Importancia de la Protección de la Información en Empresas de Seguridad Privada en Colombia

Ensayo Académico presentado por:

TOMÁS ADRIÁN GÓMEZ CASTAÑO[1]

A:

Coronel ra. JORGE ISAZA, MBA-PhD.
Docente de la Asignatura

Tutor Temático
Dr. JULIÁN ANDRÉS PUENTES

FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD

Programa ADMINISTRACIÓN DE LA SEGURIDAD

BOGOTÁ D.C.

2021

[1] **Administrador Policial**

1. Resumen

La era digital trajo consigo un sinfín de ventajas, tanto así que, con el transcurrir del tiempo, un gran número de empresas se han valido de las nuevas tecnologías para expandirse de formas inimaginables, no obstante, así como dichas herramientas han sido utilizadas de forma positiva y creativa, también, han llegado a ser una amenaza para las corporaciones que no han preservado correctamente lo más valioso que tienen: su información. En lo referente a las empresas de seguridad privada, este es un punto de suma importancia, pues, debido a que pertenecen al área de la seguridad, poseen información altamente sustancial y vital, por lo que, es sumamente indispensable para el sano desarrollo empresarial, la preservación de la confidencialidad, el aseguramiento de la integridad y la accesibilidad de la información.

Palabras clave: confidencialidad, disponibilidad, información, integridad, seguridad.

2. Abstract

The digital age brought with it endless advantages, so much so that, over the years, hundreds of companies have used new technologies to expand in unimaginable ways, however, just as these tools have been used in a positive and positive way. Creative, too, have become a threat to corporations that have not properly preserved the most valuable thing they have, their information. When it comes to private security companies, this is a point of utmost importance since, they possess highly substantial and vital information because they belong to the security area, therefore, preserving confidentiality and guaranteeing integrity and security. Availability of information is essential for its healthy development.

Keywords: confidentiality, availability, information, integrity, security.

3. Introducción

Inicialmente, para efectos académicos, se ha de revisar la definición de lo que se considera un sistema de información, siendo así, afirma Cohen & Asín (2000), que se trata de un conjunto de elementos que logran interactuar entre sí, con la finalidad de apoyar las distintas actividades de la empresa; dicho sistema de información realiza las siguientes actividades básicas: la primera es la entrada, la segunda es el almacenamiento, la tercera el procesamiento y la cuarta la salida de la información.

En virtud de lo anterior, los sistemas de información reciben como entrada unos datos que sufren un procesamiento y como resultado se obtiene la información que se maneja dentro de un negocio, en el caso de las empresas de seguridad privada, estas manejan información de suma importancia, dado su carácter dentro del ámbito de la seguridad, por lo tanto, es necesario que esta sea considerada como un activo estratégico y que sea tratada bajo estándares y normas que aumenten su seguridad.

En cuanto a la Seguridad de la información (SI) en adelante, la Organización Internacional de Normalización [ISO], (2006), la define como la preservación de la información, de manera que se garantice que esta sea confidencial, integra y este siempre disponible, lo que puede envolver además propiedades tales como: primero la autenticidad, segundo la trazabilidad, tercero el no repudio y cuarto la fiabilidad.

En este sentido, la SI son todos aquellos lineamientos que deben ser definidos dentro de las organizaciones para resguardar el que se considera hoy en día el activo más valioso: la información. Dicho activo cobra mayor valor cuando hablamos de empresas de seguridad privada, gracias a la información se toman decisiones de negocio

importantes, sobre las cuales se centran todas las estrategias de una compañía, por lo que se debe velar para que dicha información no sufra ningún tipo de alteraciones ni cambios no previstos y que siempre que el negocio necesite de ella para la toma de decisiones estratégicas, la encuentre disponible, para que ello sea posible, se debe centrar la atención en un concepto general, que es la tríada de la seguridad, conocida también en el sector como CIA Triad, que hace referencia a tres conceptos: primero, la confidencialidad, segundo la integridad y tercero la disponibilidad, sobre los cuales la norma ISO 27001 hace mucho énfasis en garantizar su cumplimiento y así poder tener segura nuestra información, dichos conceptos serán ampliados en el numeral 4.2 del presente ensayo académico.

En base a ello, este ensayo plantea un objetivo general, el cual, busca proponer un sistema de gestión que responda a los desafíos digitales que enfrenta una empresa de seguridad privada en Colombia, y para completar dicho objetivo, se plantean los siguientes objetivos específicos: se iniciará principalmente identificando riesgos y amenazas que afectan la información de las empresas de seguridad privada en Colombia, se continuará con el reconocimiento de los componentes de un sistema de gestión de seguridad de la información en adelante (S.G.S.I.) y se finalizará con el establecimiento de un modelo de S.G.S.I. que involucre el funcionamiento de una empresa del sector de la vigilancia y seguridad privada en Colombia.

