pues sólo el 20 % de los encuestados declaran tener una implementación de este tipo en sus empresas (Tabla 3-18). Se observa sin embargo que, en estos casos, la implementación se basa en estándares internacionales, como la ISO 27001:2013 (Tabla 3-19). Es importante resaltar que, aunque un mayor número de empresas cuenta con procedimientos para la gestión de riesgos informáticos (30 %) (Tabla 3-20) y con la adopción de manuales de políticas de seguridad de la información (57 %) (Tabla 3-23), continúan siendo cifras bajas para este sector de estudio, el cual, se supone, donde el sector de las TIC asido uno de los que ha mostrado mayor inversión en aspectos de la seguridad de la información, por debajo del sector financiero, gobierno y educación quien les dan mayor referencia a este tema, como se refleja en la encuesta nacional de seguridad informática elaborada por la (ACIS, 2018) y analizad por (Almanza, 2018)[7]. A pesar del bajo nivel de implementación de este tipo de sistemas, destaca la importancia que los encuestados asignan tanto a los activos de información (Tabla 3-8), y la seguridad de esta, más aun si se tiene en cuenta que un porcentaje importante de encuestados asume roles de dirección en las empresas (Tabla 3-7). A pesar de ello, se observa una tendencia a subvalorar amenazas como la suplantación de identidad, o los desastres naturales, el sabotaje y el vandalismo, que pueden materializarse en este tipo de empresas (Tabla 3-14). Esto último demuestra la necesidad de insistir en programas que mejoren la cultura hacía la seguridad de la información, desde las mismas directivas hasta todos los empleados, pues según los resultados obtenidos, para los encuestados más de la mitad de los empleados no le dan un nivel de importancia alto a la información que manejan (Tabla 3-8).
Con relación a los factores que impiden la implementación de estos sistemas, esta encuesta muestra que los encuestados indican que son el tiempo y presupuesto los factores que mayor incidencia presentan, seguido de la falta de conocimiento especializado (Tabla 3-26) En este sentido, y tal como se expusó en la introducción de este trabajo, se requiere el desarrollo de metodologías que faciliten la implementación de sistemas de gestión de seguridad de la información, sin requerir altas inversiones de recursos económicos o tiempo, pero que además pueda llevarse a cabo sin formación especializada.

4. Metodología de sistema de gestión de seguridad de la información SGSI para PyMEs

A partir de los resultados del estudio inicial, que evidenció la necesidad de ofrecer estrategías que faciliten la implementación de sistemas de gestión de la seguridad de la información a PyMEs del sector económico de la información y comunicaciones; las cuales, por lo general cuentan con personal técnico con formación general en conceptos de seguridad de la información, pero sin formación especilizada, y además presentan limitaciones para la asignación de tiempo y presupuesto para la implementación de este tipo de sistemas. Se procede a realizar una propuesta de metodología orientadas a esta necesidad, dando así cumplimiento al segundo objetivo específico de este trabajo.

Teniendo en cuenta que la propuesta metodológica debería tener en cuenta el estado actual de desarrollo de metodologías de implementación de sistemas SGSIs, antes de plantear la metodología propuesta, se realizó un estudio detallados de las normas y metodologías de SGSI y de gestión del riesgos de la información, el cual generó insumos importantes para la metodología que se presenta al final de este capítulo.

4.1. Análisis de normas y metodología de sistemas de seguridad de la información

En este caso se realizó un análisis de la norma internacional ISO 27001:2013, metodologías de SGSI COBIT v5 y la guía de NIST 800 53v4 y ISO 27002:2011 (Acosta, 2016; Olivan 2017) [37]; no se tuvo en cuenta otras metodologías de SGSI como ISM3, debido a su bajo nivel de implementación en la región. Como resultado de este análisis se construyó una tabla comparativa con información común y diferencias de los componentes de la seguridad de la información, con base en el ciclo de Deming PHVA (Ver Anexo B). Adicionalmente, a partir de los resultados de este análisis, se propone el diagrama de la Fígura **4-1**, donde se enmarcan las metodologías y normas en tres niveles (estratégico, táctico y operacional), el nivel estratégico se refiere a la planeación que se orienta a lograr los objetivos de la organización, liderada por la alta gerencia, abarca aquellos temas de las normas y metodologías

que corresponden a nivel de la organización como son el contexto de la organización, liderazgo, compromiso, roles, responsabilidades, comunicación y cultura. Para este nivel, se aplica PVA del ciclo de Deming. Como se puede observar, de acuerdo al análisis realizado, tanto ISO 27001 como COBIT presentan normas o lineamientos para este nivel. En el nivel táctico se desarrolla detalladamente la planeación del funcionamiento de la metodologías y normas del SGSI, este nivel es dirigido por jefes de área y personal clave de la organización, abarcando los temas como: la gestión del riesgo, implementación de controles, formación y concienciación del recurso humano; en este caso, del ciclo de Deming se aplica H. En este caso, de nuevo son ISO 27001 y COBIT las que contemplan estos temas. Finalmente, el nivel operacional corresponde a la asignación de las tareas puntuales que debe realizar cada empleado, o contratista consultor que apoya a la organización en la implementación de temas para el SGSI como son, la identificación y clasificación de activos, valoración y tratamiento de riesgos, y la implementación de controles de seguridad informática y de la información, es claro que estos temas se desarrollan a partir de los lineamientos proporcionados por los niveles de planeación estratégico y táctico. En este caso, del ciclo de Deming se aplica H, y tanto la ISO 27001, como COBIT y la NIST 800-53 abarcan este nivel.

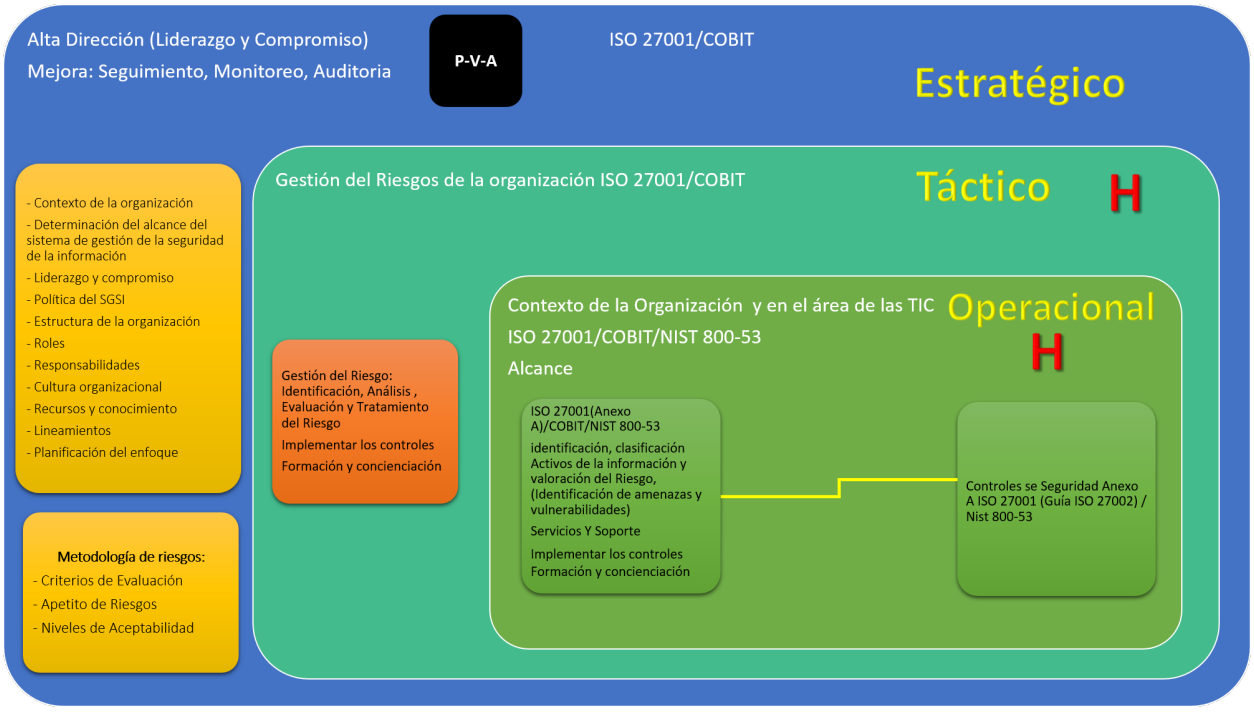

Figura 4-1.: Diagrama de niveles de planeación de normas y lineamientos de metodologías de sistemas de gestión de seguridad de la información (SGSI) - Fuente: Construcción propia

4.1.1. Resumen y conclusiones del análisis de metodologías para la implementación de SGSIs

- Considerando los procesos de las metodologías del SGSI, los tres enfoques se basan en conceptos generales, tanto en tecnología de la información como en seguridad de la información, que brinda a las organizaciones la libertad de adoptar las tecnologías más adecuadas para sus entornos.

- COBIT ver. 5 y la relación de la guía NIST SP 800 53. v4 proporcionan metodologías sobre cómo implementar los marcos en la práctica, mientras que ISO 27001:2013 ya cuenta con metodologías de implementación probadas disponibles en el mercado. Aunque sus pasos no están alineados al 100 % las adaptaciones menores pueden reducir fácilmente las brechas.

- Aplicabilidad intersectorial: Aunque NIST SP 800 53. v4 se proporciona para organizaciones de EE. UU., Y COBIT no es un servicio oficial en todo el mundo, todos ellos pueden ser aplicables a cualquier tipo y tamaño de organización, al igual que ISO 27001:2013.

- COBIT ver. 5 tiene una estructura de gobierno bien definida. Un punto crítico en el mantenimiento de una gestión de sistema, la estructura de gobierno proporcionada por COBIT ver. 5 puede ayudar a establecer y mantener la alineación de tecnología de la información y seguridad de la información con objetivos comerciales. ISO 27001:2013 no cubre este aspecto directamente, aunque se puede usar la identificación del contexto organizacional para alinear estos puntos.

4.2. Análisis de las metodologías de riesgos

En este caso se realiza un análisis GAP de la norma internacional ISO 31000 en riesgos Vs. normas técnicas de gestión ISO 27005, la guía técnica NIST 800-30, la metodología Octave y Magerit, las cuales son las metodologías más conocidas en la región para los riesgos de seguridad de la información. Para este análisis no se tuvo en cuenta otras metodologías de riesgos como DAFP, metodología aplicada por las entidades del estado colombiano, dado que esta es de orden organizacional. Como resultado se construye una tabla comparativa del análisis de metodología de riesgos (Ver Aneo C), identificando los temas en común y principales diferencias. Además, como resultado de la revisión se elabora un diagrama de metodología de riesgos (Ver Figura **4-2**), el cual, al igual que para el caso de las metodologías de SGSIs define tres niveles, de acuerdo al alcance (Estratégico, táctico y operacional). En el nivel estratégico se enmarcan las metodologías de riesgos de nivel organizacional como ISO3100 y Octave, donde se enmarcan los siguientes temas a nivel transversal de la organización (contexto, alcance, liderazgo, mejora continua), se aplica en este nivel el PVA según el ciclo

de Deming. En el nivel táctico se enmarcan las metodologías de riesgos Octave e ISO3100, para lograr los objetivos y misión estrategia de la organización, se aplica H, según el ciclo de Deming. Por último, en el nivel operativo se aplican metodologías de la gestión del riesgo de la seguridad de la información como ISO27005, Magerit y Nist 800-30, además para el tratamiento de los riesgos de seguridad de la información se mezclan los controles del Anexo A de la ISO27001, de COBIT y la NIST 800-53, en este nivel se aplica el H del ciclo de Deming.

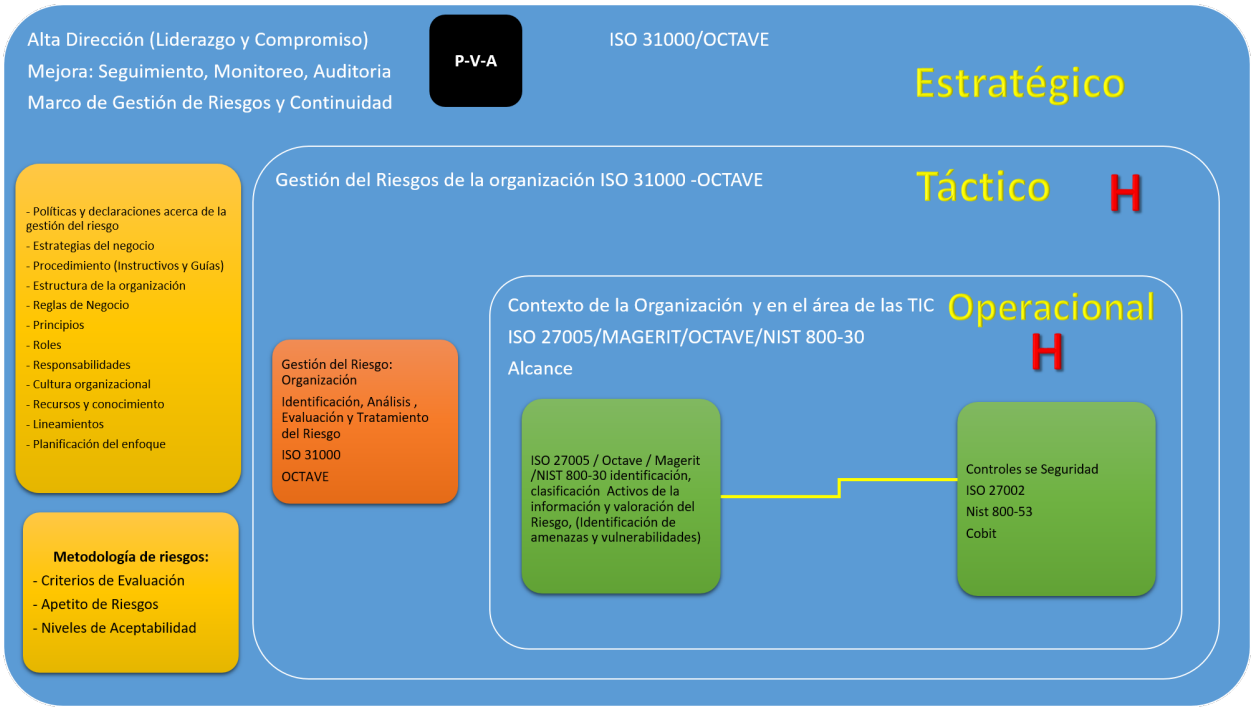

Figura 4-2.: Diagrama de las metodologías de riesgos - Fuente: Construcción propia

4.2.1. Resumen y conclusiones de las metodologías de gestión de riesgos

Una evaluación de riesgos es muy particular para cada organización, por lo que no sería lo más adecuado desarrollar evaluaciones a partir de resultados obtenidos de otras organizaciones.

