Diseño de una propuesta metodológica para la implementación de Sistemas de Gestión de Seguridad en Collective Mining Limited Sucursal Colombia

Felipe Alberto Murillo Rodríguez

Universidad de Manizales
Facultad de Ciencias e Ingeniería
Maestría en Seguridad de la Información
Manizales
2022

Diseño de una propuesta metodológica para la implementación de Sistemas de Gestión de Seguridad en Collective Mining Limited Sucursal Colombia

Felipe Alberto Murillo Rodríguez

Propuesta de trabajo de grado presentado como requisito parcial para optar al título de Magíster en Seguridad de la Información

Director:
Ing.

Línea de Investigación:
Gestión de la Seguridad de la Información en las Organizaciones
Grupo de Investigación y Desarrollo en Informática y Telecomunicaciones

Universidad de Manizales
Facultad de Ciencias e Ingeniería
Maestría en Seguridad de la Información
Manizales, 2022

Contenido

Pág.

Resumen

La información en esta nueva era tecnológica en Colombia ha adquirido un gran valor para las organizaciones, hasta el punto de convertirse en un activo más para las empresas pequeñas en el país (PYMES), generando la necesidad legal y organizacional de mantenerla segura por medio de los tres pilares, Confidencialidad, Integridad y disponibilidad. Para solucionar esta necesidad, existen componentes y lineamientos basados en la norma ISO 27001 los cuales plantean como objetivos diseñar, ejecutar, monitorear y controlar un sistema de gestión de seguridad de la información.

El presente proyecto tiene como objetivo el diseño de una propuesta metodológica para la implementación de Sistemas de Gestión de Seguridad de la Información en empresas pequeñas en el país, alineado con la familia de normas de la ISO 27000, para esto se determinarán los requerimientos mínimos de seguridad para las empresas pequeñas en Colombia, se analizaran los modelos actuales que se están utilizando para las pymes en Colombia, finalizando con una propuesta metodológica y validando en al menos 2 pymes en Colombia.

Palabras Clave: Sistemas, Información, Seguridad, Modelos, Metodología, Tecnología, PYMES, Colombia.

Abstract

Information in this new technological era in Colombia has acquired excellent value for organizations, to the point of becoming another asset for small companies in the country (SMEs), generating the legal and organizational need to keep it safe through the three pillars, Confidentiality, Integrity, and availability. To solve this need, there are components and guidelines based on the ISO 27001 standard which propose as objectives to design, execute, monitor, and control an information security management system. This project aims to design a methodological proposal for the implementation of Information Security Management Systems in small companies in the country, aligned with the ISO 27000 family of standards, for this the minimum-security requirements for small companies in Colombia will be determined, the current models that are being used for SMEs in Colombia will be analyzed, ending with a methodological proposal, and validating in at least 2 SMEs in Colombia.

Keywords: Systems, Information, Security, Models, Methodology, Technology, SMEs, Colombia.

Lista de Figuras

Pág.

Lista de Tablas

Pág.

Introducción

En Colombia, la información se muestra cada vez más importante en las empresas hasta el punto de llegar a ser un activo más para estas, por ello el interés de mantener y sostener los datos en el tiempo de una manera segura, para luego ser consultada, transformada y manipulada a las necesidades de las entidades, dicho lo anterior y ajustándose a la actualidad, las TIC empieza a jugar un papel importante, permitiendo implementar y trabar los datos de forma digital (sistemas de información), esto con el fin de simplificar la búsqueda y encontrarla de manera rápida y fiable.

Bajo este contexto, partiendo de lo mayúsculo que es la información para las empresas y el manejo de ésta en los sistemas de información, se encuentra a ella ligada los riesgos y las amenazas, llamadas vulnerabilidades informáticas que por desgracia están presentes todo el tiempo, en Colombia para evitar y contrarrestar los inconvenientes, se comienzan a implementar normas, reglas e instructivos que por medio de modelos gubernamentales y privados permiten asegurar un plan de prevención y en su defecto de contingencia que Logran contrarrestar intrusiones no permitidas.

Es inevitable decir, que en Colombia está creciendo el entorno digital para promover el manejo de la información por medio de políticas y modelos ya conocidos como gobierno en línea, CONPES, otras internacionales como la ISO 27001, MAGERT entre otros, pero al pasar de los días se hace más evidente que no es suficiente y que la implementación de las mismas no está orientada a las PYMES ya que el costo económico y tiempo es alto y dichas entidades no están dispuestas a pagar un precio tan alto por falta de presupuesto.

Por ello, se hace preciso generar una nueva idea (Modelo) que permita interactuar de manera directa, activa y permanente con el modelo socioeconómico de las entidades pequeñas y que no se desvíe totalmente de lo que buscan los modelos conocidos con efectividad evidente, pero buscando un bajo costo en tiempo y dinero.

Por lo tanto, con los avances hechos en el mundo y principalmente en Colombia, las tecnologías de la información y comunicación TIC, la información se ha convertido en un componente primordial de las relaciones sociales y de la economía en sí misma, motivo por el cual se han transformado en un valor agregado de las compañías modernas, teniendo en cuenta que la información es una importante moneda del milenio. El valor monetario de esta clase de información es grande y sigue creciendo [1].

Así, con la transformación digital que está viviendo el país se hace necesario la implementación de una metodología que puedan garantizar la integridad de la información obtenida por las empresas y esta política de tratamiento de información ayuda a proteger los datos sensibles que se entreguen en las diversas unidades organizacionales.

Para diseñar dicha metodología, se propone automatizar procesos para reducir tiempo y costes, pero adicional a ello tenga un constante reporteo hacia personal calificado (ingeniero de sistemas) para que se mantenga una línea de conocimiento y observación de los posibles problemas a tener o encontrados todo con el enfoque de gestión de riesgos que sugiere los ya mencionados modelos. De esta forma, se podrá tener una empresa segura con los mínimos estándares posible, sacrificando un poco la precisión de metodologías más robustas pero que a la larga mantendrá la filosofía de la seguridad de la información confidencialidad, integridad, disponibilidad y autenticación.

1. Planteamiento del Problema de Investigación y su Justificación

La seguridad de la información es un concepto integral de cómo salvaguardar de forma confidencial y organizada los datos de una entidad, cumpliendo unos lineamientos o modelos que permita planear, implementar, operar, monitorear y mantener la operación de las empresas de manera eficaz y eficiente.

Dentro de este contexto, la organizaciones pequeñas siempre han tenido su labor basada en las actividades, tareas y objetivos diarios las cuales se han venido complejizando de la misma forma que crece la preocupación de mantener y sostener la información, que permita hacer un trabajo confiable, rápido y seguro, para ello se hace necesario implementar modelos y estándares que se hacen costosos y complejos donde comprometen o condicionan el tamaño y el presupuesto de las entidades, adicional a ello el comportamiento, la cultura digital y organizacional de los usuarios es distinta a la que subyace las grandes entidades.

1.1. Descripción del Área Problemática

Según la World Economic Forum, existe una reciprocidad continua entre inversión en digitalización y PIB de una economía, en un acrecentamiento del 10% en la digitalización de una nación, lo cual produce un aumento del 0,75% en el PIB per cápita y un declive del 1,02% en la tasa de paro [2].

Igualmente, para la Unión Europea, la inversión en procesos TIC es fundamental para que Europa conserve el enfoque de liderazgo en ventaja competitiva, a través de disminución de costos y el alza en la creación, logrando la producción de empleo sólido y competente. Aunado a lo anterior, se debe señalar que hoy por hoy en una economía

globalizada, donde las naciones en desarrollo progresen de una manera rápida y por encima de la del viejo continente [3].

En Europa, las TICS contribuirán en un 2,5 billones de euros a la economía para el año 2025, lo que constituye un 10% sobre las perspectivas de desarrollo hoy por hoy, según investigaciones. Ahora bien, según la Unión Europea para lograr estas metas, señala unas sugerencias, las cuales van encaminadas activar la utilización del Big Data, crear aplicaciones digitales con ventajas competitivas definidas, capacitar a los profesionales en temas digitales, así como incentivar a la sociedad como promotores de seguridad de la información en las empresas, para que logren trasmitir este cambio cultural a la sociedad [3].

Según la Comisión Europea, tan solo el 16% de las Pymes europeas hacen uso de internet como fuente de distribución, ahora bien, de este 16%, menos de la mitad ofrecen sus servicios o productos por fuera de su nación. Por otra parte, los europeos no tienen un nivel de competitividad digital, siendo esto fundamental para la seguridad de la información digital, ya que las personas son el componente más relevante en dicha transformación. Así, el 45% de la ciudadanía no posee una cultura digital básica [3].

En el ámbito colombiano, es el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) basado en la familia de normas ISO 27000, que toman los elementos en los que se debe enfocar y gestionar los métodos que contienen la herramienta estratégica usada para analizar las actividades de las MIPYMES y lograr detectar sus fuentes de ventaja competitiva, como por ejemplo su fase de seguridad de la información.

Dentro de este contexto, existe resistencia en muchas MIPYMES colombianas para utilizar los procesos relacionados a transformación digital basada en la protección de la

información, por lo que se puede inferir que esta resistencia puede estar incidiendo en el nivel de competitividad de dichas organizaciones. A raíz de estos síntomas, se puede inferir que el problema puede radicar en la existencia de diversos factores de resistencia que inciden en la adopción de procesos de seguridad de datos en las MIPYMES de Colombia.

En primer lugar, se encuentra la obtención de los recursos financieros, los cuales se agudizan más teniendo en cuenta el volumen de la empresa, porque cuando es menor la empresa es más la posibilidad de tener conflictos en consentir dichos recursos, esto acarrea que no se pueda llevar a cabo diversos planes y negocios [4].

Igualmente, se encuentra el tiempo o retraso en la implementación de la seguridad de la información; se va dando paulatinamente a la medida en que las empresas vean la necesidad, el sector lo solicite, la empresa se arriesgue a hacer uso de ella, o por nuevas líneas de mercado, servicio o productos hagan que la misma llegue a ser parte del proceso de la empresa [4]. El autor, también hace hincapié en la incidencia de factores externos, tres elementos en los que se debe avanzar en la seguridad y tratamiento de la información como son: en las organizaciones, en el sector público y en la población; estos tres elementos o actores, siempre actúan y se encuentran en un punto de ventaja competitiva para un bien común.