4. Desarrollo

4.1. Riesgos y amenazas a la información de una empresa de seguridad privada

A manera de cumplir con el primer objetivo específico, se ha de iniciar identificando los riesgos y amenazas que pueden afectar la SI en las empresas de seguridad privada en Colombia.

En primer lugar, es importante tener claros los siguientes conceptos, en primer lugar, tenemos el riesgo, que según el Consejo Nacional de Política Económica y Social [CONPES], (2016), se puede considerar como el impacto o efectos que pueden ocasionar las incertidumbres sobre el sano cumplimiento de los objetivos, por su parte, el riesgo de seguridad digital, es una expresión que se utiliza para poder especificar un tipo especifico de riesgo ligado con actividades del ámbito digital. En cuanto a la gestión de riesgos de seguridad digital, afirma también el Consejo Nacional de Política Económica y Social [CONPES], (2016), que esta puede ser definida como todas aquellas actividades que se planifican al interior de las organizaciones, para la minimización de los riesgos del ámbito digital y la maximización de las oportunidades.

Ahora bien, se ha de precisar que, en el actual entorno organizacional o empresarial, existe una marcada inclinación general que define como bienes o activos de las organizaciones solo aquellos que son físicamente palpables como es el caso de la infraestructura física, los equipos tecnológicos como computadoras o servidores, entre otros, pero, es necesario recordar que también están los bienes que no son físicamente palpables, estos pueden ser: la base de datos de los clientes, los secretos comerciales, todo lo referente al ámbito reputacional, etc. (Instituto Nacional de Ciberseguridad [INCIBE], s.f.). En este sentido, en términos de gestión de riesgos de SI, afirma el instituto Nacional de Ciberseguridad [INCIBE] (2015), que el principal activo al que se debe garantizar protección es la información que fluye en los entornos empresariales, tanto

aquella almacenada en sistemas como la que se encuentra en otros medios, verbigracia, la manuscrita o impresa en papel o toda aquella información que pueden trasmitir las personas que desempeñan roles fundamentales dentro de las empresas.

En cuanto a las amenazas a las que se enfrenta la información de la empresa, siguiendo lo expuesto por el Instituto Nacional de Ciberseguridad [INCIBE] (2015), pueden ser muy variadas, verbigracia: pueden originarse por causas naturales como los sismos, desastres a causa del agua o el fuego, entre otros, a raíz de lo anterior pueden presentarse afectaciones de las infraestructuras de apoyo, afectaciones de los equipos tecnológicos ocasionando: daños o errores en los programas o aplicativos y a su vez errores humanos que pueden ser con o sin intención por parte del personal que participa en el flujo normal de la información.

En virtud de lo anteriormente descrito, según el CONPES y el INCIBE, es claro que diariamente las organizaciones se encuentran expuestas a vulnerabilidades y amenazas que generan riesgos hacia la información, específicamente su integralidad, su carácter confidencial y la posibilidad de acceder a ella en cualquier momento que sea requerida y con ello también hacia la viabilidad y continuidad del negocio; dichos riesgos provienen tanto del entorno externo en el que hacen vida las organizaciones, como del entorno interno de las mismas, como se menciona anteriormente, las personas son un factor determinante en cuanto al riesgo de SI, ya que interactúan de forma directa con ella.

Por otro lado, siguiendo al Instituto Nacional de Ciberseguridad [INCIBE], (s.f.) Hay empresas cuyo flujo de operaciones se fundamenta principalmente en el manejo de información, como las del medio televisivo, los medios escritos, los medios de

radiodifusión, las publicitarias, entre otras, pero estas no son las únicas que deben velar por la SI, también las pequeñas empresas deben hacerlo.

Resalta el Instituto Nacional de Ciberseguridad [INCIBE] (2015), que la evolución de la seguridad de la Información ha dependido de las distintas circunstancias que han permitido definir cada etapa de la historia, así pues: primeramente, en la prehistoria, el ser humano utilizaba las cuevas o cavernas en lugares montañosos para protegerse del clima o de los peligros, en la Edad Antigua (3.500 años a.C. al siglo V d.C.), se ha encontrado que se originó la información cifrada con el uso de jeroglíficos, también en Egipto se han descubierto restos de llaves y candados, y finalmente, en la edad contemporánea, es donde se produce una evolución del mercado 3.0; con la llegada de la globalización, se reformulan las antiguas leyes, cambia la preocupación por la privacidad, evoluciona la tecnología y ello trae consigo un aumento de la capacidad y velocidad de las transacciones, se crea otra forma distinta de entender los negocios, aparece el prosumidor o productor-consumidor y las iniciativas crowd.