ISO 27005 e ISO 31000 son los estándares más conocidos para la gestión de riesgos, existen otros instrumentos que están alienados con estos estándares y que facilitan a una empresa enfocarse en la implementación de herramientas y metodologías que satisfagan los requerimientos básicos de la administración de riesgos en sus sistemas de información.

ISO 27005, la guía técnica NIST 800-30, Octave y Magerit están orientadas al análisis y gestión de riesgos de los activos de información y a las de la organización de las Tecnologías de la Información (TI); en cambio, la ISO 3100 se enfocada a los riesgos de la organización. MAGERIT, está alineado con los estándares de ISO (27001 y 27002), por lo que su implementación se convierte en el punto de partida para una certificación o para mejorar los sistemas de gestión. Esta metodología tiene un doble objetivo, por un lado, pretende estudiar los riesgos que soporta el sistema de información y el entorno asociable a él y por otro recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados. La interfaz de seguridad de MAGERIT [11] proporciona un enlace clave con métodos de desarrollo de proyectos software, para considerar por fin la seguridad de un proyecto como requisito funcional del mismo. Adicionalmente, MAGERIT ofrece una herramienta para implementar la metodología de análisis de riesgos llamada PILAR [38], desarrollada por el Centro Criptológico Nacional (CCN) y de amplía utilización en la administración pública española, cuyos salvaguardas están basados en la norma ISO 27002.

La guía de riesgos NIST 800-30, cuenta con el respaldo de las siguientes guías para la administración del riesgo de seguridad de la información: 800-39, gestión del riesgo de seguridad de la información: Organización, misión y vista del sistema de información, 800-37, guía para aplicar el marco de administración de riesgos a los sistemas de información federales: Un enfoque del ciclo de vida de la seguridad, 800-53 v4 guía de controles de seguridad recomendados para sistemas y organizaciones de información federales.

Las metodologías seleccionadas para la evaluación de los riesgos son ISO 27005 y MAGERIT ya que cubre todos los aspectos tomados en cuenta como elementos de TI dentro de una organización, y además proporciona una lista de actividades de fácil entendimiento y muy simple de seguir. Como resultado final de aplicar esta metodología se tuvo la matriz de tratamiento del riesgo la cual permitirá proceder con la elaboración de las políticas de seguridad de la información.

Las metodologías de riesgos de ISO 27005, Magerit y la Nist 800-30, enfocadas en la gestión de los riesgos de seguridad de la información, relacionan los elementos de la seguridad de la información, como se observa en la Figura **4-3**.

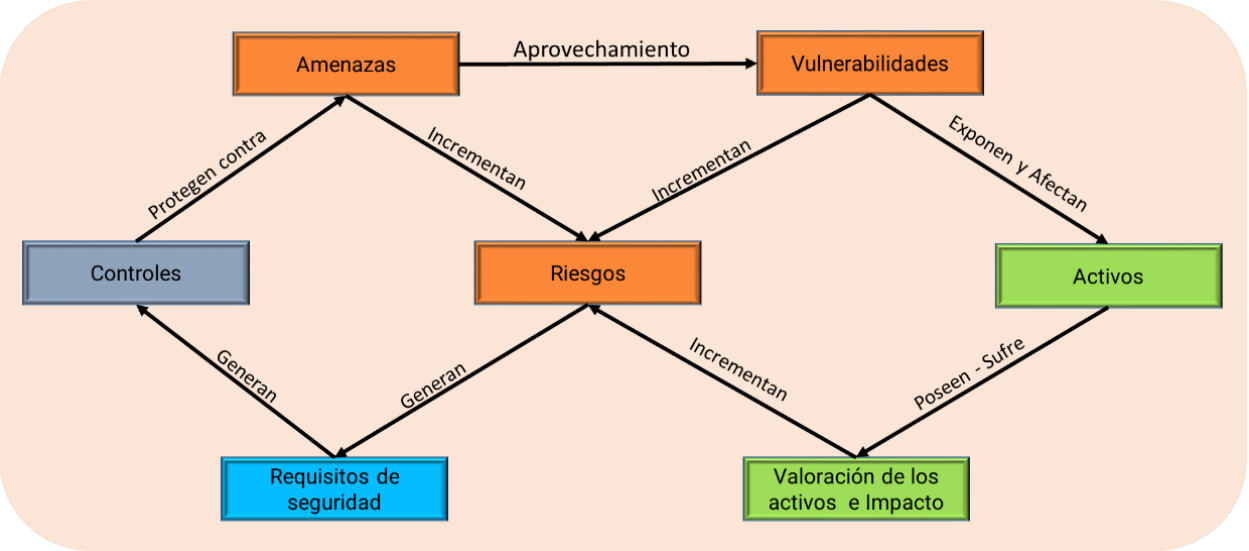

Figura 4-3.: Elementos del análisis de la gestión de los riesgos en SGSI (Fuente: www.iso27000.es)

4.3. Análisis de controles de seguridad de la información

Se realizó un análisis GAP de las normas y metodologías que contienen controles de seguridad de la información para protección de los activos de información, incluyendo ISO 27001:2013 anexo A, COBIT v5 [9] y guía de NIST 800-53 v4 [8]. La Tabla **4-1**, resume la conformación de controles para cada norma analizada.

ISO 27001:2013	**COBIT v5**	**Guía técnica NIST 800-53v4**	**ISO 27002:2011 Guía**
El anexo A este está compuesto por 14 dominios, 35 objetivos y 114 controles de seguridad.	Contiene 210 objetivos de controles.	Contiene 256 controles, distribuidos en 18 familias.	Guía técnica de ISO 27002:2011, define el cómo se aplican los controles.

Tabla 4-1.: Cantidades de controles de seguridad de la información de las normas analizadas

En la revisión de los controles se construye una tabla (Anexo E), donde se identifican que ISO 27001:2013, COBIT v5 y la guía de NIST 800 53v4, tienen en común 73 controles, COBIT v5 cuenta con 2 controles que no se encuentran en ISO 27001:2013, ni en la guía de NIST 800 53v4, además NIST 800 53 v4 cuenta con 8 controles que no se encuentran en ISO 27001:2013, ni en COBIT v5, obteniendo 83 controles, estos controles se clasifican según la función identificar, detectar, proteger, responder. Así, estos 83 controles son agrupados en

19 clasificaciones como se muestra en Tabla **4-2**.

Nro.	Categoría Controles	Descripción - Categoría
1	Gestión de activos	Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar sus objetivos de negocio se identifican y gestionan de acuerdo con su importancia relativa para los objetivos de negocio y la estrategia de riesgos de la organización.
2	Entorno empresarial	La misión, los objetivos, las partes interesadas y las actividades de la organización se entienden y priorizan; esta información se utiliza para informar las funciones, responsabilidades y decisiones de gestión de riesgos de la seguridad de la información
3	Gobierno (Políticas)	Las políticas, los procedimientos y los procesos para gestionar y supervisar los requisitos normativos, legales, de riesgo, medioambientales y operativos de la organización se entienden e informan a la gestión del seguridad de la información
4	Evaluación de riesgos	La organización comprende el riesgo de la seguridad de la información para las operaciones de la organización (incluidas la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas.
5	Estrategia de gestión de riesgos	Las prioridades, limitaciones, tolerancias de riesgo e hipótesis de la organización se establecen y utilizan para apoyar las decisiones sobre el riesgo operacional.
6	Control de acceso	El acceso a los activos y a las instalaciones asociadas está limitado a los usuarios, procesos o dispositivos autorizados, así como a las actividades y transacciones autorizadas.
7	Sensibilización y formación	El personal y los socios de la organización reciben educación sobre la seguridad de la información y están adecuadamente capacitados para llevar a cabo sus deberes y responsabilidades relacionados con la seguridad de la información de manera coherente con las políticas, procedimientos y acuerdos relacionados.

8	Seguridad de datos	La información y los registros (datos) se gestionan de forma coherente con la estrategia de riesgos de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.
9	Procesos y procedimientos de protección de información	Las políticas de seguridad (que abordan el propósito, el alcance, las funciones, las responsabilidades, el compromiso de la administración y la coordinación entre las entidades de la organización), los procesos y los procedimientos se mantienen y utilizan para administrar la protección de los sistemas y activos de información.
10	Mantenimiento	El mantenimiento y las reparaciones de los componentes del sistema de control e información industrial se realizan de acuerdo con las políticas y procedimientos.
11	Tecnología de protección	Las soluciones técnicas de seguridad se gestionan para garantizar la seguridad y la resistencia de los sistemas y activos, de acuerdo con las políticas, procedimientos y acuerdos relacionados.
12	Anomalías y eventos	La actividad anómala se detectara a tiempo y se entiende el impacto potencial de los eventos.
13	Monitoreo continuo de seguridad	El sistema de información y los activos son monitoreados a intervalos discretos para identificar eventos de seguridad y verificar la efectividad de las medidas de protección.
14	Procesos de detección	Los procesos y procedimientos de detección son mantenidos y probados para asegurar el conocimiento oportuno y adecuado de eventos anómalos.
15	Planificación de la respuesta	Los procesos y procedimientos de respuesta se ejecutan y mantienen para garantizar una respuesta oportuna a los eventos de seguridad detectados. / Los procesos y procedimientos de recuperación se ejecutan y mantienen para garantizar la restauración oportuna de los sistemas o activos afectados por eventos de seguridad

16	Comunicaciones	Las actividades de respuesta se coordinan con las partes interesadas internas y externas, según proceda, para incluir el apoyo externo de los organismos encargados de hacer cumplir la ley. / Las actividades de restauración se coordinan con partes internas y externas, como centros de coordinación, proveedores de servicios de internet, propietarios de sistemas de ataque, víctimas, otros CSIRT y proveedores.
17	Análisis	Se realizan análisis para asegurar una respuesta adecuada y apoyar las actividades de recuperación.
18	Mitigación	Las actividades se realizan para prevenir la expansión de un evento, mitigar sus efectos y erradicar el incidente.
19	Mejoras	Las actividades de respuesta de la organización mejoran al incorporar las lecciones aprendidas de las actividades de detección/respuesta actuales y anteriores.

Tabla 4-2.: Tabla de categorías de controles

4.3.1. Resumen y conclusiones sobre controles

- La estructura de los controles de seguridad en NIST SP 800 53 v4 es muy parecida al anexo A de la norma ISO 27001:2013. Sus 256 controles se encuentran organizados en 18 familias diferentes, cada uno contiene los controles relacionados con el anexo A de la norma ISO 27001:2013.

- COBIT ver.5 enfoca sus controles en las tecnologías de la información, cubriendo no sólo los controles de seguridad de la información, sino también controles relacionados con las operaciones de TI (por ejemplo, proceso de adquisición).

- El Anexo A de ISO 27001:2013 tiene controles para cubrir la protección de la información, independientemente de dónde se encuentre esta.

- En cuanto a la guía NIST SP 800 53 v4, su documentación se centra en los controles de seguridad informática, teniendo también muchos controles descritos en el anexo A de ISO 27001:2013 e ISO 27002:2011, pero con un mayor nivel de detalle, así como controles no cubiertos por ISO 27001:2013, como Ïnternet de las Cosas". Además, algunos documentos de NIST son específicos de la tecnología, como pautas para la seguridad de los sistemas operativos de Apple y Microsoft.

4.4. Propuesta de metodología de seguridad de la información para PyMEs del sector de la información y comunicación de la ciudad de Medellín.

Una vez analizadas las metodologías y normas para la implementación de SGSIs, las metodología de riesgos y los controles existentes para proteger los activos de información, se propone una metodología para la implementación de sistemas de gestión de seguridad de la información para PyMEs del sector económico de la información y comunicaciones de la ciudad de Medellín, intentando que cumpla con las condiciones de ser de fácil entendimiento e implementación, por personal de las áreas de las TIC que tengan un conocimiento básico sobre seguridad informática. La Figura **4-4** ilustra la metodología propuesta, la cual se basa en el ciclo de Deming PHVA, el planear (P) se encuentra en las fases de contexto, alcance y en el corazón del sistema que corresponde en la gestión de los riesgos, el hacer (H) se encuentra en la aplicación de los controles, además se incluyen dos fases de verificación (V) y mejora contínua (A).

4.4.1. Principios de aplicación

4.4.2. Implementación

Para lograr una fácil implementación del sistema de gestión de seguridad de la información, esta metodología propone el uso y aplicabilidad de 29 guías alineadas en el modelo propuesto en las fases de PHVA , las cuales se presentan como archivos adjuntos a este documento. Su construcción se basó en las recomendaciones de las guías de INCIBE para PyMEs [27], las guías de Mintic para PyMEs [39] y las guías de ciberseguridad para PyMEs propuesta por la cámara de comercio de Chile [40].

El propósito de estas guías es orientar a los implementadores de la metodología propuesta, sobre el cómo llevar a cabo dicha implementación. La primera de las guías, es la de conceptos, esta no incluye aspectos de implementación, sólo contiene la información necesaria para consultar la terminología usada en la metodología y demás guías propuestas. La segunda guía, implementación de la metodología SGSI (PyMEs), describe las generalidades de cómo aplicar la metodología propuesta, constituye el centro del modelo y por lo tanto, es de implementación obligatoria. Las demás guías están compuestas de dos fases; la primera es la línea base, en la cual se indica qué se debe aplicar a nivel de organización, técnico y de empleados, y la segunda fase está compuesta de una lista de chequeo que ayudará a evaluar el cumplimiento de la implementación de la guía sobre el SGSI, además esta lista de chequeo sirve para evaluar el cumplimiento y realizar las mejoras ayudas en el SGSI. En concreto la metodología propone la implementación en cinco fases, como se describe a continuación.