Consecuentemente, la seguridad y privacidad de la información al no ocurrir en la misma fase en todos los departamentos al interior de las organizaciones medianas o pequeñas, en muchos casos es más lento ese acompañamiento al cambio cultural y evolución de la empresa, haciendo en muchas ocasiones que sea único y adecuado para cada entidad dependiendo donde se quiera implementar; lo que sí es transversal a ese

proceso es ese vínculo con el cliente, ya que los procedimientos que surgen al interior de la empresa o áreas y el mismo bien, servicio o producto son digitales.

De la misma forma, se encuentra la resistencia al cambio; la seguridad y protección de los datos implica analizar todos los canales de contacto con el usuario o cliente, lo que lleva a que se tenga que reevaluar el rediseño de los métodos, procedimiento, equipo de trabajo y hasta la cultura organizacional de la empresa u organización, con el fin de perfilar al cliente objetivo [5].

De la misma manera, el autor enfatiza que, en muchos sectores o industrias del mercado, la implementación de una metodología de seguridad y privacidad de la información es dispersa o alterada, por tal razón se pone de presente que ésta no puede servir de modelo para todas las empresas MiPymes, pero si se puede traer a colación conceptos claves que surgen al momento de su implementación en las organizaciones pero que no son procesos lineales para todos los sectores.

Del mismo modo, según la Asociación de Empresas de Electrónica, Tecnologías de la Información, Telecomunicaciones y Contenidos Digitales [3], inciden algunos factores internos de la empresa, entre ellas el riesgo del tema de la capacitación digital, contando con que el 46% de la población no cuenta con aptitudes y habilidades digitales elementales, así como el elemento de la reglamentación legal, la cual deberá tener armonía con lo que se pretende desarrollar o implementar. A raíz de estos síntomas, se puede inferir que el problema puede radicar en la existencia de factores de resistencia que inciden en la adopción de procesos de seguridad de la información digital de las MiPymes en Colombia.

Así, es de suma importancia reconocer que la seguridad en la información digital de las MiPymes, es relevante la utilización de las TICS para lograr cambios que puedan

volverse ventajas competitivas al modelo de negocio, sin desconocer que al ir a esa transformación tan acelerada puede ocurrir que el factor que era ventaja competitiva se convierta en una necesidad para permanecer en el mercado [5].

Por lo tanto, de continuar la situación planteada puede traer como consecuencia el no aprovechamiento de las ventajas de la implementación de un modelo de seguridad de la información, lo que puede repercutir en la ventaja competitiva de las empresa objeto de estudio, por lo que se puede pronosticar que un futuro dicha organización no logre cumplir con eficacia los objetivos que se encuentran propuestos y pueda arriesgar en el futuro inmediato los datos empresariales, que puede afectar la permanencia de la compañía en el ámbito regional y nacional.

En síntesis, mediante la presente investigación se aspira diseñar el Sistema de Gestión de Seguridad y Privacidad de la Información de la multinacional Collective Mining, basado en el modelo MSPI del Ministerio de Tecnologías de la Información y Comunicaciones y dando cumplimiento a la familia de normas ISO 27000, además de encontrar respuesta a la pregunta de la investigación y a los objetivos planteados.

1.2. Formulación del Problema

A partir de lo anteriormente expuesto, el interrogante que busca responder el presente proyecto es: ¿Cuál es la propuesta metodológica para la implementación de Sistemas de Gestión de Seguridad en pymes en Colombia?

1.3. Justificación

El propósito principal del presente trabajo fue diseñar el Sistema de Gestión de Seguridad y Privacidad de la Información de la multinacional Collective Mining, basado en el modelo MSPI del Ministerio de Tecnologías de la Información y Comunicaciones y

dando cumplimiento a la familia de normas ISO 27000. Al respecto, el proyecto resulta relevante ya que las pymes modernas en Colombia deben evolucionar al paso de las tecnologías de la información y las comunicaciones (TIC), sino están tendiendo al fracaso.

De este modo, entre los avances que han implementado se encuentran los sistemas de información los cuales alojan y permiten el manejo de la información crítica, importante y confidencial de estas, por ello han venido siendo objeto de delincuentes informáticos que quieren usufructuar de los datos allí contenidos, sin embargo el cuidado y la importancia parece ser que no es la suficiente ya que estas creen que con un simple Firewall o un antivirus suplen las deficiencias de la seguridad informática. Consecuentemente, es necesario diseñar propuestas metodológicas para la implementación de SGSI que alcancen objetivos exitosos y logren como beneficio la seguridad de la información esperada por las políticas de la empresa.

De tal manera, es necesario que las empresas pequeñas se comporten diferente a las grandes y por lo cual se tiene diferentes necesidades tecnológicas y los modelos actuales no cumplen para las expectativas de las empresas pequeñas. Por ende, se propone este proyecto de investigación (Diseño de una propuesta metodológica para la implementación de sistemas de gestión de seguridad en PYMES. Caso Colombia) para suplir las necesidades socioeconómicas, culturales y de conocimiento para el manejo y tratamiento de los datos e información en pro de aumentar el nivel de la seguridad informática con bajo coste, en poco tiempo y con una aceptable satisfacción de cliente.

Consecuentemente, al tener conocimiento de las características que se están implementando en materia de seguridad informática en estas entidades, es más probable

que se encuentre un modelo que alcance las expectativas y de solución a las carencias de seguridad informática y cumpla las expectativas de estas empresas.

Así mismo, el tener una política de seguridad de la información en la empresa ayudará a tener una guía para la protección de los datos como activo fundamental, evitando la pérdida, el fraude y demás delitos que puedan incurrir las personas por mal uso de la información, por otro lado, ayuda a los gerentes a ser garantes de salvaguardar la información que se almacena en la organización.

Por lo tanto, la importancia de una política de tratamientos de datos en la empresa radica en minimizar el riesgo de pérdida de información obtenida, por lo que la compañía debe ser garante en cumplir con diversas normativas como el Decreto 1078 de 2015 la ISO 27000 [6], pues el buen uso de la información recolectada ayudará a que los datos sensibles sean tratados con el fin en que se brindaron.

Finalmente, en el campo metodológico y de acuerdo con su importancia, el estudio puede contribuir con el análisis del tema para su profundización en calidad de antecedentes, y/o apoyar en la consulta de otras investigaciones que se formulen a futuro en el ámbito de esta misma temática, de acuerdo con su importancia dentro de la temática abordada.

2. Objetivos

2.1. Objetivo General

Diseñar el Sistema de Gestión de Seguridad y Privacidad de la Información de la multinacional Collective Mining, basado en el modelo MSPI del Ministerio de Tecnologías de la Información y Comunicaciones y dando cumplimiento a la familia de normas ISO 27000.

2.2. Objetivos Específicos

- Determinar el estado de cumplimiento del sistema de gestión de seguridad de la información y determinar la brecha y las acciones de cumplimiento para asegurar la información de la organización.
- Construir la planeación del sistema de gestión de seguridad conteniendo el alcance, la política de seguridad de la información, el inventario de activos, la evaluación de riesgos con su metodología, identificación y análisis; y llegando a la determinación de los controles.
- Desplegar el sistema de seguridad de la información, por medio de un plan de tratamiento de riesgos y la implementación de los controles que mitiguen los riesgos altos.

3. Antecedentes

La seguridad de la información tiene un papel importante en las organizaciones, se requiere de un estándar que determine las mejores prácticas a nivel internacional en materia de SGSI.

Actualmente existen diversos estándares para el gobierno y gestión de TI que contemplan como parte de sus prácticas la seguridad de la información, entre las que se destacan: PRINCE2, OPM3, CMMI, P-CMM, PMMM, familia de normas ISO/IEC 27000, PCIDSS, COSO, SOA, ITIL y COBIT.

Partiendo de lo dicho, un grupo de estudiantes de la Universidad de Brunei [7], realizaron un estudio comparativo de los cinco grandes normas del sistema de gestión de seguridad de la información ISO 27001, BS 7799, PCIDSS, ITIL y COBIT, cada estándar juega su propio rol y posición en la implementación de sistemas de gestión de seguridad de la información, los estándares ISO/IEC 27001 y BS 7799 se centran en el sistema de gestión de seguridad de la información como dominio principal, mientras que PCIDSS se enfoca en la seguridad de la información relacionada con las transacciones comerciales y tarjetas inteligentes.

Por otra parte, ITIL y COBIT se centran en la seguridad de la información y su relación con la gestión de proyectos y el gobierno de TI. El estándar ISO 27001 lidera las otras cuatro normas ya que es implementado más fácilmente y es muy reconocido por las partes interesadas (alta gerencia, personal, proveedores, clientes), además tiene un nivel de usabilidad y confianza de más del 80% en el mundo, de acuerdo con el estudio en mención [7].

Así, como conclusión del trabajo, siendo la gestión del riesgo el insumo esencial para la implementación de un adecuado sistema de gestión de seguridad de la información, existen diversas metodologías de análisis y gestión de riesgos que han sido desarrolladas y aplicadas por la comunidad académica y profesional [7].

Igualmente, Tejena-Macias [8] elaboró un trabajo en donde recomienda la metodología MAGERIT por brindar un mayor cubrimiento del riesgo, en la medida que contempla un análisis de riesgos más detallado, protegiendo los datos en los tres principios de seguridad de la información: integridad, disponibilidad, confidencialidad, con algunos aspectos adicionales como su confiabilidad y que no permite arbitrariedades del analista.

Así mismo, Schwab [9] argumenta en su trabajo que no es suficiente gestionar el riesgo de seguridad de la información solo con la norma ISO 27005, es necesario apoyarse en otras metodologías para el análisis y gestión del riesgo, como por ejemplo OCTAVE-s, ya que la norma ISO 27005 solo describe los pasos que se deben seguir para la gestión del riesgo, pero no explica las actividades que se deben llevar a cabo específicamente, lo que OCTAVE-s si determina.