Según lo anterior, es claro que desde tiempos antiguos, la protección y la seguridad han sido ejes sumamente importantes, por lo que hasta la actualidad, en plena era digital, se han inventado e implementado las barreras necesarias para intentar prevenir la sustracción y la manipulación de los datos e información confidenciales, pero el desarrollo y el rápido avance de las nuevas tecnologías ha marcado un cambio sustancial, se han aumentado los riesgos para las empresas, que cada vez más se encuentran expuestas a nuevas y más avanzadas amenazas; lamentablemente, hoy en día, le es más fácil a personas sin ningún tipo de autorización, tener acceso a herramientas que facilitan la tarea de vulnerar los accesos y obtener la información

protegida o confidencial, a partir de poco esfuerzo o conocimiento, lo que termina generando graves perjuicios para las empresas.

En este punto es necesario traer a colación el concepto de tecnología de la información o TI, que según Laudon & Laudon (2012), es el hardware y también el software que se requieren emplear para realizar los metas de una organización empresarial, lo que implica tanto a los diferentes equipos como las computadoras, los medios digitales de almacenamiento y los diferentes equipos móviles, como a los componentes de software: S.O. Windows o Linux, programas ofimáticos como Microsoft Office y los cientos de programas informáticos para cualquier dispositivo**.**

Si prestamos especial atención a los conceptos de sistema de información referenciados en la introducción de este ensayo académico y al concepto precedente de tecnologías de la información, se concuerda que la mayor parte de la información que manejan las organizaciones se encuentra en los diferentes dispositivos informáticos, en los medios de almacenamiento, en los diferentes programas y redes de datos enmarcados en los ya conocidos sistemas de información, dichos sistemas pueden verse afectados por diferentes riesgos, entre ellos los riesgos naturales o físicos como las inundaciones, los daños causados por fuego o incendios, los sismos o el vandalismo, entre otros, que pueden generar afectación a la disponibilidad de los recursos de información, por su parte, se encuentran los riesgos lógicos; asociados con la propia tecnología y que cada día van en aumento y evolución como los robos de información, virus, espionaje industrial, robos de identidad, spam, entre otros, llevados a cabo por hackers, dichos riesgos lógicos pueden mermar la confianza de los clientes y la reputación en el mercado (riesgo reputacional).

La información de la empresa es un bien o activo esencial que debe ser protegido de manera adecuada, esto es lo que se llama SI (seguridad de la información), si se llegase a perder la información contable de la organización, la base de datos de clientes, la información confidencial de clientes como información bancaria o los secretos comerciales, las consecuencias serían nefastas. (Instituto Nacional de Ciberseguridad [INCIBE], s.f.)

Si se quiere proteger a las organizaciones de todas las amenazas y riesgos a las que se ha visto que pueden ser vulnerables, se necesita identificarlos y confrontarlos de una forma acertada, razón por la cual que se deben poner en marcha unos procedimientos idóneos, que permitan llevar a cabo contramedidas de seguridad que se basen en una adecuada identificación y evaluación de los riesgos para el diseño de los controles necesarios y su respectiva medición de eficacia. Ahora bien, cuando nos referimos a un sistema de gestión de seguridad de la información (S.G.S.I.) basado en la norma ISO/IEC 27001, estamos hablando de una herramienta o metodología no compleja que todas las organizaciones pequeñas, medianas o grandes pueden llegar a implementar, al permitir esta norma la definición de las políticas, los procedimientos y los controles, se logran disminuir los riesgos.

Poner en marcha un S.G.S.I. requiere de la participación de cada uno de los niveles de una organización, comenzando desde la alta dirección, ya que, si no existe el compromiso de esta última, no es posible poner en funcionamiento dicho sistema. La alta dirección es la que se encarga de liderar el proceso completo, ya que sabe mejor que nadie y de primera mano, los riesgos de la empresa y las obligaciones que se tienen con los accionistas y clientes, de igual manera, es la única que puede encargarse de

introducir los cambios de tareas, de pensamiento y de procedimientos que se requieren para implementar un S.G.S.I.

Una vez identificados a manera general los riesgos y amenazas que tienen posibilidad afectar la información en las empresas de seguridad privada en Colombia, se propone avanzar al ámbito específico mediante la aplicación de la metodología que busca el mejoramiento de la seguridad cibernética asociada a las infraestructuras consideradas de carácter crítico, dicho marco de trabajo desarrollado por el Instituto Nacional de Estándares y Tecnología, también conocido como NIST.