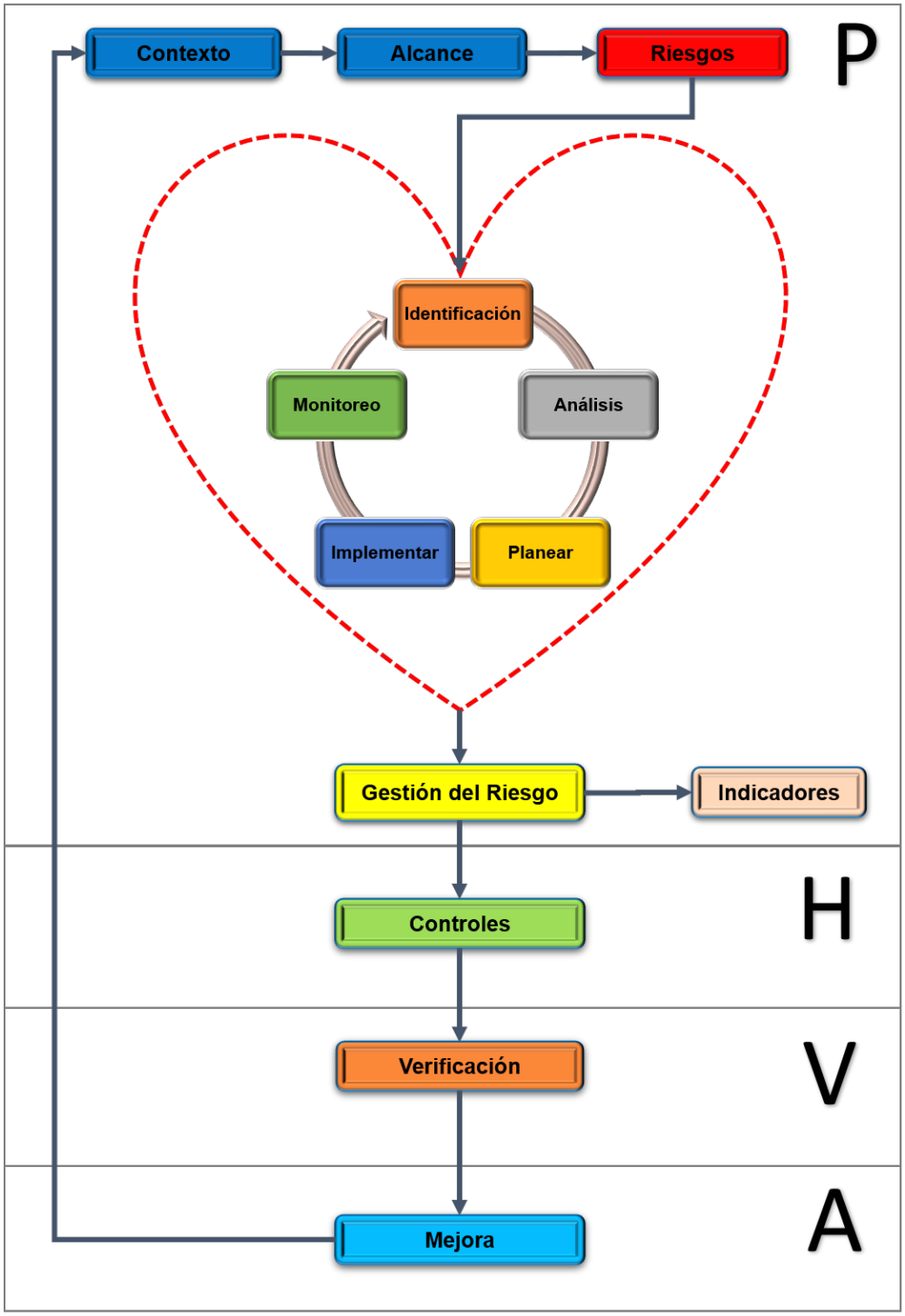

Figura 4-4.: Metodología propuesta para la implementación de SGSIs en PyMEs - Fuente: Construcción propia

- **Fase I - Diagnóstico inicial.** Busca establecer el estado inicial de la organización, respecto a la definición de políticas y la implementación de controles para gestión de la seguridad de la información. Aunque no se establece una guía para realizar este diagnóstico, se sugiere un análisis GAP para este propósito (Anexo-Analisis-GAP-Inicial-SGSI-Pymes.xlsx).

- **Fase II - Definición del contexto y alcance del SGSI (Guía 2)**. El contexto hace referencia a la identificación de los aspectos internos y externos que podrían afectar el propósito de la organización y su capacidad para lograr los resultados esperados del SGSI. El alcance describe la extensión y los límites del SGSI. El alcance del SGSI, puede ser toda la organización, o simplemente una parte de ella, o un simple proceso, o un sistema de información. Esta guía es de aplicación obligatoria y se ubica en la planeación (P) del modelo PHVA (Figura **4-4**) y (Tabla **4-3**).

- **Fase III - Gestión del riesgo (Guía 3).** Aplicación de una metodología para la gestión y tratamiento de los riesgos iniciando a partir de la identificación de los activos de información. Esta guía es de aplicación obligatoria y se ubica en la planeación (P) del modelo PHVA (Figura **4-4**) y (Tabla **4-3**). Los controles que se trabajan en esta metodología de riesgos corresponden a los 83 controles propuesto agrupados en las 19 categorías.

- **Fase IV - Definición de políticas**. Definición tanto la política general (Guía 4) como la política operacional (Guía 5) para la implementación del SGSI. Estas dos guías son de aplicación obligatoria y se ubican en la planeación (P) del modelo PHVA (Figura **4-4**) y (Tabla **4-3**).

- **Fase V - Implementación y Verificación (Guías 06 a 28).** De acuerdo a los resultados obtenidos en el análisis de riesgos, aplicar las guías que sean necesarias en la implementación del SGSI, para el aseguramiento de los activos de información. Es esta fase se proponen 23 guías, cada una de las cueles es de aplicación opcional. Estas guías se ubican en el hacer (H) y en el verificar (V) del modelos PHVA (Figura **4-4**) y (Tabla **4-3**).

- **Fase VI - Evaluación (Guía 29)**. Para evaluar la evolución de la implementación del SGSI, elaborar el diagnóstico del estado actual de los controles con los que cuenta la empresa, el cual es de aplicación obligatoria en el modelo, y se ubica en el ajustar (A) del modelo PHVA (Figura **4-4**) y (Tabla **4-3**). Además de la guía, para este diagnóstico se cuenta con una herramienta para elaborar esta actividad (Anexo-Analisis-GAP-Seguimiento-SGSI-Pymes.xlsx), los controles corresponden a los 83 controles propuestos agrupados en la 19 categorías.

La Tabla **4-3** presenta la relación de las 29 guías diseñadas, de acuerdo al modelo propuesto en la Figura **4-4**

Fase	**PHVA**	**Nro.**	**Guías**	**Nivel de Aplicación**	**Aplicación**
		0	Guía de conceptos	Nivel organización o de proceso - nivel personal	Opcional
		1	Guía implementación de la metodología SGSI (Pymes)	Nivel organización	Obligatorio
II	P	2	Guía de contextualización - alcance	Nivel organización	Obligatorio
III	P	3	Guía de gestión del riesgo	Nivel organización	Obligatorio
IV	P	4	Guía de política General del SGSI	Nivel organización o de proceso - nivel personal	Obligatorio
IV	P	5	Guía de política operacional	Nivel organización o de proceso - nivel personal	Obligatorio
V	HV	6	Guía de clasificación de la información	Nivel organización o de proceso - nivel personal	Opcionales
V	HV	7	Guía de gestión de recursos humanos	Nivel organización o de proceso - nivel personal	Opcionales
V	HV	8	Guía de relación con proveedores	Nivel organización	Opcionales
V	HV	9	Guía concienciación y formación	Nivel organización o de proceso - nivel personal	Opcionales
V	HV	10	Guía de cumplimiento legal	Nivel organización o de proceso - nivel personal	Opcionales
V	HV	11	Guía de contraseñas Nivel organización	Nivel organización o de proceso - nivel personal	Opcionales
V	HV	12	Guía aplicaciones permitidas	Nivel organización o de proceso - nivel personal	Opcionales

V	HV	13	Guía de control de acceso	Nivel organización o de proceso - nivel personal	Opcionales
V	HV	14	Guía de uso del correo electrónico	Nivel organización o de proceso - nivel personal	Opcionales
V	HV	15	Guía de almacenamiento en los equipos de trabajo	Nivel organización o de proceso - nivel personal	Opcionales
V	HV	16	Guía de uso de wifis y redes externas	Nivel organización o de proceso - nivel personal	Opcionales
V	HV	17	Guía de almacenamiento en dispositivos extraíbles	Nivel organización o de proceso - nivel personal	Opcionales
V	HV	18	Guía de protección del puesto de trabajo	Nivel organización o de proceso - nivel personal	Opcionales
V	HV	19	Guía almacenamiento en la nube	Nivel organización o de proceso - nivel personal	Opcionales
V	HV	20	Guía borrado seguro y gestión de soportes	Nivel organización o de proceso - nivel personal	Opcionales
V	HV	21	Guía de antimalware	Nivel organización o de proceso - nivel personal	Opcionales
V	HV	22	Guía de actualizaciones de software	Nivel organización o de proceso - nivel personal	Opcionales
V	HV	23	Guía de uso de dispositivos móviles	Nivel organización o de proceso - nivel personal	Opcionales
V	HV	24	Guía de uso de técnicas criptográficas	Nivel organización o de proceso - nivel personal	Opcionales
V	HV	25	Guía de respuesta a incidentes	Nivel organización o de proceso - nivel personal	Opcionales

V	HV	26	Guía de copias de seguridad	Nivel organización o de proceso - nivel personal	Opcionales
V	HV	27	Guía de continuidad de negocio	Nivel organización o de proceso - nivel personal	Opcionales
V	HV	28	Guía de auditoria de sistemas	Nivel organización o de proceso - nivel personal	Opcionales
VI	A	29	Documento de controles (Administrativo - técnico - físico)	Nivel organización o de proceso - nivel personal	Obligatorio

Tabla 4-3.: Guías de implementación de sistema de gestión de seguridad de la información para PyMEs del sector de la información y comunicaciones

5. Caso de estudio: implementación de la metodología propuesta en una empresa del sector de la información y comunicaciones de la ciudad de Medellín

5.1. Descripción del negocio

E-Global S.A. es una compañía Colombiana de la ciudad de Medellín la cual fue matriculada ante Cámara de Comercio de la ciudad de Medellín el jueves 23 de marzo de 2000 e iniciando labores el 03 de abril de 2000, fue constituida con el propósito de trabajar en el sector de las Tecnologías de Información y Comunicaciones, prestando sus servicios a clientes (grande, mediana y pequeña empresa de cualquier sector económico), para quienes estas son un factor importante en el desarrollo de sus negocios, su misión es entregar soluciones en infraestructura y servicios de tecnologías de información y comunicaciones a sus clientes, aplicando las mejores prácticas de la industria [41]. De acuerdo a la ainformación de su presentación, E-Global S.A. genera valor con base en el conocimiento, el compromiso, la idoneidad y el profesionalismo de sus colaboradores. Esta empresa cuenta con 192 empleados, tiene como domicilio principal de su actividad la ciudad de Medellín.

5.2. Diagnóstico inicial

Antes de iniciar la implementación de la metodología propuesta, se realiza un diagnóstico incial del estado de implementación desde tres perspectivas; la primera de ellas es el resultado a la encuesta planteada para la determinación del estado de implementación (Ver capítulo 3), la segunda es una evaluación por parte de quienes llevarán a cabo la implementación y la tercera, una evaluación del autor de este documento, como experto en el área de seguridad de la información. A continuación se describen los principales hallazgos de este diagnóstico.

5.2.1. Resultado de la encuesta

En este caso se revisaron los resultados de la encuesta inicial, la cual fue diligenciada por el gerente general de la empresa. El cuestionario indagaba por aspectos generales de la empresa vinculado básicamente a los siguientes ítems: Tamaño de la empresa, actividad económica, la importancia de los activos de la información con relación a la empresa y los funcionarios, amenazas informáticas, incidentes de seguridad de la información, conocimiento en SGSI, de riesgos, políticas de seguridad de la información y factores que impiden la implementación de SGIS. Como resultado de la indagación se pudo constatar lo siguiente:

El objeto social de la empresa es la consultoría informática y actividades de administración de instalaciones informáticas, Actividades de tecnologías de información y actividades de servicios informáticos, actividades de telecomunicaciones, telecomunicaciones alámbricas e inalámbricas.

La persona encuestada manifiesta que el nivel de importancia que la empresa le da a los activos de la información es alta, además considera que los empleados también le dan un nivel alto de importancia a la información que manejan; no obstante, la empresa no posee un responsable directo de la seguridad de la información y tampoco cuenta con personal especializado que maneje la gestión de seguridad de la información, a pesar de que tienen claridad en cuanto a las diferentes amenazas que pueden afectar los sistemas de información de la empresa, las cuales incluyen virus informáticos o código malicioso, uso no autorizado de sistemas informáticos, robo de información, suplantación de identidad, denegación de servicios (DoS), ataques de fuerza bruta, alteración de la información, divulgación de información, desastres naturales, sabotaje, vandalismo, pérdida de información, fuga de información, indisponibilidad del servicio, suplantación a su sitio web, e incluso declara que la empresa ha tenido incidentes de seguridad, concretamente en infecciones de malware (virus o malware de tipo ransonware) e indisponibilidad del servicio. El gerente considera que la seguridad de la información de la empresa es muy importante y a pesar de conocer que es un SGSI la empresa no posee dicho sistema, como ISO 27001:2013, COBIT V.5, NIST 800-53 V.4.

En relación a los riesgos, la empresa no cuenta con un sistema de gestión de riesgos para la seguridad de la información, lo que implica que no se utilicen metodologías de riesgos como: ISO 31000, ISO 27005, MAGERIT y OCTAVE.

En cuanto a las políticas de seguridad de la información, no existe un manual que direccione este aspecto, pero sí cuentan con algunos controles de seguridad informática como: firewall, control de malware (Antivirus), sistemas de autenticación y autorización, planes de mantenimiento (actualización de sistema sistemas operativos, bases de datos y aplicaciones), cultura en seguridad, y además firman acuerdos de confidencialidad. Con relació a los controles,

solamente tiene intervenido la amenaza asociada a virus informáticos o código malicioso.

El gerente indica que el principal factor que ha impedido la implementación de un SGSI es el tiempo.