Del mismo modo, Benavides Carranza [10] revisa a profundidad cada una de las guías del Modelo de Seguridad y Privacidad de la Información (MPSI) e identifica que las directrices, dominios y controles establecidos en la Norma Técnica Colombiana ISO/IEC 27001 se encuentran adoptadas cien por ciento con el Modelo de Seguridad y Privacidad de la Información. Este marco metodológico contribuye a una mayor adaptación de la norma en la creación y desarrollo de un sistema de gestión de seguridad de la información. Este modelo está siendo implementado por las entidades gubernamentales, pero dado su

integración con la Norma Técnica Colombiana NTC ISO 27001 puede ser implementado por empresas del sector privado.

Así mismo, Argüello [11] presentó una investigación titulada “Análisis de la seguridad de los datos en Madecentro Colombia SA”. Este trabajo tuvo como objetivo diseñar un sistema de gestión de datos e información y lograr así un mejoramiento en el proceso de la seguridad de datos de la empresa, garantizar niveles óptimos de confiabilidad y veracidad en la información de la comercializadora.

Sobre este aspecto, el informe expuso inicialmente una descripción de los conceptos de gestión de información e indicadores de control, fundamentados en la clasificación de información según los diferentes tipos de datos y haciendo uso de material actualizado sobre el tema. Así, se planteó el estudio enmarcado en una investigación descriptiva con diseño de campo no experimental.

En resumen, el autor concluyó que existen fallas notorias en la seguridad de los subsistemas de información y seguridad por lo que se recomendó diseñar un sistema en dicha comercializadora y lograr así un mejoramiento en la gestión de datos; del mismo modo, el aporte que provee esta investigación es facilitar el desarrollo de un modelo ya que sirve como ejemplo el cual hace posible la ejecución de una investigación con categoría de trabajo de grado.

Del mismo modo, Pereira [12] realizó una tesis cuyo objetivo general estuvo centrado en diseñar un modelo de referencia para el dimensionamiento de riesgos operacionales en el tratamiento de datos de una empresa MiPyme colombiana; para lo cual un modelo funcional de aplicación empresarial que permite dimensionar los riesgos implícitos en los procesos operacionales en la gestión de datos identificando y gerenciando

IT. Information Tecnologies Tecnologías de la información.

los riesgos asociados en las operaciones empresariales, con el levantamiento de datos en la fuente e integrando los resultados obtenidos mediante procesos de conocimiento enmarcados en los conceptos de seguridad de información, de forma que se agregue valor a los procesos intraempresariales en la aeronáutica privada de Colombia.

Partiendo del estudio del funcionamiento de la gestión de datos, el resultado final de este estudio presenta un modelo aplicado para las Empresas pequeñas y medianas del sector privado, donde se puede detectar y administrar los riesgos en la seguridad e la información, así como unas recomendaciones alrededor de los procesos gerenciales y operativos que deben estar presentes en toda gestión de datos; constituyendo así un importante aporte para el estudio en curso.

Bajo esta misma perspectiva, Álvarez [13] realizó una investigación cuyo propósito fue analizar el sistema de control de seguridad basado en el informe COSO para la gestión de la protección de datos en la policía de Bucaramanga. Este trabajo se basó en un estudio de campo, no experimental, con apoyo bibliográfico. Se tomó como población las cinco (5) personas que pertenecen a la división administrativo/contable, en este sentido la muestra quedó conformada por el total de la población.

Igualmente, como técnicas, se seleccionaron la entrevista, la encuesta y la observación directa, aplicando el cuestionario, previamente los datos fueron organizados y tabulados, para su posterior tratamiento estadístico, de lo cual se detectó como conclusión la necesidad de establecer un sistema de control de seguridad basado en el informe COSO para el área de inventario y producción de las fuerzas policiales, implementando los cinco elementos que componen el mismo y así poder detectar en el momento preciso cualquier irregularidad o error en la seguridad del inventario y los registros productivos. En analogía

con la presente investigación, la relación está basada en que ambas indagan sobre lineamientos gerenciales de control que ayudan a salvaguardar la información de una organización.

Siguiendo este orden de ideas, Ceballos (14) apunta a un estudio "Diseño de un Sistema de Control de la información para Empresas Ferreteras del Departamento del Valle del Cauca". La citada investigación tuvo como objetivo general diseñar un sistema de control de gestión a las empresas ferreteras de dicho Departamento, por ello, se planteó una investigación descriptiva con diseño de campo no experimental; como instrumento de recolección de datos se aplicó un cuestionario con un total de diecisiete (17) preguntas que dieron respuesta a las interrogantes de la investigación y a las variables.

En efecto, los datos recolectados fueron plasmados mediante la construcción de tablas y gráficos utilizando estadística descriptiva. Una vez presentados y analizados los resultados, se observó como conclusión la necesidad de profundizar los controles y adoptar procesos que ayuden a garantizar la custodia del material por ser éste el más extenso de los activos. Para esto, la gerencia necesita información oportuna y enfocar su atención sobre todas las áreas críticas identificadas. Así, el aporte para la presente investigación, es que ambas se enfocan en diseñar una mejora para evitar el riesgo en el tratamiento de la información en entidades privadas.

En esta misma perspectiva, Perea y Sánchez [15], elaboraron un artículo cuyo objetivo principal fue el diseño de un modelo de transferencia de la metodología de referencia de operaciones para la gestión de la información de la Fuerza Aérea Colombiana. Así, la investigación se basó a través de cuatro fases metodológicas: análisis preliminar, diagnóstico situacional, desarrollo y cierre; las cuales permitieron diseñar una propuesta

conforme a las necesidades de la organización para el desarrollo de las operaciones aéreas en todo el territorio nacional.

Seguidamente, se presenta el trabajo de Puello Rincón [16], en donde realizó una investigación enfocada el tratamiento de la información en empresas privadas; así, aborda de manera novedosa el análisis del nivel de protección presente en las herramientas creadas para proteger al uso indebido de datos personales por medio de nuevas tecnologías de la información y las comunicaciones en Colombia.

Después de la identificación del proyecto, la formulación del problema a tratar y los objetivos a cumplir, se expuso el marco referencial, compuesto por el antecedente teórico encontrado en investigaciones previas que han indagado acerca de los mecanismos de protección de datos personales.

De acuerdo a los resultados obtenidos, se concluyó que la propuesta de gestión para empresas privadas en su proceso de tratamiento de información, permitió establecer claramente cuáles son los procesos que se manejan a nivel del tratamiento de datos, así como establecer unos indicadores de gestión claros con unas mediciones que permita hacer seguimiento al desempeño en el control de la información.

Así mismo, la exploración de estudios previos permitió encontrar similitudes en diversos estudios que proponen también un modelo de protección de datos, e igualmente enriqueció el trabajo al señalarse diferencias, limitaciones y diferentes teorías de variados autores; mismos que serán de provecho a lo largo del desarrollo de los objetivos. En síntesis, el estudio señalado guarda relación con el propio ya que busca mediante el uso de técnicas y métodos reconocidos la optimización de la gestión de la información en empresas del sector privado.

4. Referente Normativo y Legal

4.1. Marco Regulatorio

En el marco legal se presentan las leyes y normas que rigen la seguridad de la información en Colombia, lo cual se describe en las siguientes líneas.

4.1.1. Constitución Política de 1991

Con respecto al artículo 15: todos los individuos tienen derecho a su privacidad personal y familiar y a su buen nombre, y el Estado debe respetarlos. De la misma manera, tienen derecho a saber, renovar y corregir los datos que se hayan recolectado inherente a éstas en las bases de datos y en archivos de organismos públicos y privados. En la reunión, tratamiento y circulación de información se respetarán la libertad y otras garantías que consagre la Carta Magna [17].

De tal manera, solamente puede ser obstaculizado o realizado su registro a través de orden judicial, en los casos y con los formulismos que normalice el estatuto. Con la finalidad de advertir la comisión de hechos terroristas, una regla estatutaria normalizará forma y circunstancias en que las autoridades que ella indique, con basamento en importantes motivos, puedan interceptar o registrar la correspondencia y otros formatos de comunicación privada, sin precedente orden judicial, con aviso contiguo a la Procuraduría General de la Nación y control judicial siguiente dentro de las treinta y seis (36) horas sucesivas [17].

4.1.2. Decreto 1078 de 2015 Sector de Tecnologías de la Información y las Comunicaciones

El Decreto 1078 de 2015, tiene como finalidad principal fortalecer la gobernanza digital, la identificación de infraestructuras cibernéticas críticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital. De tal manera, las

personas jurídicas de derecho privado que presten servicios de gestión de infraestructuras cibernéticas críticas o la prestación de servicios esenciales podrán aplicar las disposiciones de este decreto si no son contrarias a su naturaleza o a los requisitos que regulan su actividad o servicio [18].

En este sentido, este Decreto establece que la gobernanza de la seguridad digital se basará en los principios generales de la función administrativa, las TIC, el procedimiento administrativo, el tratamiento de datos personales y la política de Gobierno Digital. Asimismo, introduce como principios particulares los siguientes: Confianza, Coordinación, Colaboración de múltiples partes interesadas, Cooperación, Enfoque basado en la gestión de riesgos, Inclusión, proporcionalidad, Salvaguardar los derechos humanos y los valores fundamentales de los ciudadanos, Uso eficiente de la infraestructura y los recursos para proteger la infraestructura cibernética crítica y los servicios esenciales [18].

Así, la norma establece un modelo de gobernanza de la seguridad digital, cuyos lineamientos y estándares serán definidos por el Ministerio TIC para fortalecer la seguridad digital, la protección de redes, infraestructuras críticas, servicios esenciales y sistemas de información en el Ciberespacio. La Coordinación Nacional de Seguridad Digital, el Comité Nacional de Seguridad Digital, las Mesas de Trabajo de Seguridad Digital, las Mesas de Trabajo de Seguridad Digital y los Puestos de Mando Unificados de Seguridad Digital implementarán el modelo de acuerdo a las funciones establecidas en el decreto.

4.1.3. Normas ISO 27000

La familia de estándares ISO/IEC 27000, también conocida como la familia de estándares ISMS o, más simplemente, ISO27K, cubre una amplia gama de estándares de

seguridad de la información publicados tanto por la Organización Internacional de Normalización como por la Comisión Electrotécnica Internacional. ISO 27000 recomienda las mejores prácticas para gestionar los riesgos de la información mediante la implementación de controles de seguridad, dentro del marco de un Sistema de gestión de la seguridad de la información (SGSI) general [6].