El Marco proporciona un lenguaje común para comprender, gestionar y expresar el riesgo de seguridad cibernética para las partes interesadas internas y externas. Se puede utilizar para ayudar a identificar y priorizar acciones para reducir el riesgo de seguridad cibernética, y es una herramienta para alinear los enfoques de políticas, negocios y tecnología para manejar dicho riesgo. (Instituto Nacional de Estándares y Tecnología [NIST], 2018, p. 6)

Según el Instituto Nacional de Estándares y Tecnología NIST (2018), su metodología facilita la comprensión, la expresión y la gestión de los riesgos derivados o asociados a la seguridad en el ámbito cibernético, apoya además la identificación y priorización de los controles que permitan la reducción de dichos riesgos y la alineación a nivel estratégico y operacional necesaria para tal fin.

Aunque el marco del NIST fue diseñado teniendo en cuenta la infraestructura crítica cibernética, este es extremadamente versátil y puede aplicarse en organizaciones de todos los tamaños y sectores.

El NIST (2018), establece que este marco está compuesto por tres componentes principales: primero el núcleo de la metodología, segundo los niveles para su implementación y tercero los perfiles asociados a dicha metodología.

El núcleo de esta metodología consta de cinco objetivos simultáneos y continuos los cuales son: primero Identificar (ID), segundo Proteger (PR), tercero Detectar (DE), cuarto Responder (RS) y quinto Recuperar (RC), estas cinco funciones se ramifican en categorías, subcategorías y referencias informativas a otras normas y estándares de apoyo (NIST, 2018). Este núcleo del marco es el que se propone usar como herramienta metodológica para la identificación especifica de los riesgos y amenazas cibernéticas que pueden afectar la SI de las empresas de seguridad privada de manera previa y como complemento a la implementación del S.G.S.I.

En la figura 1 se puede observar la lista completa del núcleo del marco.

4.2. Componentes del S.G.S.I. ISO 27001.

Dando cumplimiento al segundo objetivo específico definido en este ensayo, se procede al estudio de los componentes mínimos necesarios para la implementación de un S.G.S.I. basado en la norma ISO IEC 27001, en complemento con el marco NIST.

Se puede decir que un S.G.S.I. es un instrumento que facilita el conocimiento, la gestión y reducción de los riesgos que puedan afectar la SI. Acorde con Romero, et al (2018), la función de la seguridad informática es la seguridad del medio informático, la informática ha de ser entendida como una ciencia que maneja los procesos, las técnicas y los métodos para el procesamiento, almacenamiento y trasmisión de la información, empero, el Ministerio de Tecnologías de la Información y las Comunicaciones [MINTIC] (2016), afirma, que no deben por ningún motivo confundirse las definiciones de seguridad

Identificador único de función	Función	Identificador único de categoría	Categoría
ID	Identificar	ID.AM	Gestión de activos
		ID.BE	Entorno empresarial
		ID.GV	Gobernanza
		ID.RA	Evaluación de riesgos
		ID.RM	Estrategia de gestión de riesgos
		ID.SC	Gestión del riesgo de la cadena de suministro
PR	Proteger	PR.AC	Gestión de identidad y control de acceso
		PR.AT	Conciencia y capacitación
		PR.DS	Seguridad de datos
		PR.IP	Procesos y procedimientos de protección de la información
		PR.MA	Mantenimiento
		PR.PT	Tecnología protectora
DE	Detectar	DE.AE	Anomalías y eventos
		DE.CM	Vigilancia continua de seguridad
		DE.DP	Procesos de detección
RS	Responder	RS.RP	Planificación de respuesta
		RS.CO	Comunicaciones
		RS.AN	Análisis
		RS.MI	Mitigación
		RS.IM	Mejoras
RC	Recuperar	RC.RP	Planificación de recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

Figura 1 - *Identificadores únicos de función y categoría*
Fuente: NIST (2018).

informática con seguridad de la información, ya que el primero sólo se encarga de la seguridad en el ámbito informático, pero la información como tal puede hallarse no solo en medios informáticos sino también en diferentes medios o formas como ya se ha descrito anteriormente.

Según el concepto de seguridad de la información de la Organización ISO expuesto en el párrafo cuatro correspondiente a la introducción del presente ensayo y los dos conceptos precedentes sobre seguridad informática, es importante dejar total claridad en la diferencia entre lo que es la seguridad informática y lo que es seguridad de la información, en primer lugar, la seguridad informática está orientada en la protección de las infraestructuras tecnológicas de la información y de la comunicación

que sostienen y dan grandes ventajas a los negocios, mientras que la seguridad de la información engloba la protección de los activos de información que son esenciales para el éxito de toda empresa, incluyendo a las infraestructuras, por ende, se puede entender que la seguridad informática es una parte o hace parte de la seguridad de la información.