5.2.2. Conocimiento de los implementadores

Una vez obtenido los resultados el paso a seguir fue contactar al gerente general de E-Global S.A, con el fin de contextualizarlo acerca del proyecto y de esta forma obtener el aval para realizar la gestión según el alcance de éste. Como acto seguido se asigna, como apoyo, al ingeniero encargado de la infraestructura de la empresa, para iniciar con el estudio del caso de acuerdo con el referente metodológico propuesto en el proyecto, además se vinculó un tecnólogo del área de infraestructura.

Como preámbulo a este aparte, se procedió a la aplicación de un instrumento (encuesta) a las dos personas propuestas como apoyo para el desarrollo del proyecto, la cual tiene como objetivo hacer un diagnóstico del nivel de conocimiento que poseen en términos de los SGSI. En consecuencia, se obtuvieron los siguientes resultados:

Se evidenció que las respuestas en algunos casos son contrarias y en otros se complementan o van en la misma dirección. En este sentido, para dar un mayor entendimiento a los resultados se procederá a hacer el análisis de forma independiente por cada sujeto encuestado.

Para el ingeniero de sistemas, la importancia de los activos de información es alta mientras que para el analista de soporte se encuentra en un nivel medio; en cuanto a la percepción que ambos tienen sobre la importancia que los empleados le dan a la información que manejan, el ingeniero plantea que es media, mientras que el analista considera que es bajo; ambos afirman, al igual que el gerente, que la empresa no posee con un responsable que gestione la seguridad de la información.

En relación a los diferentes riesgos informáticos a que puede estar expuesta la empresa, es plenamente conocido por el ingeniero de sistemas, lo que no sucede con el analista, quien manifiesta no conocerlo; no obstante, coinciden en que las amenazas informáticas que podrían afectar a la empresa son: Virus informáticos o código malicioso, uso no autorizado de sistemas informáticos, robo de información, fraudes basados en el uso de computadores, alteración de la información, divulgación de información, pérdida de información, fuga de información, esto complementado a los riesgos declarados por el ingeniero como: denegación de servicios (DoS), ataques de fuerza bruta, sabotaje, vandalismo, indisponibilidad del servicio, suplantación a su sitio web y desastres naturales. Aunque las amenazas reales de la que ha sido objeto

la empresa, que configuran un incidente informático, han sido por infecciones de malware (Virus o malware de tipo ransonware) y fuga de información.

El ingeniero indica que conoce qué es un SGSI, a pesar de que la empresa no lo posee, en cambio el analista manifiesta no conocerlo; de ahí la importancia que le dan a la seguridad de la información, en donde el ingeniero la considera muy importante, mientras que el analista lo considera medianamente importante. La ausencia de un SGSI en la empresa hace que no se aplique ninguna metodología de seguridad de la información.

En lo referente a los riegos, los encuestados manifiestan que no existe un sistema de gestión de riesgos en la empresa, lo que implica que no aplican ninguna metodología, como: ISO 31000, ISO 27005, MAGERIT y OCTAVE. Además, la empresa no posee un manual de políticas de seguridad de la información, aun así, ambos entrevistados afirman que la empresa posee firewall y planes de mantenimiento como controles de seguridad informática; además, el ingeniero agrega que existe un monitoreo de seguridad, mientras que el analista agrega que existe control de malware (antivirus). A pesar de la importancia que le dan a la implementación de un SGSI, consideran que esto no se da por factores asociados a tiempo y presupuesto.

Al realizar un contraste de lo establecido por los dos encuestados, frente a lo respondió por el gerente, se pudo establecer que dichas respuestas concuerdan con las del ingeniero, pero no necesariamente con las del analista, esto conduce a interpretar que a mayor conocimiento más claridad sobre el estado actual de la empresa.

5.2.3. Validación por observación de experto

Una vez aplicado los instrumentos de acuerdo al marco metodológico propuesto, se concluye que la empresa no posee un SGSI, tampoco tiene planteada unas políticas de seguridad de la información, lo que deriva además en vacíos operativos en torno a los sistemas de control, la falta de conocimiento por parte de los empleados y la ausencia de buenas prácticas de seguridad informática como: Cambio de contraseña automático de forma periódica, planes de mantenimiento de hardware y software, boletines periódicos de seguridad para los empleados, planes de formación de seguridad para los empleados. Es importante resaltar que, estas falencias pueden afectar de forma importante la operación de la empresa, dado que los empleados, son enviados a operar las infraestructuras y la información de los clientes, con lo cual puede también afectarse a terceros.

No obstante, se encuentran implementados algunos controles de seguridad de la información físicos como son, el control de acceso al edificio y registro de las personas que llegan a las instalaciones, se cuenta con cámaras de vigilancia, acceso restringido a la base de datos, con-

trol de acceso a las carpetas del servidor de archivos donde está alojada la información de clientes y proveedores y se observa que se cuenta que hay una persona con un conocimiento almenos básico en seguridad informática.

5.3. Implementación de la metodología

Para el proceso de implementación, inicialmente se hace una reunión con el ingeniero de proyectos y el analista de soporte de la empresa objeto de estudio, con el fin de contextualizarlos acerca de la metodología para el desarrollo del proceso, seguidamente se procede a realizar el plan de trabajo, el cual consta de las siguientes 5 fases:

- **Fase I.** Análisis GAP inicial.
- **Fase II.** Contextualización de la organización.
- **Fase III.** Análisis de riesgos.
- **Fase IV.** Construcción de la política general y operacional.
- **Fase V.** Evaluación de la metodología.

Cabe aclarar que, aunque la metodología propuesta se compone de 29 guías, en este caso de estudio sólo se aplicaron 6 de ellas, debido a las limitaciones de tiempo del proyecto, pues la implementación de todas las guías relacionadas con los controles requeriría un tiempo mayor de ejecución, que está fuera del alcance de este proyecto.

En adelante se describirán de forma general los principales aspectos del resultado de la implementación. Cabe aclarar que no se describirán detalles, dado que estos corresponden a datos confidenciales de la empresa.

5.3.1. Preliminares

Como primer momento de la aplicación de la metodología, el ingeniero crea una carpeta con los permisos de lectura y escritura para los intervinientes en la aplicación de la metodología, la cual se almacena en: (Infraestructura), donde se copian los documentos (Guías y herramientas de riesgos, de análisis SOA y controles). Para consultas posteriores, el ingeniero crea un portal en WordPress para acceder a consultas en la web. Para el proceso de seguimiento se realiza dos reuniones semanales con los implementadores, para que estos diligencien las encuetas una vez que se aplica cada guía. Antes de comenzar con la implementación se solicita a los dos participantes del proceso consultar la guía cero(0), que contiene el marco conceptual para la aplicación de la metodología, y la guía uno (1), que incorpora los aspectos relacionados con la operacionalidad de la metodología propuesta.

5.3.2. Fase I: Análisis GAP inicial

En esta fase se realiza el diagnóstico de la empresa con el fin de establecer la situación actual de ésta en cuanto a la evaluación de un sistema de gestión de seguridad de la información. En este proceso se contó con la participación del ingeniero de proyectos quien fue el encargado de implementar la herramienta de análisis GAP de controles. En el desarrollo de esta fase no se presentó ningún tipo de dificultad y se pudo concluir que la empresa no cuenta con un análisis de riesgos de la seguridad de la información, no hay políticas de seguridad de la información y que además debe mejorar el monitoreo de la continuidad de la seguridad, así como fortalecer las tecnologías para la protección de la información, comunicación y cultura para la seguridad de la información, por parte de los empleados como se puede apreciar en la Fígura **5-1**.

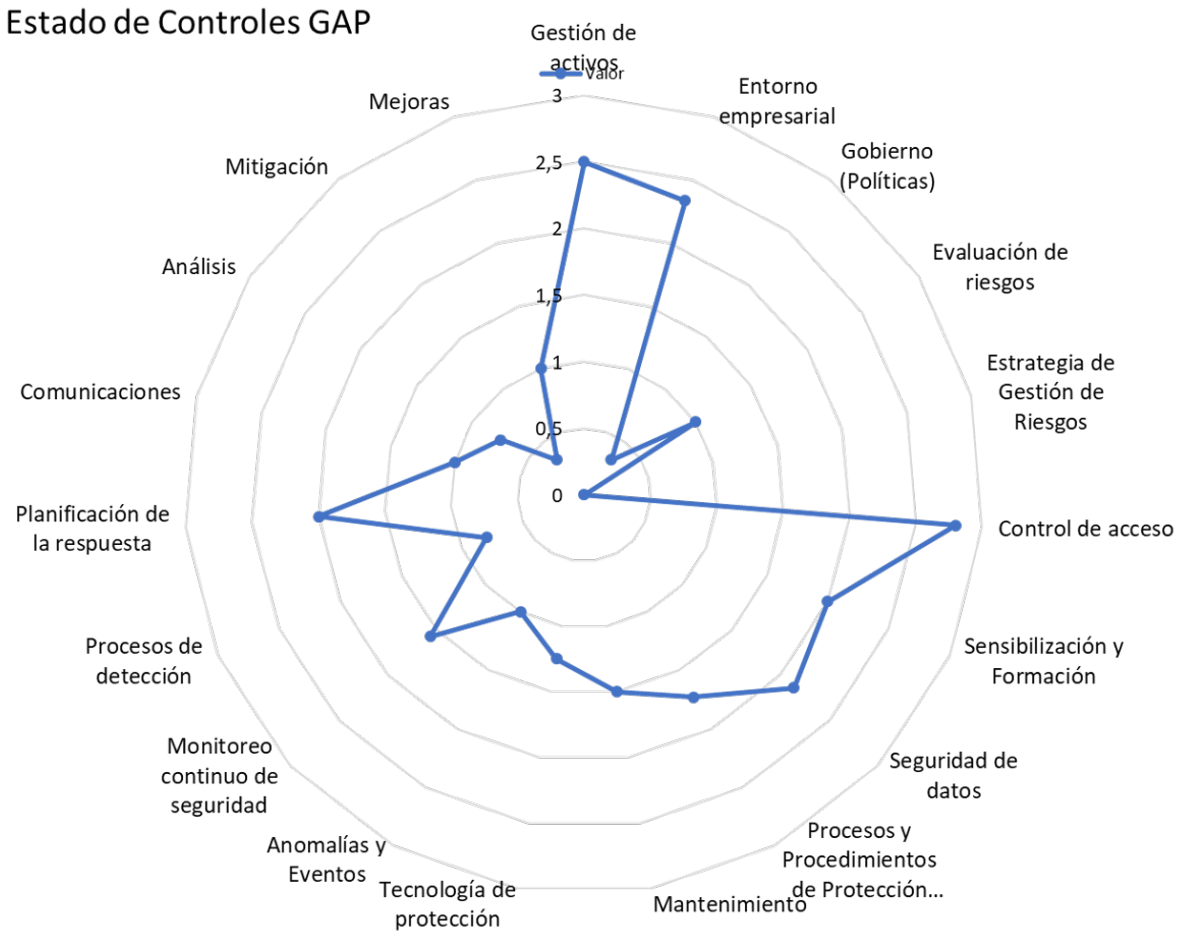

Figura 5-1.: Controles iniciales GAP caso estudio - Fuente: Construcción propia

Además de evidenciar los resultados obtenidos con la aplicación de la guía, se solicito al ingeniero implementador diligenciar una encuesta (Anexo E: Encuesta de verificación dela implementación del análisis GAP de controles existentes en la organización), con el fin de evaluar la implementabilidad de la herramienta de análisis GAP de controles fueron los siguientes:

Se estableció que la herramienta es entendible y comprensible, además que facilita la valoración de los controles existentes en la organización e igualmente, aporta al conocimiento para el desarrollo de las funciones del cargo que el implementador desempeña. Además, manifiesta que le aporta al desarrollo de la gestión de los procesos en el SGSI.
De igual forma, el funcionario entrevistado valoró con un nivel de cumplimiento amplio, aunque no le dio la mayor calificación, los ítems relacionados con la implementación de la herramienta GAP para la valoración de los controles, la interpretación de la gráfica para la toma decisiones es útil, y también consideró, en este nivel de calificación, que la herramienta es útil para el propósito del control del SGSI.

5.3.3. Fase II: Contextualización de la organización y alcance del SGSI

Esta fase fue desarrollada por el analista de soporte, en donde se aplicó la guía de contextualización y alcance de la metodología. Para el desarrollo de esta guía se utilizó como ayuda metodológica el mapa de proceso de la organización. Como resultado se entrega un informe, el cual refleja el diagrama del contexto de la organización que se obtuvo a través de la utilización de la metodología elipses, la cual consiste en presentar la información detallada por capas. En la primera capa se reflejan los procesos críticos o misionales de la organización como son el área de comercial, infraestructura y outsourcing, en la segunda se reflejan las áreas de apoyo como son recursos humanos, el área administrativa, el sistema de salud en el en trabajo, gestión estratégica y planeación y mensajería, en la capa tres se muestran los proveedores, organizaciones y clientes de la organización. Terminadas las anteriores etapas se procede a aplicar la encuesta para validar la aplicabilidad por parte del analista, obteniendo los siguientes resultados:

Según los resultados obtenidos en la encuesta (Anexo F: Encuesta de verificación dela implementación de la guía de contextualización - alcance) aplicada al analista de soporte, se evidencia que en relación al entendimiento de la guía de contextualización y alcance en lo que tiene que ver con contenidos, implementación, controles, utilización de la metodología elipses, la utilidad de la guía y el aporte de la guía al desarrollo de la gestión de los procesos en el SGSI es fácilmente comprensible.

Como observación, el analista recomienda que los documentos que se utilicen sean los reco-

mendados por el proceso de calidad de la organización.

5.3.4. Fase III: Gestión de riesgos

Esta fase fue realizada por el ingeniero del proyecto y el analista de soporte, para lo cual se usó la guía de riesgos y la herramienta de gestión de riesgos. Una vez revisada la guía inician con el proceso de implementación de ésta para realizar la gestión del riesgo, para ello se propusó una herramienta de gestión de riesgos construida en excel, la cual contiene las siguientes variables: alcance, identificar-clasificación, valoración-activos, inventario amenazas, controles actuales, escenario riesgos, agentes generadores, análisis de riesgos, aceptar-control-mapa-calor y tratamiento; y otras tablas de apoyo en la construcción como: Tabla-controles, tabla-impacto, tabla-amenazas y tabla-vulnerabilidades.