Así, es muy similar a los sistemas de gestión estándar, como los de garantía de calidad y protección del medio ambiente. ISO/IEC amplió deliberadamente el alcance de la serie ISO 27000 para que también cubra cuestiones de seguridad, privacidad y TI. las organizaciones de todas las formas y tamaños pueden beneficiarse de ella. Los controles de seguridad de la información deben adaptarse a las necesidades de cada organización para que puedan tratar los riesgos como lo consideren apropiado [6].

De tal manera, las organizaciones deben confiar en la orientación y las sugerencias de seguridad cuando corresponda. Dado que la seguridad de la información y la gestión de riesgos son disciplinas dinámicas, el concepto ISMS incorpora retroalimentación y mejoras continuas para responder a los cambios en las amenazas o vulnerabilidades que ocurrieron como resultado de los incidentes. Los expertos en seguridad de la información sugieren que el cumplimiento de la serie ISO 27000 es el primer paso hacia un programa de seguridad de la información que protegerá adecuadamente a la empresa.

Consecuentemente, los estándares, sin embargo, no son específicos de ninguna industria y esto hace que puedan aplicarse en cualquier negocio, independientemente del tamaño y la industria. La estandarización es un producto de ISO/IEC JTC1 SC27, un organismo internacional que se reúne formalmente dos veces al año.

IT. Information Tecnologies Tecnologías de la información.

4.1.4. Ley 1266 del 2008 en la Protección de los Datos Personales

La Ley Estatutaria 1266 de 2008 (Ley 1266) regula el tratamiento de datos financieros, registros crediticios e información comercial recabada en Colombia o en el extranjero. La citada normativa define términos generales sobre habeas data y establece tanto bases como principios de procesamiento de datos, derechos de los interesados, obligaciones del responsable del tratamiento y normas específicas de los datos financieros [19].

De tal forma, la Ley 1266 establece las normas y condiciones aplicables a fuentes de datos para compartir información con operadores de datos y para que dicho operador gestione y comparta la información con los usuarios. Sin perjuicio de ello, la ley privilegia el tratamiento con fines de gestión de información financiera, crediticia, comercial y de servicios, considerando que esto beneficia al sector financiero y crediticio como una actividad de interés público.

4.1.5. Ley 1581 de 2012

Los datos personales en Colombia revisten gran importancia, pues estos resultan ser un componente significativo para la identificación de una persona. Así lo ha sostenido la Superintendencia de Industria y Comercio en su Guía Sobre la Protección de datos personales “Cuando hablamos de datos personales nos referimos a toda aquella información asociada a una persona y que permite su identificación” [20]. En esa medida, ante la necesidad de un tratamiento especial de los datos personales, nace en Colombia la Ley 1581 de 2012, en la cual se incluyó todas las disposiciones generales en materia de protección de

datos personales y se emitieron lineamientos respecto a la recolección, manejo y circulación de todos los datos que fueran incluidos en las diferentes bases de datos [20].

Así las cosas, teniendo en cuenta el gran universo que abarca los datos personales, resulta importante analizar más a fondo cada uno de los parámetros establecidos en materia de protección de datos, pues ante la constante globalización respecto a las nuevas tecnologías, los datos personales se convierten en un activo de cada persona y, por lo tanto, merecen una política integral sobre el uso y la destinación de los mismos. Esto con el fin de atender al principio de responsabilidad demostrada.

De tal forma, conocer los fundamentos de la Ley Estatutaria 1581 de 2012 y los lineamientos que esta propone respecto a las condiciones de seguridad a las cuales deben sujetarse los datos personales, permite que, como dueños de la información, cada persona haga respetar el buen uso y la correcta destinación de sus datos y de esta manera prevenir los daños derivados de un uso inadecuado de los datos personales [20].

Sin embargo, si bien la norma desarrolla y abarca en su totalidad todos los lineamientos necesarios, que deben ser tenidos en cuenta para crear políticas efectivas en materia de tratamiento de datos personales, con el fin de prevenir conductas inadecuadas en este proceso, la misma es carente frente a la regulación relacionada con las responsabilidades por los daños y/o perjuicios que puede acarrear un tratamiento de datos deficiente.

Así pues, la norma destinó un Título para regular todo lo relacionado a los mecanismos de vigilancia y sanción, en donde, se enuncian los tipos de sanciones frente al incumplimiento de los deberes por parte de los Responsables o Encargados del tratamiento de datos. Es decir, se estructura un modelo sancionatorio. No obstante, frente al directo afectado, que para el caso en particular resultan ser los titulares de la información, no se

reguló un resarcimiento frente a los posibles daños a los que se vieron inmersos estos, aun cuando la norma protege de manera especial al dueño de dicho activo [20].

Es decir, se evidencia un vacío normativo, pues la Ley Estatutaria no regula de manera directa los aspectos relacionados a la reparación del perjuicio causado. El ordenamiento, a través de la promulgación de dicha norma estructuró políticas efectivas en pro de velar por el respeto y la protección a los datos personales, empero dejó de lado regular un tema relevante como lo es la Responsabilidad Civil y la reparación de daños. Un cambio relevante que ha implementado el Derecho Privado en estos temas [20].

Con todo ello, vale la pena resaltar los avances que se lograron con la expedición de dicha norma, pues la misma, obligó que todo el tratamiento de datos personales estuviera directamente relacionado con la protección de garantías constitucionales. Así mismo, obligó a todas las empresas que recolectan datos y en general para todos aquellos sujetos que administran estas bases, estructurar políticas de seguridad que se encuentren acorde a los lineamientos legales y evite de esta manera el riesgo que puede generar para los derechos y libertades de una persona el manejo inadecuado de los datos.

4.1.6. Ley 1377 de 2013 y Normativas Posteriores

El Decreto 1377 de 2013 (Decreto 1377), es una pieza de regulación secundaria relacionada con la Ley 1581 de 2012 que establece requisitos para las bases de datos personales y domésticas relacionadas a la seguridad de la información, limitaciones al procesamiento de datos, procesamiento de bases de datos y avisos de privacidad, entre otros. Este Decreto también requiere que los controladores y procesadores adopten una política de privacidad y un aviso de privacidad. Luego, surgen el Decreto 886 de 2014 (Decreto 886) y Decreto 090 de 2018 (Decreto 090) emitido por el Ministerio de Comercio, Industria y

Turismo, así como la Resolución 090 de 2018 emitida por la Superintendencia de Industria y Comercio, que regula el Registro Nacional de Bases de Datos y fija plazos para el registro de las bases de datos existentes en Colombia.

4.1.7.Análisis Jurisprudencial de los Cambios Sucedidos en la Seguridad de la Información en Colombia

En los últimos años, las sentencias judiciales han abordado otros temas, como el tratamiento de datos personales en las redes sociales. Por ejemplo, la sentencia T-260 de 2012 decidió el caso de un padre que creó una cuenta de Facebook para su hija de 4 años. En este caso la Corte declaró que se había vulnerado el principio de libertad en el tratamiento de los datos personales. Por tanto, dado que la menor no tenía conocimiento de la creación de la cuenta en Facebook, el Juzgado consideró que se había vulnerado su derecho a la protección de datos, y ordenó a su padre que eliminara la cuenta [16].

Posteriormente, el Tribunal revisó el caso de una acreedora que decidió denunciar públicamente a su deudor moroso en Facebook. En sentencia T-050 de 2016 la Corte decidió que el mensaje publicado en Facebook vulneró el derecho a la privacidad de la deudora morosa, no solo porque expuso parte de sus datos personales, sino también porque la deudora no dio autorización para que dicha información fuera revelada. Si bien el derecho que finalmente se protegió en esta sentencia fue el derecho a la intimidad, el razonamiento del Tribunal tuvo especialmente en cuenta el derecho a la protección de datos del deudor implicado [16].

De tal manera, la posición de la Corte no ha sido tan clara en cuanto a los datos personales difundidos por los medios de comunicación. En las sentencias que se han adoptado recientemente sobre datos personales publicados en medios de comunicación, la

Corte ha abordado el problema como un conflicto entre el derecho a la libertad de expresión y acceso a la información, por un lado, y el derecho al honor y al buen nombre. de la persona involucrada, por otro lado. Por tanto, no ha mencionado el derecho de hábeas data, ni ha declarado que el derecho de hábeas data no es aplicable al caso, pues la discusión se centra en la información periodística difundida por los medios de comunicación en ejercicio de la libertad de expresión, y no en información recabada en bases de datos [16].

En relación con la labor de la autoridad de protección de datos, en Colombia, el Ministerio Público es la autoridad nacional encargada de controlar el correcto manejo de las bases de datos públicas. Cuando se trata de bases de datos privadas, la Superintendencia de Industria y Comercio (Superintendencia de Industria y Comercio, 'SIC') es la autoridad colombiana de protección de datos [22].

Respecto a esto último, hay tres pronunciamientos que vale la pena mencionar. El 24 de noviembre de 2014, la SIC publicó un concepto legal que establece que el tratamiento de datos personales en las redes sociales no se encuentra dentro del alcance de la Ley 1581 de 2012 (régimen jurídico general aplicable al tratamiento de datos personales), ya que en estos casos la recolección, uso, circulación, almacenamiento o supresión de datos personales no se realiza dentro del territorio colombiano (ya que las redes sociales están domiciliadas en el extranjero) [22].

No obstante, el 3 de marzo de 2016, la SIC revisó su posición, argumentando que el tratamiento de datos personales se realiza en territorio colombiano no sólo cuando el recolector de datos tiene su domicilio en Colombia, sino también cuando para llevar a cabo

la recolección, uso, circulación o almacenamiento de los datos personales utiliza "medios que se encuentren en el territorio colombiano [22].

Finalmente, y en ejercicio de la obligación legal de garantizar la adecuada protección de los datos en la transferencia internacional de información (artículos 21 y 26 de la Ley 1581 de 2012), la SIC emitió la Circular Externa 005 del 10 de agosto de 2017, mediante la cual definió los estándares para la transferencia internacional de datos. La Circular establece una lista de países que Colombia considera que tienen un nivel adecuado de protección de datos, entre los que se encuentran los países de la Unión Europea (que han sido aprobados como adecuados por la Comisión Europea), México, República de Corea, Costa Rica, Serbia, Perú, Noruega, Islandia y Estados Unidos [22].