Entre la gran cantidad de información que se puede manejar dentro de las empresas tenemos: las páginas web, los correos electrónicos (emails), las bases de datos, las imágenes, los contratos, los documentos, presentaciones, entre otros.

Según ISACA (2012) la SI busca garantizar que los flujos de información en las empresas cuentan con las medidas de protección que permitan evitar el acceso no autorizado, las vulneraciones a la integralidad y la no disposición cuando la información en requerida.

En el punto introductorio se hizo mención de un concepto sobre el cual la norma ISO/IEC 27001 es muy enfática y es la tríada de la seguridad compuesta por tres pilares fundamentales: primero, la confidencialidad, segundo, la integridad y tercero la disponibilidad, sobre los cuales se edifica la SI.

Cuando se trata de las empresas de seguridad privada, la confidencialidad de la información juega un papel fundamental y son pocas las empresas que se preocupan por ello; las empresas de vigilancia y seguridad privada manejan una gran cantidad de información, la cual ha de tener una adecuada gestión de la confidencialidad, como por ejemplo: los estudios de seguridad son documentos de carácter confidencial que deben tener restricciones adecuadas para su acceso y divulgación, ya que en ellos se muestran las vulnerabilidades de seguridad y sus posibles propuestas de solución, otro tema que requiere extremo cuidado en cuanto a confidencialidad dentro de las empresas de

vigilancia y seguridad privada es la gestión de los escoltas, en referencia a rutas de desplazamiento, horarios de cambios de turno, no divulgar características o detalles con nadie que no esté autorizado, mantener la confidencialidad de los clientes que hacen uso de los servicios de escoltas, entre otras.

El tema de la integridad de la información en la seguridad privada debe ser prioridad para cada una de las empresas de este sector, deben ser garantes de que la información que manejan tanto a nivel propio en sus procesos como a nivel de los servicios que prestan a sus clientes conserve la mayor fidelidad durante su ciclo de vida, es fundamental que cuando un cliente requiera información esta sea certera y precisa, sin desviaciones de manera que permita una adecuada toma de decisiones.

Las empresas de seguridad privada además de garantizar que tanto su información como la de los servicios que prestan a sus clientes sea de carácter confidencial según el caso, y de asegurar su total integridad y certeza, les resulta fundamental y obligatorio que dicha información esté accesible o disponible en el momento justo que se requiera, tanto para uso interno como a solicitud de los clientes, ya que si no se tiene una disponibilidad oportuna de la información, se pone en alto riesgo la toma de decisiones.

Es debido a todo lo anterior que estos tres conceptos: confidencialidad, integridad y disponibilidad, resultan ser los ejes funcionales de todo SGSI, tal como lo indica la norma ISO/IEC 27001, por lo que todas las empresas de vigilancia y seguridad privada en Colombia deben garantizar su cumplimiento para poder tener una adecuada gestión de la SI.

La norma internacional ISO IEC 27001, se ha desarrollado con la intención de poner a disposición los requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI; está dividida en 14 grupos, 114 controles y en sus objetivos de control, de manera que en el siguiente capítulo se discutirán y profundizarán los conceptos mínimos más importantes enfocados a la seguridad privada, la norma además, posee una sección adicional sobre la subcontratación en cuanto a tercerización de servicios.

4.3. Modelo del S.G.S.I. para empresas de seguridad privada en Colombia

Teniendo en cuenta en el tercer objetivo específico de este ensayo académico, se propone un modelo de S.G.S.I. con base en la Norma ISO 2700, como aporte para su fácil implementación inicial en las organizaciones que dedican sus operaciones a la vigilancia y seguridad privada en Colombia.

Una vez se han sentado las bases fundamentales y se ha profundizado en la importancia de la seguridad de la información en la actualidad para cualquier empresa y más aún las del sector de la vigilancia y seguridad privada que gestionan información de gran importancia y confidencialidad para cada uno de sus clientes, es necesario promover y difundir este modelo para que cada vez más empresas de este sector puedan garantizar la triada de la seguridad y así aumentar la protección de ese activo tan relevante como lo es la información. Dicho modelo presenta la siguiente estructuración:

4.3.1. Contexto de la organización

4.3.1.1. Comprensión de la organización y de su contexto

Es necesario establecer todo lo referente al entorno externo e interno que son convenientes para el objetivo principal de la organización y que impactan directamente

en la posibilidad de llegar a cumplir los propósitos previstos del S.G.S.I (Organización Internacional de Normalización [ISO], 2017). Para esto se sugiere aplicar análisis PESTAL y Matriz DOFA.