La fase inicia con la construcción de las siguientes variables: alcance, identificar-clasificación, valoración – activos. La guía permitió que los actores involucrados en el proceso realizaran un adecuado diligenciamiento de la herramienta en las variables de alcance, identificar-clasificación, valoración-activos; no obstante, se dificultó el análisis en las variables de: Inventario amenazas, controles actuales, escenario riesgos, agentes generadores, análisis de riesgos, aceptar-control-mapa-calor y tratamiento, esto debido a que la información obtenida entre las amenazas, las vulnerabilidades y los activos de información fueron densos, por lo tanto poco prácticos para trabajarlos de forma manual, debido a que se obtuvieron 280 escenarios de riesgos.

Para facilitar el análisis de las variables, se construyó otra herramienta de gestión de riesgos en excel, en donde se analizaron 11 de las 280 amenazas encontradas. Esta herramienta consta de dos hojas donde se encuentran las variables de alcance y gestión del riesgo; en esta última, se encuentran las variables de clasificación y valoración de activos, análisis de riesgos y tratamiento de riesgos; además, se adicionan cuatro hojas de consulta y de referencia para el implementador, (impacto y probabilidad, inventario de amenazas, inventario de vulnerabilidades e inventario de controles).

Según lo arrojado en la encuesta (Anexo G: Encuesta de verificación de la implementación de la guía de gestión del riesgo), una de las guías que presentó más dificultad en el proceso de implementación en la empresa, fue la de gestión de riesgos. Como ya se ha mencionado el análisis de riesgos es el corazón del sistema de gestión de seguridad de la información, uno de los trabajos futuros que queda es el desarrollo de una herramienta la cual debe ser intuitiva en el momento de realizar el análisis de riesgos, dicho trabajo se viene desarrollando con un estudiante de ingeniería en su proyecto de grado.

5.3.5. Fase IV Aplicabilidad de las guías

El ingeniero solicita aplicar las dos guías siguientes:

- Política de seguridad de la información general.
- Política de seguridad de la información operacional.

Estas dos guías fueros entregadas al ingeniero para su aplicabilidad en la empresa.

5.3.6. Aplicabilidad de las guías política de seguridad de la información

Esta fase fue realizada por el ingeniero, donde indica que la guía fue muy practica y por lo tanto facilitó la elaboración de la política general de la seguridad de la información de la empresa, esto se refleja en el instrumento de evaluación (Anexo H: Encuesta de verificación dela implementación de la guía de política de seguridad de la información) el cual arrojó los siguientes resultados: Manifiesta que el conjunto de definiciones contenidas en la guía es comprensible y se ajusta a un adecuado entendimiento; igualmente, considera que la línea base descrita en la guía le permite la implementación en el proceso del SGSI; además, declara que la guía le facilitó la identificación de los componentes de la política relacionados con el alcance, aspectos legales y nivel de cumplimiento en la organización; no obstante, en este aspecto, la persona encuestada retroalimenta el proceso donde identifica que es necesario ajustar los mismos al contexto del negocio; también considera que la guía de políticas y seguridad de la información es de fácil entendimiento para las partes interesadas y que la guía es útil para los propósitos de la metodología propuesta del SGSI de la empresa. Así mismo, manifiesta que la guía le aporta al conocimiento para el desarrollo de sus funciones e igualmente aporta a la gestión de los procesos en el SGSI de la organización.

Una vez materializados los resultados en la implementación de la guía de la política de seguridad de la información, se recibe el aval de parte de la gerencia general para que dicha política sea socializada e implementada en la empresa.

5.3.7. Aplicabilidad de las guías política de seguridad de la información operacional

Esta fase fue realizada por el ingeniero de proyectos, donde se indica que la implementación de la guía de la política de seguridad de la información operacional se realizó sin ninguna dificultad, además menciona que la guía es lo suficientemente amplia y que tiene aplicabilidad en cualquier organización que quiera implementar un SGSI, ya que en su contenido aborda aspectos relacionados con medios almacenamiento, software, hardware, personas y procesos,

necesarios en una política de seguridad de la información operacional para la protección de los activos de la información. En la aplicación del instrumento (Anexo I: Encuesta de verificación dela implementación de la guía de política de seguridad de la información operacional) se obtuvo como resultados que los aspectos evaluados fueron valorados con el rango mas alto, los cuales estaban orientados a verificar la aplicabilidad en cuanto a comprensibilidad, entendimiento, implementación, identificación de los componentes operacionales de la estructura para proteger los activos de información, de fácil comprensión por las personas interesadas, es útil y aporta a la gestión de procesos.

La política de seguridad de la información operacional es aprobada y cuenta con el consentimiento del gerente general para su aplicación en la empresa.

5.4. Conclusiones y aplicabilidad de la metodología propuesta

Una vez aplicados los instrumentos propuestos (encuestas) al ingeniero de procesos y al analista de soporte, quienes fueron las personas que acompañaron todo el proceso de estudio de campo designados por la administración de la empresa objeto de estudio, para la fase de implementación de la metodología propuesta del SGSI, manifestaron su percepción relacionada con la implementación de cada guía propuesta para el estudio, tanto el ingeniero como el analista declararon reconocer un alto nivel de importancia de las guías, lo que generó facilidades en las diferentes etapas del proceso, concretamente en: La implementación del sistema, la utilidad en la toma de decisiones, la importancia al logro de la implementación del SGSI de la organización, el provecho de nuevos conocimiento adquiridos y la importancia en el desarrollo de la gestión del SGSI de la organización. Se resalta que esta fase tenía como propósito analizar la metodología implementada en el caso de estudio, como intención fundamental de este objetivo, para ello se elaboró un instrumento (Anexo J: Encuesta de verificación de la implementación de la metodología de SGSI para pymes del sector de la información y comunicaciones de la ciudad de Medellín) la cual, una vez aplicada a los ejecutores (ingeniero – analista) se obtienen los siguientes resultados:

Valoran con una calificación alta la importancia de la metodología para la protección de los activos de la información, en el mismo sentido de valoración reconocen que la metodología reduce los tiempos de implementación con relación a otros sistemas existentes en la industria, además son concluyentes al afirmar que la metodología cumple con los principios institucionales de seguridad de la información declarados por la empresa como: Integridad, confidencialidad y disponibilidad, y al mismo tiempo coinciden en que el proceso de aplicación de la metodología los cualifica para el desarrollo de las funciones del cargo que desempeñan.

En cuanto a la claridad y comprensión de la metodología es totalmente clara para el ingeniero, lo cual no es lo mismo para el auxiliar, que, aunque la ubica en un rango de calificación alto, no la valora en el rango mayor. En relación a la guía que identifica los componentes del sistema como riesgos, políticas y controles, que permiten proteger los activos de información, es valorado por el auxiliar con el rango más alto, mientras que el ingeniero la califica con un nivel alto, pero no con el mayor. Frente a la necesidad de requerimiento de personal especializado con formación específica para la implantación del SGSI, las dos personas intervinientes en el proceso los califican en un nivel alto de cumplimiento, aunque no lo valoran con el rango mayor, y además están de acuerdo en afirmar que la metodología contribuye a los requerimientos de gestión de seguridad de la información de sus clientes, en este ítem el auxiliar lo valora con el nivel mayor mientras que el ingeniero considera que tienen un valor alto pero no lo califica con el valor máximo.

6. Conclusiones y trabajos futuros

Este trabajo presentó una propuesta metodológica para la implementación de sistemas de gestión de seguridad de la información en pequeñas y medianas empresas del sector de la información y de las comunicaciones de la ciudad de Medellín, la cual consta de 29 guías completamente documentadas.

El desarrollo de este trabajo con un estudio inicial que mostró que, como ha sido descrito en la literatura, la implementación de sistemas de gestión de seguridad de la información es baja en pequeñas y medianas empresas, aún en las empresas del sector de la información y las comunicaciones. Este estudio, basado en encuestas realizadas a 40 PyMEs de este sector en la ciudad de Medellín, mostró además que, aún cuando la mayoría de las empresas reconocen la importancia de la información y de la adopción de estrategías que propendan por la seguridad de la misma, la adopción de procedimientos y estándares es bajo. Así mismo, se evidenció un conocimiento promedio entre los encuestados sobre las amenazas informáticas que podrían afectar a sus empresas, aunque se observó una subvaloración de riesgos como la suplantación de identidad, el vandalismo y los mismos desastres naturales, que son comunmente controlados en una implementación de un SGSI. Entre los factores que impiden la implementación de un SGSI en las empresas de este sector, el estudio mostró que, para los participantes, el tiempo, el presupuesto y la falta de conocimiento especializado son los de mayor incidencia. En este punto es importante mencionar que de 304 empresas invitadas a participar, sólo 45 respondieron a la solicitud, y de estas sólo 40 respondieron a la encuesta en su totalidad, a pesar de haber insistido 3 veces en la invitación. Esto podría ser también una evidencia de una baja preocupación por los temas de seguridad de la información en este sector. Por lo anterior, este estudio pesenta un nivel de confianza del 85 %, con una tasa de error del 10 %, por lo cual, sus resultados no se pueden considerar absolutamente concluyentes. Por lo anterior, se considera que una investigación orientada exclusivamente a este aspecto puede ser relevante, caso en el cual se deberán buscar aliados o estratégias para aumentar la participación de las empresas.

La metodología propuesta se centra en la gestión de riesgos, pero involucra aspectos del contexto de la organización, la implementación de controles, la verificación y la mejora continua. Para su diseño se tomaron en cuanta aspectos propuestos por las metodologías más usadas para la implementación de SGSIs, gestión de riesgos e implementación de controles, como son: ISO 27001, ISO 27002, ISO 27005, ISO 31000, COBIT, NIST 800-53, NIST 800-30,

Octave y MAGERIT. Esto permitió desarrollar una metodología que involucra componentes desde el nivel estratégico, táctico y operacional de la compañia.

Como se puede observar en el caso de estudio llevado a cabo en el marco de este proyecto, la implementación de la metodología propuesta no requiere grandes inversiones de recursos económicos o de tiempo, y tampoco exige la participación de personal experto en el área de la seguridad de la información, pues para los participantes, quienes tienen diferentes niveles de formación, un ingeniero y un tecnologo, las guías fueron comprensibles y fáciles de implementar. Además, en todos los casos, les permitió mejorar sus conocimientos sobre el tema, los cuales les permitirán mejorar el desempeño de sus funciones. Sin embargo, es necesario aclarar que sí es requerido que el implementador tenga un conocimiento básico sobre temas relacionados, de forma tal que pueda comprender con facilidad el documento conceptual que soporta todas las guías (guía 0). Por lo anterior, como manifiestan los implementadores del caso de estudio, esta metodología podría ser facilmente aplicable a cualquier PyME, incluso de otros sectores económicos.

De acuerdo con los participantes en el caso de estudio, la implementación de un SGSI usando la metodología propuesta trae ventajas para la empresa las cuales se condensan en los siguientes puntos:

- Permite a las empresas la adopción de la seguridad de la información a sus activos core del negocio.
- Reduce costos en proyectos relacionados con la implementación de SGSI.
- Proporciona mecanismos para generar sensibilidad y conciencia en los colaboradores de las compañías sobre la seguridad de la información.
- Genera consciencia a la alta dirección sobre los riesgos a los que están sujetos los activos de la información.
- Permite ser proactivos ante la resolución de incidentes relacionados con la seguridad de la información.

De igual forma, como aspecto concluyente, los participantes plantearon que con la metodología empleada se logró apreciar, conocer y profundizar sobre temas que no se conocían ni manejaba en labores propias del cargo, entre las que se encuentra, conocer el nivel de importancia que tiene la información con la que se interactúa diariamente, comprender el riesgos y amenazas sobre esta identificar dichos riesgos y amenazas de una manera sencilla y práctica.

Uno de los componentes que requiere más atención para un próximo proceso de investigación es la herramienta para la gestión del riesgo, la cual, según los implementadores, debe ser

más intuitiva y de fácil compresión. Por lo anterior, se ha planteado como trabajo futuro, el desarrollo de una herramienta de software que tome como base la guía de gestión de riesgo planteada en esta metodología; este trabajo se ha planteado como un trabajo de grado para un estudiante de ingeniería de sistemas, el cual se encuentra en ejecución.

Adicionalmente, las demás guías propuestas y la tabla de controles en la metodología podrían incorporar nuevos elementos o mejorar lo existentes, todo depende de las necesidades de cada organización que quiera implementarla la metodología propuesta.

Bibliografía

[1] Dmitry, "Kaspersky Lab registra un alza de 60 % en ataques cibernéticos en América Latina — Blog oficial de Kaspersky," tech. rep., Kaspersky Lab, 2018.

[2] Karspersky Lab, "Kaspersky Security Bulletin:OVERALL STASISTICS FOR 2017," tech. rep., 2018.

[3] Tecnósfera, "Informe sobre ataques informáticos en Colombia y al sector financiero - Novedades Tecnología - Tecnología - ELTIEMPO.COM," tech. rep.

[4] Caivirtual.policia.gov., "Informe de Amenazas del cibercrimen en Colombia 2016-2017," tech. rep., Centro Cibernetico de la Policia Nacional de Colombia, 2017.

[5] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems :," tech. rep., National Institute of Standards and Technology, Gaithersburg, MD, 2002.

[6] PriteshGupta.com, "ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información," 2018.

[7] C. J. Almanza Andres, "ACIS - XVIII Encuesta Nacional de Seguridad Informática Evolución del perfil del profesional de seguridad digital," p. 76, 2018.

[8] NIST - National Institute of Standards and Technology, "Guia de la NIST 800-53 (Rev. 4)," 2019.

[9] ISACA, *COBIT 5 Framework*. 2012.

[10] Axelos Global Best Practice, "ITIL — Gestión de servicios informáticos — ITSM — AXELOS," 2019.

[11] P. administracion electronica, "PAe - MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información," 2019.

[12] B. Shojaie, H. Federrath, and I. Saberi, "The Effects of Cultural Dimensions on the Development of an ISMS Based on the ISO 27001," in *2015 10th International Conference on Availability, Reliability and Security*, pp. 159–167, IEEE, aug 2015.

[13] A. Santos Olmo Parra, L. E. Sanchez Crespo, E. Alvarez, M. Huerta, and E. Fernandez Medina Paton, "Methodology for Dynamic Analysis and Risk Management on ISO27001," *IEEE Latin America Transactions*, vol. 14, pp. 2897–2911, jun 2016.