Sin embargo, la SIC no explica por qué estos países se consideran adecuados y, sobre todo, cómo justifica la inclusión de Estados Unidos, que ha sido criticado por Human Rights Watch por no ofrecer a los extranjeros las mismas garantías que tienen sus nacionales [23].

Además, no define cómo se mantendrá la adecuación de estos países (ya que las leyes cambian con el tiempo), ni cómo se evaluará el nivel de protección de otros países en el futuro. Por último, y contrariamente al modelo europeo, la Circular no prevé un procedimiento para impugnar las decisiones de “adecuación seguridad de la información” [22].

En relación a los ejemplos de violaciones de datos; en 2014 se conoció que una red de individuos logró acceder ilegalmente a la base de datos que maneja la Unidad para la Atención y Reparación Integral a las Víctimas. Se informó que estas personas lograron acceder a la base de datos utilizando códigos de autorización que se les habían filtrado.

Estos datos se vendían para permitir que personas sin escrúpulos se hicieran pasar por víctimas reales, acelerar el pago de indemnizaciones a determinados demandantes o conocer los datos personales de los denunciantes, entre otros delitos [23].

Igualmente, el 16 de febrero de 2016, la periodista Vicky Dávila, directora de la emisora de radio "La Fm", divulgó una grabación en la que aparece un viceministro colombiano manteniendo una conversación de carácter sexual con un policía. Según el periodista, quien alegó haber sido intervenido por la Policía, esta grabación forma parte de los registros que evidenciarían la relación del viceministro con una red de prostitución que opera dentro de la Policía. Este escándalo terminó tanto en la renuncia del viceministro como en el despido del periodista [23].

Del mismo modo, el 3 de abril de 2016 se filtraron 11,5 millones de documentos de la firma de abogados panameña Mossack Fonseca & Co., que detallan información financiera de más de 214.488 entidades off-shore, exponiendo a cientos de colombianos [23].

4.1.8. Normativas ISO/IEC 27000

La familia de las normas ISO/IEC 27000 [X], son un marco de referencia de seguridad a nivel mundial desarrollado por la International Organization for Standardization - ISO e International Electrotechnical Commission – IEC, que proporcionan un marco, lineamientos y mejores prácticas para la debida gestión de seguridad de la información en cualquier tipo de organización. Estas normas especifican los requerimientos que deben cumplir las organizaciones para establecer, implementar, poner en funcionamiento, controlar y mejorar continuamente un Sistema de Gestión de Seguridad de la Información [6].

En Colombia, el Instituto Colombiano de Norma Técnicas y Certificaciones, ICONTEC, es el organismo encargado de normalizar este tipo de normas. De tal manera, las siguientes son algunas de las normas que componen la familia ISO/IEC 27000, las cuales estructuran el marco normativo del presente trabajo.

Tabla 1. Marco Normativo y Legal

Norma	Descripción
ISO/IEC 27000:2018	Suministra información introductoria a seguridad de la información y a la gestión de la seguridad de la información, el estado y la relación de las normas de la familia de estándares para un SGSI.
ISO/IEC 27001:2013 (antigua BS 7799-2:2002)	Es una norma que admite certificación y especifica los requerimientos para la definición, implementación, implantación, mantenimiento y mejora de un SGSI.
ISO/IEC 27002:2013 (antigua ISO 17799:2005	Proporciona la guía de implementación de los controles aplicables a la seguridad de la información. Contiene once (11) cláusulas de control de la seguridad que contienen un total de treinta y nueve (39) categorías de seguridad e igual número de indicaciones de objetivos de Control. Estas cláusulas, objetivos de control y controles, son incorporados en el Anexo A de la norma ISO/IEC 27001.
ISO/IEC 27003:2017	Proporciona información práctica y una guía de implementación de la norma ISO/IEC 27001, indicando las directivas generales necesarias para la correcta implementación de un SGSI. Incluye instrucciones sobre cómo lograr la implementación de un SGSI con éxito.
ISO/IEC 27004:2016	Proporciona una guía y suministra recomendaciones para el desarrollo y uso de métricas para evaluar la efectividad de un SGSI, los objetivos de control y controles utilizados para implementar y gestionar la Seguridad de la Información, según la norma ISO/IEC 27001.
ISO/IEC 27005:2018 (antigua ISO TR 13335-	Proporciona una guía metodológica para la Gestión de Riesgos de una organización, alineada con los requerimientos

IT. Information Tecnologies Tecnologías de la información.

3:1998 e ISO TR 13335-4:2000)	de la norma ISO/IEC 27001.
ISO/IEC 27006:2015	Crea los requerimientos para organismos que prestan servicios de auditoría y certificación.
ISO/IEC 27007:2017	Provee una guía para la realización de las auditorías de un SGSI y la competencia de los auditores, de acuerdo con la norma ISO/IEC 27001.
ISO/IEC TR 27008:2011	Es un reporte técnico que brinda una guía para la revisión de la implementación de los controles del SGSI.
ISO/IEC 27009:2016	Detalla los requisitos para usar la norma ISO/IEC 27001 en cualquier otro ámbito. El documento explica cómo refinar e incluir requisitos adicionales a los de la norma ISO/IEC 27001 y cómo incluir controles o conjuntos de control adicionales
ISO/IEC 27010:2015	Provee una guía para gestionar la seguridad de la información en caso la organización intercambie o comparta información importante, ya sea que pertenezca al sector público o privado, que lo haga nacional o internacionalmente, o en el mismo sector u otros sectores del mercado en el que opera.
ISO/IEC 27011:2016	Provee una guía para apoyar la implementación de un SGSI en una empresa de telecomunicaciones.
ISO/IEC 27013:2015	Brinda una guía para la implementación integrada del ISO/IEC 27001 y el ISO/IEC 20000 (gestión de servicios de TI), ya sea implementándolos al mismo tiempo o uno después de otro.
ISO/IEC 27014:2013	Brinda una guía para conocer los principios y procesos del gobierno de la seguridad de la información, que busca que las organizaciones puedan evaluar, dirigir y monitorear la gestión de la seguridad de la información.
ISO/IEC 27015:2012	Es una guía de SGSI orientada a organizaciones del sector financiero y de seguros.
ISO/IEC TR 27016:2014	Es un reporte técnico que brinda una metodología que permite a las organizaciones saber cómo valorar adecuadamente los activos de información identificados, los riesgos potenciales a los activos, apreciar el valor de los controles que protegen a estos activos y determinar el nivel óptimo de recursos que deben ser usados para asegurarlos.

ISO/IEC 27017:2015	Es una guía de seguridad para Cloud Computing alineada con ISO/IEC 27002 y con controles adicionales específicos de estos entornos de nube.
ISO/IEC 27018:2014	Es un código de buenas prácticas en controles de protección de datos para servicios de computación en cloud computing.
ISO/IEC TR 27019:2017	Es una guía para el proceso de sistemas de control específicos relacionados con el sector de la industria de la energía.
ISO/IEC 27031:2011	Abarca todos los eventos e incidentes que se relacionan con la seguridad que puede tener un impacto en la infraestructura y los sistemas TIC. Incluye y se extiende a las prácticas de manejo de incidentes de seguridad de la información y la gestión de la planificación y preparación para las TIC y los servicios.
ISO/IEC 27032:2012	Ofrece unas líneas generales de orientación para fortalecer el estado de la ciberseguridad en una empresa, utilizando los puntos técnicos y estratégicos más importantes para esa actividad y los que están relacionados con la seguridad en las redes, seguridad en internet, seguridad de la información y la seguridad de las aplicaciones.
ISO/IEC 27033:2015	Provee una descripción general de los controles que soportan arquitecturas técnicas de seguridad de red y controles técnicos relacionados, así como aquellos controles no-técnicos y técnicos que son aplicables no sólo a las redes.
ISO/IEC 27034:2011	Proporciona una guía de seguridad de la información dirigida a los agentes de negocio y de TI, auditores y desarrolladores y los usuarios finales de las TIC, es decir, sirve para aquellas personas que llevan a cabo el diseño, programación, adquisición y uso de los sistemas de aplicación. La finalidad de dicha norma es asegurar que las aplicaciones informáticas conceden el nivel necesario o deseado de la seguridad en apoyo del Sistema de Gestión de Seguridad de la Información de las empresas.
ISO/IEC 27035:2011	Explica un enfoque de mejores prácticas destinado a la gestión de la información de incidentes de la seguridad. Los controles de la seguridad de la información no son perfectos debido a que pueden fallar, pueden trabajar sólo parcialmente o incluso, a veces, están ausentes, es decir, no están en funcionamiento. Debido a esto, los incidentes pasan debido a que los controles preventivos no son totalmente eficaces o fiables.
ISO/IEC 27036:2014	Guía en cuatro partes de seguridad en las relaciones con proveedores.

IT. Information Tecnologies Tecnologías de la información.

ISO/IEC 27037:2012	Está claramente orientada al procedimiento de la actuación pericial en el escenario de la recogida, identificación y secuestro de la evidencia digital, no entra en la fase de Análisis de la evidencia.
ISO/IEC 27038:2014	Es una guía de especificación para seguridad en la redacción digital.
ISO/IEC 27039:2015	Es una guía para la selección, despliegue y operación de sistemas de detección y prevención de intrusión.
ISO/IEC 27040:2015	Es una guía para la seguridad en medios de almacenamiento.
ISO/IEC 27041:2015	Es una guía para garantizar la idoneidad y adecuación de los métodos de investigación.
ISO/IEC 27042:2015	Es una guía con directrices para el análisis e interpretación de las evidencias digitales.
ISO/IEC 27043:2015	Desarrolla principios de investigación para la recopilación de evidencias digitales.
ISO/IEC 27050:2016	Desarrolla en tres partes sobre la información almacenada en dispositivos electrónicos en relación con su identificación, preservación, recolección, procesamiento, revisión, análisis y producción.
ISO/IEC 27103:2018	Es una norma desarrollada para proporcionar orientación sobre cómo aprovechar las normas existentes en un marco de ciberseguridad.
ISO/IEC TR 27701:2019	Este documento especifica los requisitos y proporciona orientación para establecer, implementar, mantener y mejorar continuamente un Sistema de gestión de información de privacidad (PIMS) a modo de extensión de ISO/IEC 27001 e ISO/IEC 27002 para la gestión de privacidad dentro del contexto de la organización. Especifica los requisitos relacionados con PIMS y proporciona orientación para los controladores y procesadores de PII que tienen la responsabilidad y la responsabilidad del procesamiento de PII.