4.3.1.2. Entendimiento de las necesidades y expectativas de las partes interesadas

Es importante que la organización determine las partes interesadas que son relevantes para el SGSI, y aquellos requisitos que estas tengan que sean fundamentales para la SI, estos pueden ser: de naturaleza legal, regulatorios o contractuales. (Organización Internacional de Normalización [ISO], 2017).

4.3.1.3. Definición del alcance del SGSI

Es trascendental precisar tanto los límites como la aplicabilidad del S.G.S.I., con el fin de entender que alcance puede llegar a tener, dicho alcance debe quedar disponible como información documentada, se ha de considerar: primero, las cuestiones externas e internas identificadas en la parte 4.3.1.1, segundo, los requisitos de las partes interesadas determinados en la parte 4.3.1.2, tercero, la interfaz y la dependencia existente entre las actividades llevadas a cabo por la organización y las que realizan otras organizaciones. (Organización Internacional de Normalización [ISO], 2017).

4.3.2. Liderazgo (alta dirección)

4.3.2.1. Liderazgo y compromiso

La alta dirección debe evidenciar su liderazgo y su compromiso con el S.G.S.I de la siguiente manera: primero, ha de establecer una política y unos objetivos de SI que sean acordes con la dirección estratégica de la empresa; segundo, ha de asegurar que los requisitos del S.G.S.I. estén acoplados en los procesos de la organización, tercero,

ha de salvaguardar los recursos requeridos para el S.G.S.I. y su disponibilidad, cuarto, ha de comunicar la relevancia que tiene una correcta gestión de la SI de manera eficaz y de conformidad con los requerimientos del S.G.S.I., quinto, ha de direccionar y respaldar las personas, sexto, ha de contribuir al desarrollo eficaz y estimular la mejora continua del S.G.S.I. y además ha de apoyar cualquier otra función pertinente de la dirección. (Organización Internacional de Normalización [ISO], 2017).

4.3.2.2. Política

Una política de SI debe tener en cuenta lo siguiente: primero, debe ajustarse al propósito esencial de la organización, segundo, debe incluir los objetivos o como mínimo proporcionar un marco que sirva de referencia para poder precisar los objetivos de SI, tercero, debe incluir un pacto de cumplimiento de aquellos requerimientos que pueden aplicarse a la SI, cuarto, debe incluir el compromiso de un mejoramiento continuo del S.G.S.I, quinto, debe estar accesible como información documentada y para las partes interesadas, y sexto, debe ser comunicada oportunamente al interior de la empresa. (Organización Internacional de Normalización [ISO], 2017).

4.3.2.3. Autoridades, roles y responsabilidades en la empresa

La asignación y comunicación de los roles, las responsabilidades y autoridades ha de hacerse para: garantizar que el S.G.S.I. esta en consonancia con los requerimientos de la norma ISO-27001 manteniendo al tanto a la alta dirección sobre el desenvolvimiento del mismo (Organización Internacional de Normalización [ISO], 2017).

4.3.3. Planificación

4.3.3.1. Acciones para tratar los riesgos y oportunidades

La determinación de los riesgos y las oportunidades que se deben tratar se hace para: primero, garantizar que el S.G.S.I. logre los resultados propuestos, segundo, prevenir efectos no deseados; tercero, lograr la mejora continua, cuarto, planificar las acciones tendientes a manejar dichos riesgos y oportunidades, buscando la integración e implementación de estas en los procesos del S.G.S.I., con el fin de evaluar su eficacia. (Organización Internacional de Normalización [ISO], 2017).

Para llevar a cabo lo anterior, se requieren dos fases: en la primera fase se define y aplica un método de apreciación de riesgos de SI que permita la identificación, el análisis y la evaluación de los riesgos de SI, este proceso de apreciación de los riesgos debe conservarse como información documentada (Organización Internacional de Normalización [ISO], 2017).

En la segunda fase se establece y efectúa un procedimiento para tratar los riesgos de SI, para ello se debe: primero, realizar la selección de las opciones más apropiadas para el tratamiento de los riesgos de SI y segundo, hacer la determinación de los controles que se requieran para una correcta ejecución de la(s) opción(es) elegida(s) de tratamiento de riesgos de SI, en este punto, la norma ISO-27001 suministra en su Anexo A una lista de 114 controles con sus respectivos objetivos de control, de los cuales se deben seleccionar los necesarios de acuerdo a la dimensión y las características propias de la organización. Adicionalmente, se debe elaborar una “Declaración de Aplicabilidad” que contenga: los controles requeridos que fueron elegidos, la explicación de las inclusiones, si los controles necesarios están implementados o no, y la explicación de las exclusiones de cualquiera de los controles del anexo A (Organización Internacional de

Normalización [ISO], 2017). De igual manera el proceso de tratamiento de riesgos ha de salvaguardarse como información documentada.