[14] M. Panjwani, M. Jantti, and J. Sormunen, "IT Service Management from a Perspective of Small and Medium Sized Companies," in *2016 10th International Conference on the Quality of Information and Communications Technology (QUATIC)*, pp. 210–215, IEEE, sep 2016.

[15] Gutiérrez Amaya Camilo, "¿Cuánto demoraremos en lograr la madurez de la seguridad en PyMEs? — WeLiveSecurity," Welivesecurity, 2017.

[16] Departamento Administrativo de la Función Pública, "Ley 590 de 2000 - Gestor Normativo Función Pública," 2000.

[17] CCMA, "Camara de Comercio de Medellin," 2019.

[18] Y. J. Medina Cabrera, H. Castro Rios, and H. G. Pulido Quedo, "Plan de negocio para la implementación de una empresa de consultoría en el sistema de gestión de la seguridad de la Información," *Universidad Tecnológica del Perú*, 2017.

[19] G. Pallas and M. E. Corti, "Metodología de Implantación de un SGSI en grupos empresariales de relación jerárquica," 2009.

[20] Á. M. Parra-Giraldo, "ISO 27001 PARA PYMES," oct 2014.

[21] International Organization for Standardization, "ISO 31000 Gestión de riesgos," 2019.

[22] Instituto Nacional de Estándares y Tecnología de los Estados Unidos la NIST, "Publication Number: NIST Special Publication (SP) 800-53 Revision 4 Title: Security and Privacy Controls for Federal Information Systems and Organizations," no. NIST, 2013.

[23] Aceituno Vicente, "ISM3 The Open Group lanza modelo de madurez para la gestión de seguridad de la información," 2011.

[24] P. E. Crespo Martínez, "Metodología de seguridad de la información para la gestión del riesgo informático aplicable a MPYMES," 2016.

[25] UNGRD, "TERMINOLOGÍA SOBRE GESTIÓN DEL RIESGO DE DESASTRES Y FENÓMENOS AMENAZANTES," 2017.

[26] International Organization for Standardization, "ISO 31000 Gestión de riesgos."

[27] INCIBE, "INCIBE —," 2019.

[28] Gutierrez Pinilla Nelson Alberto, "Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 - Octubre de 2018." 2018.

[29] Direccion del Departamento Administrativo de la Función Pública, "DAFP - Decreto 1537 de 2001 - Gestor Normativo Función Pública," 2001.

[30] Erik José Enríquez Carmona, "OCTAVE, metodología para el análisis de riesgos de TI," tech. rep., UniVerso: El Periódico de los Universitarios, 2013.

[31] Organización Internacional para la Estandarización, "ISO / IEC 27005: 2018 - Tecnología de la información - Técnicas de seguridad - Gestión de riesgos de seguridad de la información," 2018.

[32] PriteshGupta.com, "El portal de ISO 27002 en Español," 2019.

[33] DANE, "CIIU - clasificación industrial internacional uniforme de todas las actividades económicas," tech. rep., DANE, 2012.

[34] ONU Departamento de Asuntos Económicos y Sociales and División de Estadística, *Clasificación Industrial Internacional Uniforme de todas las actividades económicas (CIIU) Rev.4*. No. 4, 2009.

[35] Departamento Administrativo Nacional de Estadística (DANE), "DANE," 2019.

[36] M. R. Spiegel and L. J. Stephens, *Estadística/Theory and problems of statistics*. No. 519.2, McGraw-Hill,, 2009.

[37] D. E. Acosta, "Guía rápida para entender el marco de trabajo de ciberseguridad del NIST — Blog de Internet Security Auditors," tech. rep., 2016.

[38] Magerit, "EAR / PILAR / Magerit," 2012.

[39] MinTIC, "Modelo de Seguridad Guías de Seguridad para Pymes," 2019.

[40] C. la camara de chile, "Guía de ciberseguridad para PYMEs," 2019.

[41] E-global, "E-Global — Profesionales en TIC," 2019.

A. Encuesta empleada para el diagnóstico del nivel de implementación de SGSIs

Corresponde a la plantilla que contiene la información de las preguntas de la encuesta utilizada para identificar el nivel de implementación del SGSI en las Pymes del sector de las comunicaciones e información de la ciudad de Medellín, las pregunta están dividida en las siguientes 10 dicciones:

1. Consentimiento Informado de la encuesta
2. Información de la empresa
3. Activos de información
4. Amenazas informáticas
5. Incidentes informáticos
6. Sistema de gestión de la información "SGSI"
7. Administración del riesgo
8. Políticas de seguridad de la información
9. Controles de seguridad informática
10. Factores cree usted que afectan la implementación del Sistema de seguridad de la información, en la compañía.

La encuesta fue elaborada en la aplicación de formularios de Google

Sección / Preguntas
Concentimiento Informado: Con base en el Consentimiento Informado anteriormente, escoja alguna de las siguientes opciones: - Sí responderé el cuestionario - No responderé el cuestionario
1. Información de la empresa 1.1. ¿Cuál es la razón social de su empresa?

1.2.¿Con cuántos empleados cuenta la empresa? (Opción unica)
- Menos de 10 empleados
- Entre 11 a 50 empleados
- Entre 51 a 200 empleados
- Mas de 200 empleados

1.3. Indique la actividad económica de la empresa
(seleccione todas las que apliquen)
- Consultoría informática y actividades de administración de instalaciones informáticas
- Desarrollo de sistemas informáticos planificación, análisis, diseño, programación, pruebas
- Actividades de servicio de información
- Actividades de tecnologías de información y actividades de servicios informáticos
- Actividades de telecomunicaciones
- Portales web
- Procesamiento de datos, alojamiento hosting y actividades relacionadas
- Telecomunicaciones alámbricas
- Telecomunicaciones inalámbricas
- Otra Actividad

1.4. Si su respuesta a la pregunta anterior fue (Otra Actividad), Indique cuál:

1.5. ¿Cuál es el cargo que ocupa en la empresa?

2. Activos de información

2.1. ¿Qué nivel de importancia le da su empresa a los activos de información? (Opción unica)
- Alta
- Media
- Baja

2.2. Según su percepción, qué nivel de importancia le dan sus empleados a la información que estos manejan (Opción unica)
- Alta
- Media
- Baja

2.3. ¿Cuenta su empresa con un responsable de la seguridad de la información? (Opción unica)

- Si
- No

2.4. La persona encargada de la seguridad de la información tiene formación especializada en el área (Opción unica)
- Si
- No
- No Sabe

3. Amenazas informáticas

3.1. ¿Conoce usted los diferentes tipos de amenazas informática que pueden afectar a su empresa? (Opción unica)

- Si
- No

3.2. En términos generales, cuáles de las siguientes amenazas informáticas considera usted que podrían afectar la información de su empresa (seleccione todas las que apliquen)

- Virus informáticos o código malicioso
- Uso no autorizado de sistemas informáticos
- Robo de información
- Fraudes basados en el uso de computadores
- Suplantación de identidad
- Denegación de servicios (DoS)
- Ataques de fuerza bruta
- Alteración de la información
- Divulgación de información
- Desastres naturales
- Sabotaje, vandalismo
- Espionaje
- Pérdida de información
- Fuga de información
- Indisponibilidad del servicio
- Suplantación a su sitio Web
- Otras Amenazas

3.3. Si su respuesta a la pregunta anterior fue .ºtro Amenaza", describa cuál:

4. Incidentes informáticos

4.1. ¿Su empresa ha sufrido algún tipo incidente informático? (seleccione todas las que apliquen)

- Infecciones de Malware (Virus o Malware de tipo Ransonware)
- Accesos no autorizados a la información
- Perdida de información
- Fuga de información
- Indisponibilidad del servicio
- Suplantación a su sitio Web
- No he sufrido ataque informático
- Otro Incidente Informático

4.2. Si su respuesta a la pregunta anterior fue .ºtro Incidente Informático", describa cuál:

5. Sistema de gestión de la información "SGSI"

5.1 ¿Qué tan importante es la seguridad de la información en su empresa? (Opción unica)

- Muy importante
- Medianamente importante
- De importancia baja

5.2. ¿Sabe usted qué es un sistema de gestión de seguridad de la información "SGSI¿ (Opción unica)

- Si
- No

5.3. ¿Su empresa cuenta con una implementación de un sistema de gestión de la información "SGSI¿ (Opción unica)
- Si
- No

5.4. Los procesos y procedimientos de seguridad implementados en su empresa se basan en alguna de las siguientes normas internacionales (seleccione todas las que apliquen)

- ISO 27001:2013

- NIST.SP 800-53r4
- COBIT ver 5
- ISM3
- Otra norma internacional de seguridad
- Ninguna de las anteriores normas internacionales de seguridad

5.5. Si su respuesta a la pregunta anterior fue .ºtra norma internacional de seguridad", describa cuál:

6. Administración del riesgo

6.1. ¿Cuenta su empresa con un procedimiento para la gestión de riesgos informáticos? (Opción unica)

- Si
- No

6.2. ¿Cuál de las siguientes metodologías utiliza su sistema para la gestión de riesgos? (seleccione todas las que apliquen)

- DAFP
- ISO 31000
- Nist. 800-30 ver 54
- MAGERIT
- ISO 27005:2011
- Otra Metodología de Riesgos
- Ninguna de las anteriores metodologías de Riesgos

6.3. Si su respuesta a la pregunta anterior fue .ºtra Metodología de Riesgos", describa cuál:

7. Políticas de seguridad de la información

7.1. ¿Cuenta su empresa con un manual de políticas de seguridad de la información?
- Si
- No

8. Controles de seguridad informática

8.1. ¿Qué controles de seguridad informática tiene implementados? (selecciones los que aplique)

- Firewall
- Detectores de intrusos (IDS/IPS)
- Control de malware (Antivirus)
- Sistemas de autenticación y autorización (con token, password, biométricos, 2 factos o similar)
- Monitoreo de seguridad
- Manejo de incidentes de seguridad
- Planes de mantenimiento (Actualización de sistema sistemas operativos, bases de datos y aplicaciones)
- Cultura en seguridad
- Acuerdos de confidencialidad
- Otros controles

8.2. Si su respuesta a la pregunta anterior fue .ºtros controles", describa cuál:

8.3. En términos de controles, cuáles de las siguientes amenazas informáticas considera usted tiene controladas (selecciones los que aplique)

- Virus informáticos o código malicioso
- Uso no autorizado de sistemas informáticos
- Robo de información
- Fraudes basados en el uso de computadores
- Suplantación de identidad
- Denegación de servicios (DoS)
- Ataques de fuerza bruta
- Alteración de la información
- Divulgación de información
- Desastres naturales
- Sabotaje, vandalismo
- Espionaje
- Pérdida de información
- Fuga de información
- Indisponibilidad del servicio
- Suplantación a su sitio Web

9. Factores cree usted que afectan la implementación del Sistema de seguridad de la información, en la compañía

9.1. ¿Qué factores cree usted que afectan la implementación del Sistema de seguridad de la información, en la compañía? (selecciones los que aplique)

- Presupuesto
- Tiempo
- Conocimiento especializado
- Desconocimiento
- No es el foco ni la proyección de la empresa
- Otro factor

9.2. Si su respuesta a la pregunta anterior fue 'Otro factor', describa cuál:

Tabla A-1.: Plantilla de preguntas de la encuesta

B. Análisis SGSI, con su contenido.

Tabla comparativa correspondiente al análisis realizado a la norma internacional ISO 27001:2013 Vs. Metodologías de SGSI COBIT v5 Vs. Guía de NIST 800 53v4 y ISO 27002:2011, donde se obtienen los siguientes resultados

Ciclo PHVA	**ISO 27001:2013**	**COBIT v5**	**NIST 800-53v4**	**ISO 27002:2011**	**Descripción de la integración**
Planear	-Definir el Alcance del SGSI -Definir la Política -Metodología de Evaluación del Riesgo -Definir los roles, responsabilidades y autoridades en la organización -Inventario de Activos -Identificar Amenazas y Vulnerabilidades -Identificar Impacto -Análisis de Evaluación del Riesgo -Selección de Controles SOA (Declaración de Aplicabilidad)	Planeación y organización (PO): -PO1 Definir un Plan Estratégico de TI -PO2 Definir la Arquitectura de la Información -PO3 Determinar la dirección tecnológica -PO4 Definir la Organización y Relaciones de TI -PO5 Manejar la Inversión en TI -PO6 Comunicar las directrices y aspiraciones gerenciales -PO7 Administrar Recursos Humanos -PO8 Asegurar el cumplir Requerimientos Externos -PO9 Evaluar Riesgos -PO10 Administrar proyectos -PO11 Administrar Calidad	1.1 Propósito y aplicabilidad 1.2 Público objetivo 1.3 Relación con otras publicaciones de control de seguridad 1.4 Responsabilidades de la organización 1.5 Organización de esta publicación especial 2.1 Gestión de riesgos multiterior 2.2 Estructura de control de seguridad 2.3 Bases de control de seguridad 2.5 Proveedores de servicios externos		Las metodologías ISO 27001:2013, COBIT v5, Guía técnica y NIST 800-53v4, cuentan con la fase de Planeación en la implementación del SGSI contando con el contexto de la organización, alcance del SGSI, Roles, Responsabilidad y la gestión del riesgo, la ISO 27002:2011 por ser una guía de ISO no cuenta con esta fase. En esta fase la metodología de ISO27001:2013 es más clara y concisa que la metodología COBIT v5 y Nist 800-53 ver 4.