Fuente: Elaboración propia.

5. Referente Conceptual

5.1. Seguridad de la Información

El tratamiento de la información el día de hoy en Colombia, es supremamente importante para las organizaciones tanto públicas como privadas y evocarla es sinónimo de paradigmas, los cuales por el trasegar insoluble y acelerado del avance tecnológico supone un gran reto instantáneo para los empresarios y sus organizaciones, permitiendo considerar a la información como un activo fundamental de las compañías y su seguridad el objetivo principal de las nuevas tecnologías de la información y la comunicación.

En este sentido, con respecto a la seguridad de la información y sus salvaguardas cobra una gran relevancia las tecnologías de la información y la comunicación, las cuales obligan a generar diversos procesos estratégicos para el procesamiento, almacenamiento y distribución de los datos, obligando a las compañías a establecer reglas de juego y objetivos claros que cumplan con estándares que sean transversales a los tres pilares que todos los textos teóricos como la ISO 27001 2013, MAGERIT, COBIT entre otros indican, confidencialidad, Integridad y disponibilidad, abriendo indudablemente la brecha a la necesidad de la seguridad de la información y los equipos tecnológicos que se utilizan para su administración [15].

Así, sucesos e incidentes informáticos que asechan, manipulan y destruyen la información y que son de amplio conocimiento público en Colombia y en el mundo tales como el hackeo de China a Microsoft para espiar a más de 250.000 servidores donde se ubicaban datos de miles de empresas occidentales ocurrido en el mes de enero del 2021, los ataques del grupo Hacktivista Anonimus al gobierno nacional de Colombia y sus

fuerzas armadas durante las manifestaciones del 2021 con el fin de desestabilizar el país [15].

De tal forma, el ataque a los sistemas de información de una empresa pequeña o los simples correos Phising que se envían diariamente a los buzones de correos personales para el robo económico y de información personal, son una firme muestra de que las amenazas están latentes y han llevado a las empresas a preocuparse más por sus activos de información y a cerciorarse si estos se encuentran correctamente identificados y valorados [15].

Por lo tanto, la Norma NTC ISO/IEC 27001:2013 la define como: preservación de la confidencialidad, integridad y disponibilidad de información, pero a la vez aclara que dicha seguridad puede involucrar características tales como la autenticidad, no repudio y fiabilidad. Autenticidad: Propiedad de que una entidad es lo que dice ser. No repudio: Capacidad que se tiene de probar la ocurrencia de un evento o acción que se atribuye y las entidades que lo originan. Fiabilidad: Propiedad de tener un comportamiento y resultados previstos [6].

5.2. **Sistemas de Gestión**

Un sistema de gestión es un conjunto de políticas, procesos y procedimientos utilizados por una organización para garantizar que pueda cumplir con las tareas requeridas para lograr sus objetivos. Estos objetivos cubren muchos aspectos de las operaciones de la organización (incluido el éxito financiero, la operación segura, la calidad del producto, las relaciones con los clientes, el cumplimiento de las leyes y reglamentaciones y la gestión de los trabajadores) [2].

Por ejemplo, un sistema de gestión ambiental permite a las organizaciones mejorar su desempeño ambiental, y un sistema de gestión de seguridad y salud ocupacional permite que una organización controle sus riesgos de salud y seguridad ocupacional. En este sentido, la norma internacional ISO 9000:2015 (Título: Sistemas de gestión de calidad - fundamentos y vocabulario) define el término en el capítulo 3.5.3 como un "conjunto de elementos interrelacionados o que interactúan de una organización para establecer políticas y objetivos, y procesos para lograr esos objetivos" [6].

De este modo, una simplificación de los aspectos principales de un sistema de gestión es el enfoque de 4 elementos "planificar, hacer, verificar, actuar". Un sistema de gestión completo cubre todos los aspectos de la gestión y se centra en apoyar la gestión del desempeño para lograr los objetivos. El sistema de gestión debe estar sujeto a una mejora continua a medida que la organización aprende [8].

Consecuentemente, entre los ejemplos de estándares de sistemas de gestión incluyen: ISO 9000: normas para sistemas de gestión de la calidad (SGC); ISO 13485: estándar para dispositivos médicos; ISO 14000: normas para sistemas de gestión ambiental; Sistema de Información Gerencial (SIG).

5.3. Modelo de Privacidad y Seguridad de la Información

Un Modelo de Privacidad y Seguridad de la Información debe tomar en cuenta en primer lugar el control de acceso que es una técnica de seguridad que regula quién o qué puede ver o utilizar recursos en un entorno informático. Es un concepto fundamental en seguridad que minimiza el riesgo para la empresa u organización. Hay dos tipos de control de acceso: físico y lógico. El control de acceso lógico limita las conexiones a las redes informáticas, los archivos del sistema y los datos [24].

IT. Information Tecnologies Tecnologías de la información.

De tal manera, los sistemas de control de acceso realizan la autenticación de identificación y la autorización de usuarios y entidades mediante la evaluación de las credenciales de inicio de sesión requeridas que pueden incluir contraseñas, números de identificación personal (PIN), escaneos biométricos, tokens de seguridad u otros factores de autenticación. La autenticación multifactor (MFA) que requiere dos o más factores de autenticación, suele ser una parte importante de una defensa en capas para proteger los sistemas de control de acceso [24].

Consecuentemente, el objetivo del control de acceso es minimizar el riesgo de seguridad del acceso no autorizado a los sistemas lógicos. El control de acceso es un componente fundamental de los programas de cumplimiento de seguridad que garantiza que la tecnología de seguridad y las políticas de control de acceso estén implementadas para proteger la información confidencial, como los datos de los usuarios. La mayoría de las organizaciones cuentan con infraestructura y procedimientos que limitan el acceso a redes, sistemas informáticos, aplicaciones, archivos y datos confidenciales, como información de identificación personal (PII) y propiedad intelectual.

De tal manera, los sistemas de control de acceso son complejos y pueden ser difíciles de administrar en entornos de TI dinámicos que involucran sistemas locales y servicios en la nube. Después de algunas infracciones de alto perfil, los proveedores de tecnología han pasado de los sistemas de inicio de sesión único (SSO) a la gestión de acceso unificado, que ofrece controles de acceso para entornos locales y en la nube [24]. Así, el gobierno colombiano ha dictado lineamientos para un modelo de privacidad y seguridad de la información, lo cual se detalla a continuación.

Al respecto, el gobierno de tecnología de la información (TI) gubernamental en Colombia, es un concepto que con la promesa de hacer visible el valor que generan, ha ido tomando forma para ser mejor interpretado, implementado y aplicado, globalmente. Actualmente, existen muchas definiciones, lo enmarca en una estructura de relaciones para dirigir y controlar el papel de la tecnología de TI dentro de una organización con el fin de lograr los objetivos con la agregación de valor y el balance de riesgo, en comparación con el retorno de TI y sus procesos.

Consecuentemente, parte de la estrategia en informática del gobierno radica en diseñar, aplicar y evaluar un conjunto de criterios que rijan la función respectiva óptimamente, lo explica como un conjunto de reglas, principios, políticas u organigramas que definen o limitan el alcance de los jefes de área.

Paralelamente, el gobierno de TI se define como un conjunto de prácticas o actividades institucionalizadas que minimizan la incertidumbre y adquieren un mejor desempeño en cuanto a la relación de externalización entre Proveedores y subcontratistas de servicios de TI. En relación, se refiere que el instituto de gobierno de TI (ITGI) estableció cinco dominios de cobertura en la alineación estratégica de TI con el negocio: entrega de valor, riesgo, administración, administración de recursos y medición del desempeño [23].

Así, el gobierno de TI es la responsabilidad de los ejecutivos de la junta directiva y contempla liderazgo, estructuras y procesos operativos para asegurar que la TI de la empresa apoye las estrategias organizacionales y objetivos. En este sentido, la información es el activo más importante con el que cuenta una organización, por lo que su deber es

protegerlo. Su seguridad depende de garantizar el cumplimiento de su confidencialidad, integridad y disponibilidad, pilares o principios fundamentales de la información.

En la actualidad, una organización tiene claro que para mantenerse actualizado y mejorar la expansión del mercado, la interconectividad de Internet, los negocios, la automatización y los procesos en línea son relevantes. Esta tendencia de "tecnodependencia" además de traer beneficios, también implica riesgos para el activo de información, como consecuencia de las vulnerabilidades en el software y hardware de productos tecnológicos [23].

Así, la inmersión en la red de redes, como además de expandir el negocio, también expone un mayor número de amenazas al activo de información, porque amplía el área a controlar. Por lo tanto, la implementación de mecanismos para salvaguardar las TI es actualmente una necesidad para las organizaciones [24].

De acuerdo con las nuevas tendencias tecnológicas y con el objetivo de orientar a las entidades públicas de orden nacional y territorial en la mejora de los estándares de seguridad de la información, el Gobierno de Colombia a través del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), en el marco de la estrategia de gobierno en línea (GEL), diseñó la seguridad de la información y modelo de privacidad (MSPI), basado en las referencias de ISO/IEC 27001 versión 2013, National Marco de seguridad cibernética de Information Solutions Cooperative (NISC), la base legal de la ley sobre protección de datos personales, transparencia y acceso a la información pública entre otros, relevantes en la gestión de la seguridad de los activos de información [23].

En este sentido, el modelo contiene un marco holístico que aborda el gobierno de TI, a través de un patrón que diseña los requisitos de gestión, para la seguridad de la información, el ciclo de vida, la gestión de riesgos y el cumplimiento, desde el marco de gobierno de TI. Así, el MSPI tiene un enfoque sustentable que va desde preparar a la entidad para iniciar la implementación, definiendo brechas, hasta la alineación con el sistema de gestión de seguridad de la información (SGSI) [24].

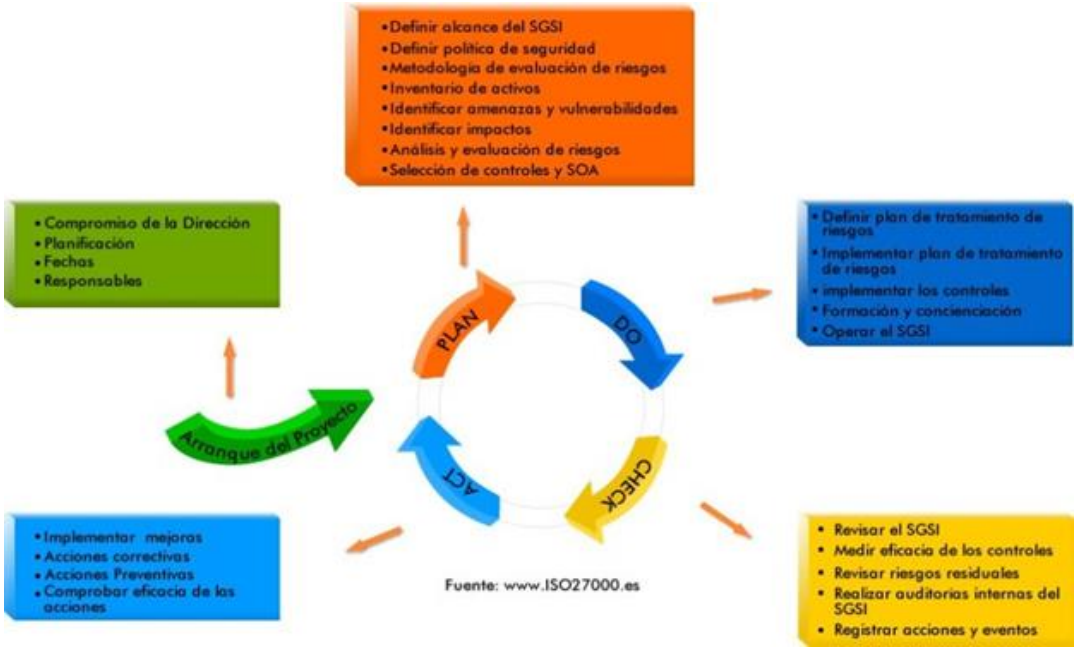
Esto permite deducir, que el MSPI es un modelo orientado a la gestión, denotando la ausencia de control directo que ayuda a ejercer la dirección y complementa la gestión de las nuevas tecnologías en administración pública y privada. Además, se destaca en el área informática y en especial en las entidades, la necesidad de instrumentos de control relacionados con los procesos clave de TI, que permiten a la alta dirección monitorear, prevenir y controlar.

6. Metodología

Para cumplir de manera efectiva con los objetivos que se plantean en la presente investigación es necesario definir adecuadamente los elementos metodológicos en los cuales se contextualiza el presente trabajo. Los pasos a seguir para el desarrollo del proyecto se pueden visualizar mediante la siguiente figura.

Figura 1

Definición de metodología



Fuente: www.ISO27000.es.

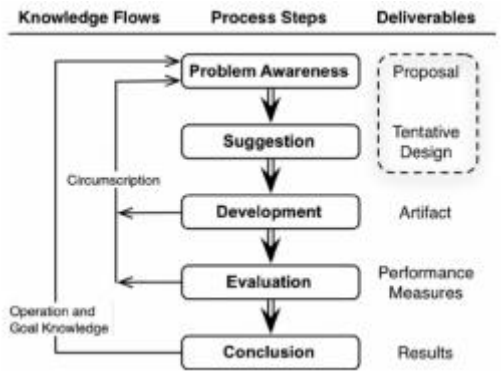
6.1. Tipo de Estudio

Estudio de carácter cualitativo, utilizado normalmente para solventar preguntas de investigación. Su propósito es abstraer la realidad, de la manera en que es percibida por las partes interesadas y que participan directa o indirectamente en el objeto de estudio [25]. El trabajo adopta este enfoque dado que desea generar buenas prácticas en base a los lineamientos dados por los procesos establecidos en la norma ISO/IEC 27001:2013, los cuales propenden garantizar la seguridad de la información en las organizaciones.

Por tanto, los resultados se traducen en un proceso expresado en palabras, no en cifras. Se utiliza la metodología Design Science Research (DSR) “Ciencia del diseño”, de acuerdo con el modelo sugerido por Peffers, Tuunanen, Rothenberger, & Chatterjee [26], (ver figura), teniendo en cuenta que esta metodología permite desarrollar un proceso que potencia el quehacer de los ingenieros en seguridad de la información a la vez que, indirectamente mejora la percepción de calidad y oportunidad de sus clientes.

Figura 2

Design Science Research



Fuente: Peffers, Tuunanen, Rothenberger, & Chatterjee (2007).

Como punto de partida de la investigación, se ha establecido un análisis del contexto actual de los procesos de seguridad de la información que permitan dar una mejor compresión de la problemática, posteriormente se hará el análisis comparativo de los procesos ágiles en relación con la norma ISO 27001:2013, que permita definir estrategias para la propuesta del proceso de la seguridad de la información, el cual será validado a través de la implementación del modelo sugerido en el documento.

6.1.1. El Modelo Piloto del Proceso

Para el presente trabajo de investigación, se trabajará con una auditoría de seguridad de la información que permitió validar el proceso de desarrollo propuesto,

IT. Information Tecnologies Tecnologías de la información.

empleando para ello la “escalera de pruebas”, Concepto, valor y uso. A continuación, se detalla cada uno.

6.1.1.1. Prueba de Concepto. Para adelantar dicha prueba se tuvieron en cuenta los siguientes elementos: 1. Definir el propósito de la prueba 2. Selección de la población a encuestar 3. Selección de la forma de aplicación de la encuesta 4. Comunicación del concepto a través de EPF-Composer 5. Medición de la respuesta de los encuestados 6. Interpretación de los resultados [26].

6.1.1.2. Prueba de Valor. Esta prueba es aplicada con dos empleados vitales de la compañía para la seguridad de la información, uno de los cuales empleará su proceso habitual y el otro el proceso propuesto, determinando productividad y competitividad; se emplearán las métricas señaladas en la siguiente tabla [26].

Tabla 2. Métricas empleadas para la prueba de valor

Métrica	Descripción
Esfuerzo	Esfuerzo requerido por el desarrollador para lograr los objetivos propuestos en el proyecto
Cubrimiento de requisitos	Permite identificar la cantidad de requisitos que se han dejado sin cubrir durante el proceso de desarrollo
Terminación de módulos en los tiempos esperados	Cumplimiento del tiempo de entrega de las versiones planificadas

58

Duración del proyecto	Estimación de la duración real del proyecto contrastada con la planificada.

Fuente: Peffers, Tuunanen, Rothenberger, & Chatterjee (2007).

6.1.1.3. Prueba de Uso. Permite determinar si los resultados de la seguridad de la información del Modelo propuesto son los esperados. Se tendrán en cuenta las métricas del SGSI en la siguiente tabla [26].

Tabla 3. Métricas para la prueba de uso

Métrica	Descripción
Cantidad de defectos	Permite calcular la cantidad de defectos en el proceso que se han generado en una iteración
Costos de desarrollo	Determina el costo presupuestal relacionado con el esfuerzo
Fallas de requerimientos descubiertas	Identifica las fallas que se han presentado en el proceso de recolección de requerimientos
Cantidad de inconformidades relacionadas con el proceso	Retroalimentación cuantificada de las inconformidades del proceso manifestadas por el desarrollador
Puntos de historia de usuario por iteración	Permite identificar la cantidad de puntos de historia de usuario que se han desarrollado en cada iteración del proceso
Líneas de código	Cantidad aproximada de líneas de código lógicas implementadas en el desarrollo
Cantidad de documentos de soporte que se entregan	Número total de documentos que entrega el desarrollador como soporte

Fuente: elaboración propia

Fuente: Peffers, Tuunanen, Rothenberger, & Chatterjee (2007).

6.2. Técnicas e Instrumentos de Recolección de Información

Se diseñaron los siguientes instrumentos: 1. Determinación de las prácticas y principios de los procesos de seguridad de la información actualmente utilizados en la compañía. 2. Comparación de las prácticas actuales con los objetivos establecidos en la norma 27001:2013 3. Encuestas para las pruebas de concepto 4. Diseño de instrumentos para determinar las métricas del modelo.

6.3. Procedimientos

Para alcanzar los objetivos propuestos se establecieron las siguientes fases: Fase 1: Planeación de los procesos de seguridad de la información según la norma ISO 27001:2013, la cual consiste en establecer las etapas y características del SGSI, está fase involucra actividades tales como: 1. Definir el alcance del SGSI 2. Definir política de seguridad 3. Metodología de evaluación de riesgos 4. Inventario de activos 5. Identificar

amenazas y vulnerabilidades 6. Identificar impactos 7. Análisis y evaluación de riesgos 8. Selección de controles SOA.

Igualmente, Fase 2: Hacer, la cual corresponde a implementar el SGSI, de acuerdo con las especificaciones dadas por la norma ISO 27001:2013 1. Identificación de las mejores prácticas de los procesos de desarrollo analizados 2. Correspondencia de las mejores prácticas Fase 3: Definición del proceso 1. Diseño de un modelo de proceso de seguridad de la información con base en los resultados obtenidos en las fases anteriores 2. Diseño de los procedimientos, actividades y artefactos detallados que constituirán el proceso propuesto alineado con los requisitos de la Norma ISO 29110:2014. Fase 4: Diseño del proceso propuesto en EPF - Composer 1. Puesta a punto del proceso modelado con EPF-Composer para su distribución. Fase 5: Validación del proceso 1. Aplicación del proceso en un modelo de seguridad de la información 2. Aplicación de las pruebas de concepto, valor y uso 3. Análisis de resultados.

6.4. Plan de Análisis

El análisis de los resultados parciales y totales se adelantó igualmente por fases de la siguiente manera: Fase 1: Correspondencia de los procesos ágiles con la norma ISO 27001:2013 1. Interpretación de los resultados obtenidos en la correspondencia de los procesos ágiles con relación a los requisitos establecidos en la norma ISO 27001:2013. Grado de acoplamiento de los requisitos establecidos en la norma ISO 27001:2013 con relación a los procesos ágiles. Fase 2: Identificación de las mejores prácticas de los procesos analizados 1. Identificación de mejores prácticas de cada proceso. 2. Grado de acoplamiento de los requisitos establecidos en la norma ISO 27001:2013 con relación a las mejores prácticas identificadas.