Para las fases de apreciación y tratamiento de riesgos se sugiere consultar el Marco NIST referenciado en el apartado 4.1 de este ensayo, además de la norma ISO-31000.

4.3.3.2. Objetivos de la SI y planificación para su logro

Los objetivos de seguridad de la información deben: primero, establecerse en las funciones y niveles adecuados, segundo, ser congruentes con la política de SI, tercero, ser mensurables en lo posible, cuarto, ser comunicados, quinto, ser actualizados y sexto, considerar los requisitos de SI aplicables y los resultados de la apreciación y del tratamiento de los riesgos. (Organización Internacional de Normalización [ISO], 2017).

4.3.4. Soporte

4.3.4.1. Recursos

La organización es la encargada de establecer y suministrar los recursos que se necesiten para establecer, implementar, mantener y mejorar de manera constante el S.G.S.I (Organización Internacional de Normalización [ISO], 2017).

4.3.4.2. Competencia

Es necesario precisar la competencia de las personas, que, de manera controlada, realizan alguna función que afecte cómo se desenvuelven en SI; estás personas no solo deben contar con experiencia, formación o educación, sino que además deben tener la aptitud para realizar las acciones qué se requieran con el fin de adquirir la competencia necesaria, pudiendo evaluar la eficacia de las mismas. (Organización Internacional de Normalización [ISO], 2017)

4.3.4.3. Concienciación

Se requiere que las personas que realizan sus funciones de manera controlada dentro de la organización, tengan conciencia de la política de la SI, de su aporte a la eficacia del S.G.S.I, de los beneficios que puede traer consigo el mejoramiento del desempeño en SI y de las consecuencias de no cumplir con los requerimientos que están dispuestos para el S.G.S.I. (Organización Internacional de Normalización [ISO], 2017).

4.3.4.4. Comunicación

La determinación de la necesidad de comunicaciones adecuadas al S.G.S.I, tanto internas como externas, es fundamental. (Organización Internacional de Normalización [ISO], 2017).

4.3.4.5. Información documentada

El S.G.S.I. debe incluir la información documentada que se ha mencionado en cada apartado específico, para esta debe garantizarse su elaboración, actualización y control (Organización Internacional de Normalización [ISO], 2017).

4.3.5. Operación

4.3.5.1. Planificación y control operacional

Se necesita la planificación, implementación y control de los procesos que se requieran para llevar a cabo los requisitos de SI y para ejecutar todas las acciones tendientes al manejo de los riesgos y oportunidades; además, deben ponerse en marcha los planes trazados para poder lograr los objetivos de SI y en la medida en que se necesite, debe mantenerse toda la información documentada, con el fin de garantizar que los procesos realizados se ejecutaron conforme a lo planificado. (Organización Internacional de Normalización [ISO], 2017).

4.3.5.2. Apreciación de los riesgos de seguridad de la información

Se debe realizar las apreciaciones de riesgos de SI no solo en los intervalos que hayan sido planeados, sino también cuando se produzcan cambios importantes, además debe conservar documentación de este punto (Organización Internacional de Normalización [ISO], 2017).

4.3.5.3. Tratamiento de los riesgos de seguridad de la información

Es necesario llevar a cabo el plan de tratamiento de los riesgos de SI y mantener documentación al respecto (Organización Internacional de Normalización [ISO], 2017).

4.3.6. Evaluación

Se debe realizar el seguimiento, la medición, el análisis y la evaluación del rendimiento de la SI y la eficacia del S.G.S.I., de igual forma, han de realizarse auditorías internas según los intervalos planeados, para verificar si el S.G.S.I. cumple los requerimientos intrínsecos de la organización y con los requisitos dispuestos en la norma ISO-27001, para lo cual se recomienda consultar la norma ISO-19011, además, la alta dirección tiene el deber de supervisar el S.G.S.I. a intervalos planificados, con el fin de revisar que sea conveniente, adecuado y eficaz. (Organización Internacional de Normalización [ISO], 2017).

4.3.7. Mejora

4.3.7.1. No conformidades y acciones de corrección

Si sucediese una no conformidad, dependiendo del caso, la organización debe hacerle frente, implementando las acciones necesarias para controlarla, corregirla y enfrentar sus efectos, igualmente, se requiere que la organización evalúe si es necesario la implementación de acciones tendientes a suprimir las causas originarias de la no

conformidad, ello para que a futuro está no vuelva a suceder. (Organización Internacional de Normalización [ISO], 2017).