Hacer	-Definir plan de tratamiento de riesgo -Implantar plan de tratamiento de riesgos -Implementar los controles -Formación y concienciación -Operar el SGSI	Adquisición e implementación (AI): -AI1 Identificar Soluciones -AI2 Adquirir y Mantener Software de Aplicación -AI3 Adquirir y Mantener Arquitectura de TI -AI4 Desarrollar y Mantener Procedimientos relacionados con TI -AI5 Instalar y Acreditar Sistemas -AI6 Administrar Cambios Servicios Y Soporte (DS): -DS1 Definir niveles de servicio -DS2 Administrar Servicios de Terceros -DS3 Administrar Desempeño y Calidad -DS4 Asegurar Servicio Continuo -DS5 Garantizar la Seguridad de Sistemas -DS6 Identificar y Asignar Costos -DS7 Capacitar Usuarios -DS8 Asistir a los Clientes de TI -DS9 Administrar la Configuración -DS10 Administrar Problemas e Incidentes -DS11 Administrar Datos -DS12 Administrar Instalaciones -DS13 Administrar Operaciones	2.4 Designaciones de control de seguridad 3.1 Selección de línea de control de seguridad 3.2 Controles de seguridad de línea base a medida 3.3 Creación de planchas 3.4 Documentación del proceso de selección de control 3.5 Nuevos sistemas de desarrollo y legado		Las metodologías ISO 27001:2013, COBIT v5, Guía técnica y NIST 800-53v4, cuentan con la fase de hacer en la implementación del SGSI, la ISO 27002:2011 por ser una guía de ISO no cuenta con esta fase.
Verificar	-Revisar el SGSI -Medir la eficacia de los controles -Revisar los riesgos residuales -Realizar las auditorías internas del SGSI -Registrar acciones y eventos	Monitoreo (M): -M1 Monitorear los procesos. -M2 Evaluar lo adecuado del control interno -M3 Obtener aseguramiento independiente -M4 Proveer auditoría independiente	2.7 Revisiones y extensiones		Las metodologías ISO 27001:2013, COBIT v5, Guía técnica y NIST 800-53v4, cuentan con la fase de Verificación en la implementación del SGSI, la ISO 27002:2011 por ser una guía de ISO no cuenta con esta fase

Ajustar	-Implantar mejoras -Acciones correctivas -Acciones preventivas - Comprobar eficacia de las acciones	Evaluar orientar y supervisar: -EDM01 Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno. -EDM02 Asegurar la Entrega de Beneficios -EDM03 Asegurar la Optimización del Riesgo -EDM04 Asegurar la Optimización de los Recursos -EDM05 Asegurar la Transparencia hacia las Partes Interesadas	2.6 Garantía y confiabilidad		Las metodologías ISO 27001:2013, COBIT v5, Guía técnica y NIST 800-53v4, cuentan con la fase de Actuar o ajustar en la implementación del SGSI, la ISO 27002:2011 por ser una guía de ISO no cuenta con esta fase.
Controles	El anexo A este está compuesto por 14 Dominios, 35 Objetivos y 114 controles de seguridad	Contiene 210 objetivos de Controles	Contiene 256 controles, distribuidos en 18 familias	Guía técnica de ISO 27002:2011, define el cómo se aplican los controles	COBIT ver.5 enfoca sus controles en las tecnologías de la información, cubriendo no solo los controles de seguridad de la información, pero también controles relacionados con las operaciones de TI (por ejemplo, proceso de adquisición). El Anexo A de ISO 27001:2013 tiene controles para cubrir la protección de la información, independientemente de dónde se encuentre.

					En cuanto a la guía NIST SP 800 53 v4, su documentación se centra en los controles de seguridad informática, teniendo también muchos controles descrito en ISO 27001:2013 e ISO 27002:2011, pero con un mayor nivel de detalle, así como controles no cubiertos por ISO 27001:2013, como Ïnternet de las Cosas". Además, algunos documentos de NIST son específicos de la tecnología, como pautas para la seguridad de los sistemas operativos de Apple y Microsoft.
Estructura de la metodología	La norma se divide en 11 secciones más el anexo A correspondiente a los controles operacionales de seguridad	Está constituida por 5 dominios y 34 procesos y 210 Controles	Está compuesta por tres capítulos y 10 apéndices de apoyo en la implementación de los controles de seguridad y cuenta 256 controles distribuidos en 18 familias diferentes.		
Se requiere expertos en Seguridad Informática	Si	Si	Si	Si	
Certificable	Empresas La entidad Certificadora es el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC)	Personas Entidad Certificadora: ISACA (Asociación de Control y Auditoría de Sistemas de Información)	Procesos		NIST SP 800 53 v4 también proporciona algún tipo de proceso de certificación, pero solo los usa internamente la agencias gubernamentales para la liberación de sistemas de información en producción.

Tabla B-1.: Análisis del SGSI

C. Anexo C: Análisis de metodología de riesgos con su contenido

Tabla comparativa correspondiente al análisis realizado a la norma internacional ISO 31000 en riesgos Vs. Normas Técnicas de Gestión ISO 27005:2011, Guía técnica NIST 800-30, Metodología Octave y Magerit, donde se obtienen los siguientes resultados

ISO 31000 Análisis de Alto Nivel	**ISO 27005**	**Guía técnica NIST 800-30**	**Magerit**	**Octave Análisis de Alto Nivel**	**Descripción de la integración**
5.4.1 Contexto de la organización	7. Contexto de la organización	TAREA 1-1: Identifique el propósito de la evaluación de riesgos en términos de la información que la evaluación pretende producir y las decisiones que la evaluación pretende respaldar	Defino el alcance, como se debe hacer el análisis de riesgos y se Incorpora los controles de la ISO 27002:2005 y 2013 Submodelo de eventos dinámico organizativo de MAGERIT	Fase de Preparación de la introducción, donde se cuenta el contexto de la organización	En las normas comparadas tienen en común el contexto de la organización, entendiendo sus necesidades desde una vista interna y externa desde los ámbitos (sociales, culturales, políticos, legales, reglamentarios, financieros, tecnológicos, económicos y ambientales). Este abarca Roles Responsabilidades. OCTAVE se centra en el estudio de riesgos organizacionales, principalmente en los aspectos relacionados con el día a día de las empresas. La evaluación inicia a partir de la identificación de los activos relacionados con la información, definiendo este concepto con los elementos de TI que representan valor para la empresa (sistemas de información, software, archivos físicos o magnéticos, personas).

5.2 Liderazgo y compromiso	El compromiso de la alta dirección se menciona en la norma 27001:2013 (Sección 5. Liderazgo) de alto nivel para el sistema de gestión de la información y no en la 27005.			Fase de Adaptación de la dirección	Es te punto es esencial ya que la alta dirección debe estar comprometida con los riesgos expuestos en el medio tanto internos como externos, solo están cubiertas por las metodologías de riesgos ISO 3100 y OCTAVE.
5.4.4 Asignación de recursos	En apoyo de los recursos, sea hace referencia en la 27001:2013 (sección 7.1 Recursos)		Submodelo de eventos estático de MAGERIT: relacional del submodelo de eventos refleja las relaciones generales entre los elementos reseñados en el submodelo de entidades y se necesita básicamente para establecer el modelo lógico de datos que requiere toda herramienta de apoyo a la aplicación de MAGERIT.		La organización debe garantizar la asignación de los recursos necesarios para la gestión del riesgo, las metodologías que cubren este punto es ISO 3100, ISO27007 y MAGERIT.

6.2 Comunicación y consulta	11 Comunicación y consulta de los riesgos para la seguridad de la información	3.3 comunicación y compartir información de evaluación de riesgo. Abarca las siguientes tareas: TAREA 3-1: comunicar los resultados de la evaluación de riesgos a los responsables de la toma de decisiones de la organización para respaldar las respuestas de riesgo. TAREA 3-2: Comparta la información relacionada con el riesgo producida durante la evaluación del riesgo con el personal de la organización apropiado.			Las normas ISO 31000, ISO 27005 y Nist 800-30 definen el propósito de la comunicación y consulta es asistir a las partes interesadas pertinentes a comprender el riesgo y definir los planes en estas tres metodologías.
6.3.4 Definición de los criterios del riesgo	7.2.2 Criterios de evaluación del riesgo	TAREA 1-3: Identifique las suposiciones y restricciones específicas bajo las cuales se lleva a cabo la evaluación de riesgos. Fuentes de amenazas. Eventos de Amenaza Vulnerabilidades y condiciones predisponentes Probabilidad Impactos Tolerancia al riesgo e incertidumbre Enfoque analítico Abarca las siguientes tareas: TAREA 1-5: Identifique el modelo de riesgo y el enfoque analítico que se utilizará en la evaluación de riesgos	Submodelo de elementos cubre (Activos, Amenazas, Vulnerabilidades, Impactos, Riegos y Salvaguardas)	Fase para establecer los criterios de medición del riesgo.	La organización debería precisar la cantidad y el tipo de riesgo que puede o no puede tomar, con relación a los objetivos.

6.3.4 Definición de los criterios del riesgo	7.2.3 Criterios de impacto	TAREA 1-4: Identifique las fuentes de información descriptiva, de amenazas, de vulnerabilidad y de impacto que se utilizarán en la evaluación de riesgos	Submodelo de los elementos, el cual contempla 6 temas: Activos, Amenazas, vulnerabilidades, Impacto, Riegos y Salvaguardas (Controles).	Fase de Identificar escenarios de amenaza	La organización debe establecer, implantar y mantener. un proceso formal y documentado de análisis de impacto en el negocio y de apreciación del riesgo
6.3.4 Definición de los criterios del riesgo	7.2.4 Criterios de aceptación del riesgo	TAREA 1-4: Identifique las fuentes de información descriptiva, de amenazas, de vulnerabilidad y de impacto que se utilizarán en la evaluación de riesgos.	Submodelo de los elementos, el cual contempla 6 temas: Activos, Amenazas, vulnerabilidades, Impacto, Riegos y Salvaguardas (Controles).	Analizar riesgos, OCTAVE en esta fase mide de forma cualitativa el grado en el que la organización es afectada por una amenaza y se calcula una puntuación para cada riesgo de cada activo de información	Las normas en mención definen los criterios correspondientes al apetito del riesgo y parámetros para el proceso del diseño del análisis del riesgo estos deben estar alineados al contexto de la organización.
6.3.2 Definición del alcance	7.3 Alcance y límites	Identificar alcance TAREA 1-2: Identifique el alcance de la evaluación de riesgos en términos de aplicabilidad organizacional, marco de tiempo compatible y consideraciones de arquitectura / tecnología	Submodelo de procesos: Planificación del proyecto de riesgos		Se definen los límites y alcance de gestión del riesgo, en las organizaciones, se remite a la ISO 3100, ISO 27005, Nist 800-30 y MAGERIT para la gestión del riesgo

5.4.3 Asignación de roles, autoridades, responsabilidades y obligación de rendir cuentas en la organización	7.4 Organización para la gestión de riesgos en materia de seguridad de la información	3.1 preparación para la evaluación del riesgo	Submodelo de procesos: Planificación del proyecto de riesgos	OCTAVE contempla para su implementación la conformación de un equipo mixto, compuesto de personas de las áreas de negocios y de TI. Esta configuración explica el hecho de que los funcionarios del negocio son los más indicados para identificar qué información es importante en los procesos y cómo se usa dicha información; por su parte, el equipo de TI, es el que conoce la configuración de la infraestructura y las debilidades que pueden tener, estos dos puntos de vista son importantes para tener una visión global de los riesgos de seguridad de los servicios de TI.	Las normas definen roles y responsabilidades, que tendrán en las normas que sea aplicada.
6.4 Evaluación del riesgo	8 Evaluación del riesgo para la seguridad de la información	3.2 realización de la evaluación de riesgos identificar fuentes de amenaza: TAREA 2-1: Identifique y caracterice las fuentes de preocupación de amenazas, incluidas la capacidad, la intención y las características de focalización para las amenazas adversas y el rango de efectos para las amenazas no adversas.	Submodelo de procesos: Análisis de riesgos	Fase de Identificar riesgos Fase para desarrollar el perfil de los activos informáticos partiendo de de las siguientes dos fases: Fase 1 de Construcción de perfiles de amenazas basadas en activos. Fase 2 de Identificación de vulnerabilidades en la infraestructura. Fase de Identificar contenedores de activos de información.	Este literal cubre Evaluación, identificación, análisis y evaluación del riesgos en las metodologías en mensión (ISO 31000, ISO 27005, Nist 800-30, MAGERIT y OCTAVE)

		TAREA 2-2: Identifique los eventos de amenaza potenciales, la relevancia de los eventos y las fuentes de amenazas que podrían iniciar los eventos. TAREA 2-3: Identifique las vulnerabilidades y las condiciones predisponentes que afectan la probabilidad de que los eventos de amenaza de preocupación resulten en impactos adversos. TAREA 2-4: Determine la probabilidad de que los eventos de amenaza de preocupación resulten en impactos adversos, considerando: las características de las fuentes de amenaza que podrían iniciar los eventos; las vulnerabilidades / condiciones predisponentes identificadas; y la susceptibilidad organizativa que refleja las medidas de seguridad / medidas preventivas planificadas o implementadas para impedir tales eventos.			

		TAREA 2-5: Determine los impactos adversos de los eventos de amenaza de preocupación, considerando: las características de las fuentes de amenaza que podrían iniciar los eventos; las vulnerabilidades / condiciones predisponentes identificadas; y la susceptibilidad que refleja las salvaguardas / contramedidas planeadas o implementadas para impedir tales eventos. TAREA 2-6: Determine el riesgo para la organización de los eventos de amenaza de preocupación, considerando: el impacto que podría resultar de los eventos; y la probabilidad de que ocurran los eventos.			
6.5 Tratamiento del riesgo	9. Tratamiento de riesgos de seguridad de la información	Seleccionar los controles que ayudaran a eliminar los riesgos	Submodelo de procesos: Gestión de riesgos Submodelo de procesos: Selección de salvaguardas	Fase de Seleccionar un enfoque de mitigación, en esta se desarrolló de estrategias y planes de seguridad.	En este literal de las tres normas se menciona el tratamiento del riesgo, con el fin de transferirlo, evitarlo, aceptarlo y reducirlo.

5.7.2 Mejora continua	12.2 Seguimiento, revisión y mejora de la gestión de riesgos	3.4 mantenimiento de la evaluación de riesgos El objetivo de este paso es mantener actualizado el conocimiento específico de las organizaciones de riesgo. Los resultados de las evaluaciones de riesgos informan las decisiones de gestión de riesgos y guían las respuestas de riesgos. TAREA 4-1: Realice un monitoreo continuo de los factores de riesgo que contribuyen a los cambios en el riesgo de las operaciones y activos de la organización, individuos, otras organizaciones o la Nación. TAREA 4-2: Actualice la evaluación de riesgos existente utilizando los resultados del monitoreo continuo de los factores de riesgo.			La mejora continua es la fase final de la norma, la cual debe mejorarse continuamente según sea la referencia de la gestión del riesgo y la continuidad del negocio, las metodologías de riesgos donde se enmarcan esta fase es ISO 31000, ISO 27005 y Nist 800-30.

Tabla C-1.: Análisis de metodologías de gestión de riesgos

D. Tabla de controles y guías del SGSI de la metodología propuestadel

Los anexos de las controles y las guías para la implementación del SGSI propuestas obtenidos por su tamaña deben ser descargados de en la siguiente URL de OneDrive:

URL: https://correoitmedu-my.sharepoint.com/:f:/g/personal/cesargonzalez249935$_{c}orreo_{i}tm_{e}du_{c}o/En-HkCGHk_{p}IvcRh_{F}cPpRIBTFfrWQ8bOO_{K}T3BmM75GjA?e = Bn4MLA$

E. Encuesta de verificación de la implementación del análisis GAP de controles existentes en la organización

El siguiente cuestionario tiene como objetivo verificar el nivel de compresibilidad y entendimiento de la herramienta de análisis GAP de Controles existentes en la organización. En este sentido es importante que su respuesta cumpla con los parámetros de objetividad ya que de dicho resultado permite retroalimentar el proceso de aplicación de la metodología de SGSI.

Nombre del cargo: Ingeniero de Proyectos
Título profesional: Ingeniero de sistemas

Escala de valoración: 1 a 5, donde (1 es totalmente en desacuerdo y 5 totalmente de acuerdo).

Nro.	Preguntas	Nivel de Valoración				
		1	2	3	4	5
1	El conjunto de definiciones contenido en la herramienta de análisis GAP de Controles existentes en la organización es comprensible y ajusta a un adecuado entendimiento.?					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						
2	La herramienta le permite la implementación del proceso del SGSI.				**X**	
Si la respuesta es igual o menor a 3 explicar por qué:						
3	La herramienta de análisis GAP de Controles existentes en la organización le facilitó la identificación de los controles existente en su organización					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						
4	La herramienta de análisis GAP de Controles existentes en la organización guía le facilito la valoración del estado cada uno de los controles implementados en la organización.					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						
5	La grafica de radar, es una herramienta útil para la toma de decisiones sobre la implementación de controles para la organización.				**X**	
Si la respuesta es igual o menor a 3 explicar por qué:						
6	La línea base declarada en la herramienta de análisis GAP de Controles existentes en la organización es útil para los propósitos del control del SGSI de su empresa.				**X**	
Si la respuesta es igual o menor a 3 explicar por qué:						
7	La herramienta de análisis GAP de Controles existentes en la organización le aporta a su conocimiento para el desarrollo de sus funciones en su cargo.					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						
8	La herramienta de análisis GAP de Controles existentes en la organización le aporta al desarrollo de la gestión de los procesos en el SGSI.					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						

Tabla E-1.: Analisis inicial GAP controles

F. Encuesta de verificación de la implementación de la guía de contextualización - alcance

El siguiente cuestionario tiene como objetivo verificar el nivel de compresibilidad y entendimiento de la Guía de contextualización - alcance. En este sentido es importante que su respuesta cumpla con los parámetros de objetividad ya que de dicho resultado permite retroalimentar el proceso de aplicación de la metodología de SGSI.

Nombre del cargo: Analista de soporte
Título profesional: Tecnólogo de redes

Escala de valoración: 1 a 5, donde (1 es totalmente en desacuerdo y 5 totalmente de acuerdo)

Nro.	Preguntas	Nivel de Valoración				
		1	2	3	4	5
1	El conjunto de definiciones contenido en la guía de contextualización - alcance es comprensible y ajusta a un adecuado entendimiento.?					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						
2	La línea base descrita en la guía de contextualización - alcance le permite su implementación en el proceso del SGSI.					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						
3	La guía de contextualización - alcance le facilitó la identificación de los controles existente en su organización					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						
4	La grafica de elipses obtenida, es una metodología útil para la toma de decisiones la descripción del alcance del SGSI.					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						
5	La metodología de elipses, le ayudo a identificar los procesos críticos de la organización					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						
6	La línea base declarada en la guía de contextualización - alcance es útil para los propósitos de la metodología propuesta del SGSI de su empresa.				**X**	
Si la respuesta es igual o menor a 3 explicar por qué:						
7	La guía de contextualización - alcance le aporta a su conocimiento para el desarrollo de sus funciones en su cargo.					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						
8	La guía de contextualización - alcance le aporta al desarrollo de la gestión de los procesos en el SGSI.					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						

Tabla F-1.: Encuesta de verificación de la implementación de la guía de contextualización - alcance

G. Encuesta de verificación de la implementación de la guía de gestión del riesgo

El siguiente cuestionario tiene como objetivo verificar el nivel de compresibilidad y entendimiento de la guía de gestión del riesgo En este sentido es importante que su respuesta cumpla con los parámetros de objetividad ya que de dicho resultado permite retroalimentar el proceso de aplicación de la metodología de SGSI.

Nombre del cargo: Ingeniero de Proyectos
Título profesional: Ingeniero de sistemas

Escala de valoración: 1 a 5, donde (1 es totalmente en desacuerdo y 5 totalmente de acuerdo).

Nro.	Preguntas	Nivel de Valoración Ingeniero					Nivel de Valoración Analista				
		1	**2**	**3**	**4**	**5**	**1**	**2**	**3**	**4**	**5**
1	El conjunto de definiciones contenido en la guía de gestión del riesgo es comprensible y ajusta a un adecuado entendimiento.?					**X**				**X**	
Si la respuesta es igual o menor a 3 explicar por qué:											
2	La línea base descrita en la guía le permite su implementación en el proceso del SGSI.					**X**					**X**
Si la respuesta es igual o menor a 3 explicar por qué:											
3	La guía de gestión del riesgo le facilitó la identificación de los controles existente en su organización					**X**				**X**	
Si la respuesta es igual o menor a 3 explicar por qué:											
4	La guía de gestión del riesgo guía le facilito la valoración del estado cada uno de los controles implementados en la organización.					**X**				**X**	
Si la respuesta es igual o menor a 3 explicar por qué:											
5	El resultado obtenido en la herramienta es útil para la toma de decisiones sobre el tratamiento de los riesgos.					**X**					**X**
Si la respuesta es igual o menor a 3 explicar por qué:											
6	La línea base declarada en la herramienta de análisis de riesgos es útil para los propósitos del control del SGSI de su empresa.					**X**				**X**	
Si la respuesta es igual o menor a 3 explicar por qué:											
7	La guía de gestión del riesgo le aporta a su conocimiento para el desarrollo de sus funciones en su cargo.					**X**					**X**
Si la respuesta es igual o menor a 3 explicar por qué:											
8	La guía de gestión del riesgo le aporta al desarrollo de la gestión de los procesos en el SGSI.					**X**					**X**
Si la respuesta es igual o menor a 3 explicar por qué:											

Tabla G-1.: Gestión del riesgo

H. Encuesta de verificación de la implementación de la guía de Política de seguridad de la información

El siguiente cuestionario tiene como objetivo verificar el nivel de compresibilidad y entendimiento de la guía de política de seguridad de la información. En este sentido es importante que su respuesta cumpla con los parámetros de objetividad ya que de dicho resultado permite retroalimentar el proceso de aplicación de la metodología de SGSI.

Nombre del cargo: Ingeniero de Proyectos
Título profesional: Ingeniero de sistemas

Escala de valoración: 1 a 5, donde (1 es totalmente en desacuerdo y 5 totalmente de acuerdo)

Nro.	Preguntas	Nivel de Valoración				
		1	2	3	4	5
1	El conjunto de definiciones contenido en la guía de guía de Política de seguridad de la información es comprensible y ajusta a un adecuado entendimiento.?					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						
2	La línea base descrita en la guía de Política de seguridad de la información le permite su implementación en el proceso del SGSI.					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						
3	La guía de Política de seguridad de la información le facilitó la identificación de los componentes de la política como (alcance, aspectos legales y nivel de cumplimiento en organización.					**X**
Si la respuesta es igual o menor a 3 explicar por qué: A pesar de que la guía aporta componentes para relevantes es necesario ajustar los mismos al contexto del negocio.						
4	La política propuesta en la guía se acopla a las necesidades de su SGSI en implementación.					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						
5	Considera que la Política de seguridad de la información resulto de fácil entendimiento para las partes interesadas en la empresa.					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						
6	La línea base declarada en la guía de Política de seguridad de la información es útil para los propósitos de la metodología propuesta del SGSI de su empresa.					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						
7	La guía de guía de Política de seguridad de la información le aporta a su conocimiento para el desarrollo de sus funciones en su cargo.					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						
8	La guía de guía de Política de seguridad de la información le aporta al desarrollo de la gestión de los procesos en el SGSI.					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						

Tabla H-1.: Política general de seguridad de la información

I. Encuesta de verificación de la implementación de la guía de política de seguridad de la información operacional

El siguiente cuestionario tiene como objetivo verificar el nivel de compresibilidad y entendimiento de la guía de política de seguridad de la información operacional. En este sentido es importante que su respuesta cumpla con los parámetros de objetividad ya que de dicho resultado permite retroalimentar el proceso de aplicación de la metodología de SGSI.

Nombre del cargo: Ingeniero de Proyectos
Título profesional: Ingeniero de sistemas

Escala de valoración: 1 a 5, donde (1 es totalmente en desacuerdo y 5 totalmente de acuerdo)

Nro.	Preguntas	Nivel de Valoración				
		1	2	3	4	5
1	El conjunto de definiciones contenido en la guía de guía de Política de seguridad de la información Operacional es comprensible y ajusta a un adecuado entendimiento.?					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						
2	La línea base descrita en la guía de Política de seguridad de la información Operacional le permite su implementación en el proceso del SGSI.					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						
3	La guía de Política de seguridad de la información Operacional le facilitó la identificación de los componentes operacionales en su infraestructura para proteger sus activos de información.					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						
4	La política propuesta en la guía se acopla a las necesidades de su SGSI en implementación.					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						
5	Considera que la Política de seguridad de la información Operacional resulto de fácil entendimiento para las partes interesadas en la empresa.					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						
6	La línea base declarada en la guía de Política de seguridad de la información Operacional es útil para los propósitos de la metodología propuesta del SGSI de su empresa.					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						
7	La guía de guía de Política de seguridad de la información Operacional le aporta a su conocimiento para el desarrollo de sus funciones en su cargo.					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						
8	La guía de guía de Política de seguridad de la información Operacional le aporta al desarrollo de la gestión de los procesos en el SGSI.					**X**
Si la respuesta es igual o menor a 3 explicar por qué:						

Tabla I-1.: Política operacional de seguridad de la información

J. Encuesta de verificación de la implementación de la metodología de SGSI para Pymes del sector de la información y comunicaciones de la ciudad de Medellín

El siguiente cuestionario tiene como objetivo verificar la factibilidad e implementación de la metodología de SGSI para Pymes del sector de la información y comunicaciones de la ciudad de Medellín. En este sentido es importante que su respuesta cumpla con los parámetros de objetividad ya que los resultados permitirán retroalimentar a los proponentes para realizar mejoras a la metodología propuesta.

Nombre del cargo: Ingeniero de Proyectos
Título profesional: Ingeniero de sistemas

Escala de valoración: 1 a 5, donde 1 es totalmente en desacuerdo con la afirmación y 5 totalmente de acuerdo con esta.

Nro.	Preguntas	Nivel de Valoración Ingeniero					Nivel de Valoración Analista				
		1	2	3	4	5	1	2	3	4	5
1	Los componentes de la metodología propuesta para el SGSI están claramente definidos y son comprensibles para personal técnico no especializado.					**X**					
Si la respuesta es igual o menor a 3 explicar por qué:											
2	Las guías desarrolladas para la metodología propuesta facilitan la implementación de un SGSI en empresas Pyme del sector de la información y las comunicaciones.					**X**					
Si la respuesta es igual o menor a 3 explicar por qué:											
3	La metodología de SGSI propuesta facilita la identificación de los componentes del sistema, como riesgos, políticas y controles, que permiten proteger los activos de información.				**X**						
Si la respuesta es igual o menor a 3 explicar por qué:											
4	La metodología propuesta reduce la necesidad de contar con personal especializado y con formación específica para la implementación de un SGSI				**X**						
Si la respuesta es igual o menor a 3 explicar por qué:											
5	La metodología propuesta reduce el tiempo de implementación de un SGSI, con respecto a otras metodologías existentes en la industria.					**X**					
Si la respuesta es igual o menor a 3 explicar por qué:											
6	La metodología propuesta reduce el costo de implementación de un SGSI, con respecto a otras metodologías existentes en la industria.					**X**					
Si la respuesta es igual o menor a 3 explicar por qué:											
7	La metodología propuesta cumple con los Principios Institucionales de Seguridad de la Información, como Integridad, confidencialidad y disponibilidad					**X**					
Si la respuesta es igual o menor a 3 explicar por qué:											

8	La Metodología de SGSI propuesta le aporta a su conocimiento para el desarrollo de las funciones de su cargo.					**X**					
Si la respuesta es igual o menor a 3 explicar por qué:											
9	La implementación del SGSI, siguiendo la metodología propuesta, contribuye a los requerimientos de gestión de seguridad de la información de sus clientes				**X**						
Si la respuesta es igual o menor a 3 explicar por qué:											
10	Como resultado de la participación en la implementación de esta metodología: ¿Cuáles son los aspectos a mejorar y las ventajas que ofrece la implementación del SGSI en las empresas PYMEs del sector de la información y las comunicaciones de Medellín?										
Ventajas: (Ingeniero) - Permite a las empresas la adopción de la seguridad de la información a sus activos core del negocio. - Reduce costos en proyectos relacionados a implementación de SGSI. - Proporciona mecanismos para generar sensibilidad y conciencia en los colaboradores de las compañías sobre la seguridad de la información. - Genera consciencia a la alta dirección sobre los riesgos a los que están sujetos los activos de información. - Permite ser proactivos ante la resolución de incidentes relacionados con la seguridad de la información. Ventajas: (Analista) - Con la metodología empleada logre apreciar, conocer y profundizar sobre temas que no conocía o manejaba en mis labores, como a tener en cuenta el nivel de importancia que tiene la información con la que interactúo diariamente, riesgos y amenazas sobre esta. La identificación de dichos riesgos y amenazas de una manera sencilla y cómoda. Aspectos a Mejorar: (Ingeniero) - La guía relacionada a la gestión de riesgos podría tener un enfoque que simplifique la metodología global para la gestión de los riesgos.											

Tabla J-1.: Evolución metodología propuesta