IT. Information Tecnologies Tecnologías de la información.

Del mismo modo, la Fase 3: Definición del proceso En esta fase se construyó una matriz que permite visualizar las mejores prácticas, en contraste con los requisitos de la Norma ISO 27001:2013. Fase 4: Diseño del proceso propuesto, incluyendo tareas, procesos, artefactos y demás herramientas que garantizan un adecuado Modelo de seguridad de la información.

Igualmente, la Fase 5: Validación del proceso Se realizó la escalera de pruebas empleando pruebas de concepto, valor y uso. 1. La prueba de concepto se realizó a través de encuestas a interesados lo que permitió determinar a viabilidad técnica del proceso propuesto. 2. La prueba de valor se determinó mediante la aplicación de un modelo de seguridad de la información a dos colaboradores, de los cuales uno aplica el proceso propuesto y el otro no, lo que permitió determinar la productividad y competitividad del modelo definido, empleando para ello métricas del proceso de seguridad de la información. 3. La prueba de uso nos permitió verificar si el uso del modelo definido generaría los resultados esperados, para lo cual se aplicaron métricas del proceso de seguridad de la información.

7. Desarrollo del proyecto

7.1 Planeación del sistema de gestión de seguridad de la información.

La planeación del sistema de gestión de seguridad de la información en la compañía CM se define después de una búsqueda exhaustiva de las diferentes metodologías y normas que ofrecen valor y modelos distintivos para el buen desarrollo del proyecto, el modelo escogido es la ISO 27001:2013 con la ayuda de la herramienta MSPI que plantea Mintic de gobierno Nacional Colombiano.

7.1.1 Definición del alcance del sistema de gestión de seguridad de la información.

En función del contexto de la empresa y de cada momento particular en que se despliegan las acciones, objetivos y tareas diarias, la compañía está inevitablemente expuesta a situaciones de riesgo en base a diversos elementos que pueden afectar y que, de hecho, afectan, negativamente a los activos de información más importante; por ello se define el alcance.

Para definir el alcance del SGSI de la entidad Collective Mining se debe iniciar con una descripción pequeña de la labor de la compañía y el tiempo que llevan en funcionamiento. Collective Mining es una compañía Minera Canadiense, fundada en el mes de agosto del año 2020, esta tiene su sede principal en Colombia en el municipio de Supia en el departamento de Caldas, como su nombre lo indica prima lo colectivo y el bienestar de las comunidades y sus empleados, sus principales pilares son la Gestión Ambiental, Gestión Social y Gobernanza, tiene alrededor de 20 empleados de los cuales 10 hacen labor administrativa y de oficina y 10 labor de Campo, en general es una compañía nueva o Junior en su campo, con un potencial de manejo de las tecnologías de la información pequeño pero en crecimiento, con poco presupuesto en temas de TI por su tamaño y su

core de Negocio, pero con la disposición de generar conocimiento e implantarlo en su estructura organizacional a medida que se complejiza la productividad de la misma.

Con veras de definir mejor el alcance se hace una evaluación del estado inicial de la seguridad de la información por medio de la Herramienta MSPI del MINTIC colombiano, a continuación, se muestra una imagen donde se detalla que el estado actual de la compañía es difícil, pero esto se da por su condición de ser una compañía demasiado nueva y con bajo presupuesto para el área de TI, a lo cual se determina la importancia de implementar un SGSI con un modelo que se acople fácilmente a ese tipo de compañías.

Imagen #xx Evaluación inicial de la seguridad de la información Collective Mining.

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	20	100	INICIAL
A.8	GESTIÓN DE ACTIVOS	20	100	INICIAL
A.9	CONTROL DE ACCESO	0	100	INEXISTENTE
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	20	100	INICIAL
A.12	SEGURIDAD DE LAS OPERACIONES	20	100	INICIAL
A.13	SEGURIDAD DE LAS COMUNICACIONES	40	100	REPETIBLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	40	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	40	100	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	40	100	REPETIBLE
A.18	CUMPLIMIENTO	0	100	INEXISTENTE
PROMEDIO EVALUACIÓN DE CONTROLES		17	100	INICIAL

Como se observa la compañía se encontraba limitada en temas de seguridad de la información, esto se da porque la empresa solo llevaba un año de existencia y no se contaba con área de TI y mucho menos manejaban temas de seguridad de la información, sin embargo, ya disponían de equipos de cómputo, impresoras, canales de internet y redes de comunicación LAN, personal administrativo, logístico y de campo y lo más importante información construida y valiosa para la entidad.

Por lo anterior la compañía toma la decisión de crear un área (IT) que pueda gestionar y administrar los procesos, procedimientos, seguridad y custodia de la información y las tecnologías que la sostiene. Partiendo de la construcción del área se toma la decisión de construir el modelo de seguridad y privacidad basado en la ISO 27001 – 2013 y el MSPI planteado por el MINTIC del gobierno nacional colombiano, el cual pone a disposición de las empresas, la guía, para poder cimentar una línea base durante los estudios de la implementación del modelo propuesto y de esta manera ayudar a proteger los bienes, activos y servicios de la compañía Guía No. 1 Seguridad y privacidad de la información página 7.

7.1.1.1 Comprensión de las necesidades y expectativas de las partes

Para empezar a dar forma al alcance se debe entender que independientemente de la actividad, tamaño y tipo, cualquier compañía obtiene, procesa, almacena y transporta información mediante el uso y aplicación de sistemas, procesamiento, redes y personas internas y externas que se relacionan directa e indirectamente con la organización.

Todos estos entes son activos de información fundamentales para lograr los objetivos de la compañía, los cuales están dirigidos por partes interesadas que son pertinentes para la gestión de la seguridad de la información, apoyadas en unos requisitos corporativos, legales, contractuales y reglamentadas por parte de la alta gerencia de la compañía.

Referencias Bibliográficas

[1]. Chopra S, Meindl P. Administración de la seguridad de los datos. (Tercera ed.). Ciudad de México: Pearson Education; 2008.

[2]. Villalba C. Implementación de Sistema de Seguimiento de Control de Datos. Artículo de investigación. Escuela Técnica Superior de Ingeniería Universidad de Sevilla, Sevilla; 2018.

[3]. Ametic. (s.f.). *Transformación digital - Visión y Propuesta de AMETIC*. Recuperado de: https://www.thinktur.org/media/TD-Vision-y-Propuesta.-AMETIC.pdf; (s.f).

[4]. Chiavenato I. Procesos Administrativos**.** 3era edición. Bogotá: Mc Graw Hill; 2011.

[5]. Roca G. La transformación digital de los negocios. Recuperado de: http://boletines.prisadigital.com/transcastdef.pdf.; 2014.

[6]. ISO 27000. Sistema de Gestión de la Seguridad de la Información; 2012.

[7]. Rea-Guaman A, Sanchez-Garcia I, Feliu, T. Maturity models in cybersecurity: A systematic review; 2017. 10.23919/CISTI.2017.7975865.

[8]. Tejena-Macías, M. Análisis de riesgos en seguridad de la información. 2018; Vol 3, No 4.

[9]. Schwab K. La cuarta revolución industrial. Barcelona: Random House; 2016.

[10]. Benavides Carranza J. Integración de la NTC ISO/IEC 27001:2013 con el Modelo de Seguridad y privacidad de la Información-MSPI del MinTIC; 2019.

[11]. Argüello C. Gestión de la seguridad de los datos en Madecentro Colombia S.A. Trabajo para optar al grado de Licenciado en Contaduría; 2015.

[12]. Pereira F. Modelo de referencia para el dimensionamiento de riesgos operacionales en la gestión de los datos del sector MiPyme. Trabajo presentado para optar al grado de Magister en Logística Integral. Universidad Autónoma de Occidente Facultad de Ingeniería Maestría en Logística Integral. Santiago de Cali, Colombia; 2015.

[13]. Álvarez J. Sistema de control basado en el informe COSO, para el tratamiento de los datos en la policía de Bucaramanga, Colombia; 2016.

[14]. Ceballos J. Diseño de un Sistema de Control de la Gestión de datos para Empresas Ferreteras del Departamento del Valle del Cauca. Universidad Nacional, Abierta y a Distancia, Bogotá, Colombia.; 2017.

[15]. Perea E, Sánchez P. Diseño de un modelo de transferencia de la metodología de referencia de operaciones para la seguridad de la información de la Fuerza Aérea Colombiana. Artículo de investigación. Ciencia y Poder Aéreo, Revista Científica de la Escuela de Postgrados de la Fuerza Aérea Colombiana; 2018.

[16]. Puello Rincón C. Herramientas Jurídicas Para La Protección de los Datos Personales en empresas privadas; 2016.

[17]. Constitución Política de Colombia. Bogotá, Colombia; 1991.

[18]. Decreto 1078 de 2015 Sector de Tecnologías de la Información y las Comunicaciones. Bogotá, Colombia; 2015.

[19]. La Ley Estatutaria 1266 de 2008 (Ley 1266). Bogotá, Colombia; 2008.

[20]. Ley 1581 de 2012. Bogotá, Colombia; 2012.

[21]. Ley 1377 de 2013. Bogotá, Colombia; 2013.

[22]. Reynoso J. Análisis de la gestión de los datos dentro del ejército, Colombia. Artículo de investigación. Revista Comercio Exterior. 2017; 55 (3), 23.

[23]. Villalba C. Implementación de Sistema de Seguimiento de Control de Datos. Artículo de investigación. Escuela Técnica Superior de Ingeniería Universidad de Sevilla, Sevilla; 2018.

[24]. Garriga A. Tratamiento de Datos Personales y Derechos Fundamentales. Madrid, España: Dykinson. Avances y Retos. 2004; (4), 195-214.

[25]. Arias J. El proyecto de Investigación: Introducción a la investigación científica. Edición 6ta. Ciudad de México: Episteme; 2012.

[26]. Peffers C, Tuunanen, E, Rothenberger D, Chatterjee A. Design Science Research (DSR). Ciencia del Diseño. 2007; 196-211.