4.3.7.2. Mejora continua

"La organización debe mejorar de manera continua la idoneidad, adecuación y eficacia del sistema de gestión de la seguridad de la información" (Organización Internacional de Normalización [ISO], 2017).

5. Conclusiones

Para terminar, se concluye dando respuesta al objetivo general planteado en este ensayo académico cuyos resultados son:

La política, los objetivos y las actividades de SI deben estar en conformidad con los objetivos de la organización.

El Sistema de gestión de seguridad de la información S.G.S.I. comprende todos aquellos recursos, guías, actividades, políticas y procedimientos asociados para que las empresas puedan garantizar la seguridad de su valiosa información.

Un S.G.S.I. requiere un soporte notorio en todos los niveles de la organización, principalmente de la alta gerencia, pues en esta última, debe existir un compromiso claro, de modo que toda la organización pueda darse cuenta de que desde la alta dirección están interesados y apoyando la implantación del S.G.S.I.

Para que un S.G.S.I. tenga éxito, debe existir unos programas efectivos de concienciación, formación y capacitación de los empleados en términos de seguridad, siendo necesario que cada uno entienda la importancia de su trabajo dentro de la empresa y como puede influir en la seguridad, además, debido a que los empleados

pueden ser el eslabón más débil de la cadena, su formación y capacitación debe ser continua y mantenerse actualizada a los nuevos requerimientos de la empresa.

La mejora continua es fundamental en el S.G.S.I., este debe ser un proceso iterativo e incremental, según la evolución y crecimiento de la organización.

El S.G.S.I. aumenta la confianza de todas las partes interesadas en la organización y ayuda a la gestión eficaz de los recursos invertidos en seguridad de la información.

Un S.G.S.I. incorpora la apreciación y tratamiento de los riesgos de seguridad de la información, reduciendo su posible materialización mediante la implementación de controles y objetivos de control según la norma ISO 27001.

Otro de los factores críticos para el éxito de un S.G.S.I. es realizar una gestión eficaz de los incidentes de SI, recordar que un incidente de este tipo es aquel que puede interrumpir cualquiera de los elementos de la tríada de seguridad confidencialidad, integridad o disponibilidad, por tanto, el proceso de gestión debe ser eficaz en cuanto a la identificación, la atención y la resolución de dichos incidentes, de manera que el impacto sea el menor posible.

El S.G.S.I. no debe verse como un simple sistema en papel o para obtener una certificación y luego olvidarlo, SI debe ser parte de la cultura empresarial hoy más que nunca.

6. Referencias

Cohen, D., & Asín, E. (2000). *Sistemas de información para los negocios* (3 ed.). México: McGRAW-HILL/INTERAMERICANA EDITORES S.A.

Consejo Nacional de Política Económica y Social [CONPES]. (2016). *Documento CONPES 3854 POLÍTICA NACIONAL DE SEGURIDAD DIGITAL.* Bogotá, Colombia.

Instituto Nacional de Ciberseguridad [INCIBE]. (17 de 08 de 2015). *Desde entonces hasta ahora…y lo que nos queda por ver en Seguridad de la Información*. Obtenido de https://www.incibe.es/protege-tu-empresa/blog/entonces-ahora-seguridad-informacion

Instituto Nacional de Ciberseguridad [INCIBE]. (2015). *Gestión de riesgos. Una guía de aproximación para el empresario.* España. Obtenido de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf

Instituto Nacional de Ciberseguridad [INCIBE]. (s.f.). *Protección de la información.* España. Obtenido de https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

Instituto Nacional de Estándares y Tecnología [NIST]. (2018). *Marco para la mejora de la seguridad cibernética en infraestructuras críticas.* Estados Unidos. Obtenido de https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf

ISACA. (2012). *COBIT 5 para seguridad de la información.* Estados Unidos.

Laudon, K., & Laudon, J. (2012). *Sistemas de información gerencial* (12 ed.). México: Pearson Educación de México, S.A.

Ministerio de Tecnologías de la Información y las Comunicaciones [MINTIC]. (2016). *Guía para la Implementación de Seguridad de la Información en una MIPYME.* Obtenido de https://mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

Organización Internacional de Normalización [ISO]. (2006). *NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001 TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). REQUISITOS.* Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

Organización Internacional de Normalización [ISO]. (2017). *Norma Española UNE-EN ISO/IEC 27001 Tecnología de la información, Técnicas de seguridad, Sistemas de Gestión de la Seguridad de la Información, Requisitos.* España: AENOR. Obtenido de https://www.eoi.es/es/file/166057/download?token=k6tPtilN

Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., Álava, C., . . . Castillo, M. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.* España: 3 Ciencias Área de Innovación y Desarrollo,S.L. Obtenido de https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf