IMPORTANCIA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) Y SU INCIDENCIA EN MATERIA DE CONTROL INTERNO

Karen Andrea Mogollón Jimenez

Código: 2501210

Universidad Militar Nueva Granada

Facultad de Ciencias Económicas

Dirección de Posgrados

Especialización en Control Interno

Bogotá D.C.

2022

Tabla de contenido

1. Resumen

Actualmente, las tecnologías de la información y comunicación (TIC) representan un apoyo fundamental en materia de progreso y sostenibilidad al interior de las empresas. Este recurso estratégico no solo aporta valor en la mejora de la prestación de servicios y ejecución de procesos internos, sino que actúa como una herramienta que a través de un uso sistematizado, provee seguridad a la información que genera día a día una empresa. Un sistema de gestión de seguridad de la información (SGSI) representa un apoyo en la aplicación y ejecución de todos los procesos relacionados con la generación, almacenamiento y disposición de información. Siendo el aseguramiento de la oportunidad y confiabilidad de los registros de la información, uno de los propósitos del control interno, la importancia del optimo tratamiento de la información se verá reflejada en este análisis conceptual de los aspectos fundamentales y estándares internacionales relacionados tales como: La norma ISO/IEC 27001, El modelo COBIT y el modelo ITIL. Esto, con el propósito de identificar los lineamientos que logran un nivel de seguridad de la información aceptable, en donde las posibilidades de que se materialice alguna amenaza sean mínimas y así se preserve de la mejor manera la administración y control de la información de las organizaciones sin importar si su naturaleza es pública o privada.

1.1 Palabras clave: Información, seguridad, gestión, control, sistemas, partes interesadas, objetivos, oportunidad.

2. Abstract

Currently, information and communication technologies (ICT) represent a fundamental support in terms of progress and sustainability within companies. This strategic resource not only adds value in improving the provision of services and execution of internal processes, but also acts as a tool that, through systematic use, provides security to the information generated by a company on a daily basis. An information security management system (SGSI) represents support in the application and execution of all processes related to the generation, storage and provision of information. Being the assurance of timeliness and reliability of information records, one of the purposes of internal control, the importance of optimal treatment of information will be reflected in this conceptual analysis of the fundamental aspects and related international standards such as: ISO/IEC 27001 standard, the COBIT model and the ITIL model. This, with the purpose of identifying the guidelines that achieve an acceptable level of information security, where the chances of any threat materializing are minimal and thus the administration and control of information of organizations is preserved in the best way. regardless of whether its nature is public or private.

2.1 Keywords: Information, Security, Management, Control, Systems, Strackeholders, Objectives, Opportunity.

3. Introducción

Las tecnologías de información (TI) como recursos técnicos en hardware y software, los sistemas de información (SI) como un conjunto formal de labores y las tecnologías de la información y comunicación (TIC) las cuales soportan dichas tareas relacionadas con la emisión, acceso y tratamiento de datos. Al integrar en conjunto sus componentes relacionados (Información, equipamiento, el factor humano, la infraestructura, los mecanismos de intercambio de información, políticas, regulaciones y los recursos financieros) han facilitado la automatización de los procesos internos, creación de ventajas competitivas, suministro de información integral para la toma de decisiones y han proveído la diligencia necesaria para identificar y atender retos, y estar en línea con las tendencias que exige un mercado tan dinámico en la actualidad.

Para atender dicha exigencia, las organizaciones han tenido la necesidad de implementar nuevas estrategias y procesos de gobierno recurriendo a los modelos y estándares internacionales en materia de seguridad de la información. Estos, brindan un marco de referencia que le permite a las empresas lograr sus objetivos con base en la implantación de procesos de control y gestión de las TI, todo esto, alineando sus objetivos de TI con los objetivos generales de la organización.

Al fortalecer la interacción de las unidades de negocio y sus intereses respecto a las tecnologías de información, se crea una cadena de valor, al ser un método que les permite a los directivos y todas las partes interesadas, comunicarse y cerrar la brecha que ha existido entre la necesidad de control y los riesgos de operación, ya que se establecen políticas claras y mejores prácticas de control de TI de forma global.

Es por esto, que el SGSI pretende suministrar un marco de trabajo basado en las buenas prácticas para el sector público o privado y propuestas que faciliten la gestión de estos procesos y evitar la fuga de información. Por lo anterior, se pretende mostrar la importancia y los múltiples beneficios que brinda un SGSI, diseñado bajo estándares internacionales y modelos de control que han sido adoptados por gran parte de las empresas interesadas en la protección de su información. Además, se pretende sustentar el papel fundamental que juega en las labores de control interno y su aporte al mejoramiento continuo de los procesos en las organizaciones.

4. Pregunta de investigación: ¿Cuál es la importancia del sistema de gestión de seguridad de la información y su incidencia en materia de control interno al interior de una organización?

5. Justificación

Siendo la integridad una característica fundamental de la información, se requiere que la misma sea confiable, pues en ella se fundamenta la toma de decisiones. La información se convierte en un factor muy sensible, ya que representa la realidad de una organización con sus ventajas y desventajas. Es por esto, que es elemental que se aseguren a través de mecanismos de control, los procesos y se monitoreen constantemente los posibles riesgos internos y externos que puedan afectar la calidad de la información y divulgación de resultados, procedimientos y toma de decisiones diariamente; garantizando el cumplimiento de las tres variables fundamentales en las cuales versa este sistema: Confidencialidad, integridad y disponibilidad. A través del presente documento se pretende identificar la importancia de un SGSI y su papel en materia de Control interno.

6. Objetivos

6.1 Objetivo general

Identificar la importancia de la administración de información a través de un sistema de gestión de seguridad de la información (SGSI) y su papel en la ejecución del control interno.

6.2 Objetivos específicos

- Realizar un análisis conceptual sobre el SGSI con sus precedentes y aspectos fundamentales en la actualidad.
- Identificar estándares internacionales establecidos en materia de seguridad y tratamiento de la información.
- Justificar la importancia de la implantación y aplicación de un SGSI en las organizaciones a través de su contribución al control interno.

7. Metodología

La metodología utilizada para la elaboración de este ensayo científico será la aplicación de un método cualitativo con el cual se recopilarán diferentes apreciaciones teóricas e identificarán directrices normativas relacionadas con el tema en materia, los cuales perimirán establecer una apreciación para justificar la importancia del SGSI y su papel en las labores relacionadas al control interno al interior de una organización.

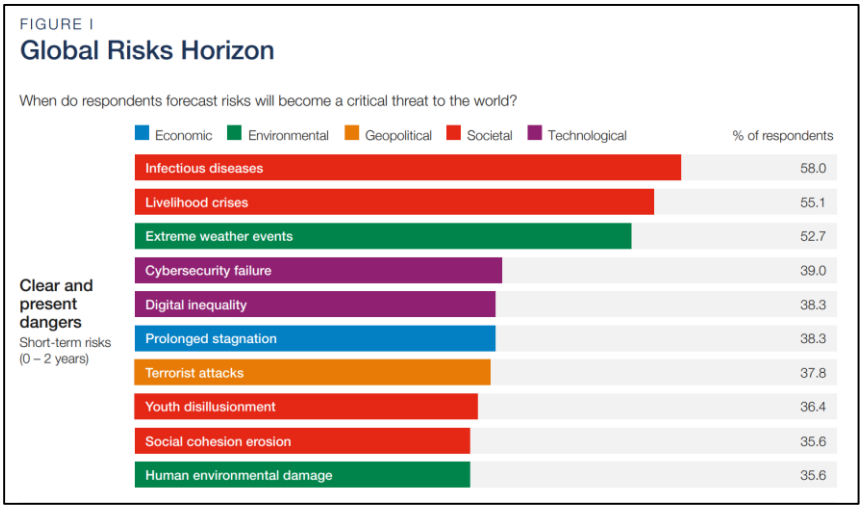
8. La seguridad de la información y sus antecedentes en Colombia

En un mundo globalizado la interconexión a través de redes de datos está presente de manera permanente en el estilo de vida en la mayor parte de los individuos. En materia corporativa, sin importar la naturaleza de la organización ya sea pública o privada, el tratamiento de información a través de herramientas o aplicaciones tecnológicas y digitales, soporta gran parte de su gestión y coopera en la realización de sus objetivos o misión institucional. Es por esto que una organización debe adoptar medidas que permitan limitar el riesgo de una mayor superficie de ataque de sus canales de acceso a la producción de datos y los canales de comunicación de los mismos.

Los más grandes retos relacionados con seguridad de la información conocidos actualmente son los ataques de bases de datos, fraudes y filtración de la información. Recientemente, la pandemia por COVID-19 recrudeció la interacción y comunicación presencial, surgió entonces la necesidad de identificar las alternativas que nos permitieran seguir comunicados y conectados. Esto, provocó el aumento magistral, despliegue y consumo de tecnología, lo que implicó una penetración mucho más rápida de la ola tecnológica en los mercados. Por esto, así mismo se agudizaron los riesgos y vulnerabilidades relacionados con seguridad de la información.

Según el informe de riesgos globales emitido por (The World Economic Forum, 2021) en alianza con la firma MarshMCLennan, el fallo de ciberseguridad se encuentra entre los 5 riesgos que se han convertido en una amenaza crítica para el mundo.

Figura 1. *Horizonte de riesgos globales*



Nota. La figura expone el peso porcentual de los riesgos más influyentes en materia de seguridad durante el año 2021. Fuente: (The World Economic Forum, 2021)

Este riesgo es particularmente importante para la región de América Latina y el Caribe, ya que en los últimos años ha sido un territorio de enorme expansión en el uso de las TIC. A medida que la región progresa a pasos agigantados hacia la economía digital, viene creciendo la necesidad de garantizar una mayor seguridad de los procesos relacionados. Los esfuerzos orientados a una gestión del riesgo en materia de seguridad digital y protección de la privacidad representan una responsabilidad compartida entre el gobierno, el sector privado y los individuos que participan en un ambiente económico que está cada vez más soportado por en las fuentes de datos digitales. Por esto, surge la Propuesta de Agenda Digital para América Latina y el Caribe (eLAC2022), cuyo objetivo establecido es el de ser un instrumento que promueva el diseño de políticas e investigación en función de los retos y oportunidades que implica la transformación digital de la sociedad actual y su economía (CEPAL, 2020).

En Colombia, a través de los documentos Conpes 3701 de 2011 y 3854 de 2016 (CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, 2016) se adoptaron políticas en materia de ciberseguridad, cuyo propósito más reciente compartió el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC, 2016) es el de fortalecer las capacidades de los stakeholders para identificar, gestionar y mitigar los riesgos asociados a la seguridad digital.

Dentro de las políticas de gestión y desempeño, el gobierno nacional por primera vez incluyó la política de seguridad digital adherida a la operación estratégica de las entidades públicas y privadas. Simultáneamente, el MINTIC tiene implementado a nivel nacional el modelo de seguridad y privacidad de la información (MSPI) para apoyar la gestión e implementación de buenas prácticas y estándares que protejan la información, infraestructura tecnológica y sistemas de información y comunicaciones. Recientemente el presidente de la república profirió la directiva presidencial 02 de 2022, donde reitera la política pública en materia de seguridad digital, allí expone los 19 lineamentos fundamentales debe adoptar una entidad pública que garantice la implementación y desarrollo seguro de la política de gobierno digital (Transformación digital del Estado).

Pese a que el Gobierno Nacional ha instaurado este tipo de medidas que fortalecen la seguridad de la información, el sector privado (en particular las pymes) tiene grandes retos para estar preparado ante las constantes amenazas que se presentan, puesto que en la mayoría de casos no disponen de recursos suficientes para fortalecer su cultura de seguridad.

8.1 Ámbito organizacional

En la actualidad, la necesidad de diseñar políticas en materia de seguridad de la información en las organizaciones públicas o privadas ha tenido mayor un protagonismo impulsado por la percepción de inseguridad que crece día a día, así como las nuevas consideraciones normativas en la materia.

Esto ha sido fundamental para que los gerentes y las juntas directivas comprendan de una manera más sencilla los riesgos en materia tecnológica, asociados a su modelo de operación y logren un equilibrio entre proteger la seguridad de sus activos, evitar pérdidas y mantener una rentabilidad en un ambiente tan competitivo. Una mayor conciencia en el liderazgo empresarial y promoción de la higiene básica de seguridad cibernética se convierte aspecto mandatorio en la toma de decisiones para una mejor planificación de la seguridad de la información, mecanismos de ayuda, planes de contingencia y proyectos asociados.

9. La información como uno de los activos más importantes para las empresas

La información de una organización es todo lo que se utiliza para reflejar la situación de su contexto interno y externo, el estado actual de sus objetivos con los resultados asociados que permitan establecer un panorama o varios para la toma de decisiones. Por esto, las organizaciones necesitan contar con un proceso de gestión de información especifico que les permita procesar, organizar y almacenar la información y que así mismo garantice su disponibilidad y recuperación. Entendiendo la gestión de información como un conjunto de actividades orientadas al control, almacenamiento y recuperación de la información que cualquier empresa produzca.

Es importante que previo a la implementación de un SGSI, todos los activos de información sean claramente identificados y también inventariados, existen estándares internacionales que establecen una clasificación sugerida, expuesta a continuación:

Figura 2. *Clasificación sugerida de los activos de información*

Activos de informacion pura	
Datos Digitales	Bases de datos
	Unidades lógicas
	Copias de seguridad
Activos Tangibles	Personales
	Financieros
	Legales
Activos Intangibles	Conocimiento
	Relaciones
	Secretos Comerciales
Software de aplicación	Propietario desarrollo por la organización
	Herramientas de bases de datos
	Aplicaciones de comercio electrónico
	Middleware
Sistemas operativos	Servidores
	Dispositivos de red
	Dispositivos de mano e incrustados
Activos fisicos	
Infraestructura de TI	Edificios
	Centros de datos
	Habitaciones de equipos y servidores
Controles de entorno de TI	Equipos de alarma
	Supresión contra incendio
	Sistemas de alimentación ininterrumpida
Hardware de TI	Dispositivos de almacenamiento
	Ordenadores de mesa
	Estaciones de trabajo
	Ordenadores portátiles
Activos de servicios de TI	Servicios de autenticación de usuario
	Administración de procesos
	Enlaces
Activos Humanos	
Empleados	Personal y directivos
	Participar los que tienen roles de gestión como altos cargos
	Arquitectos de software y desarrolladores
	auditores
Externos	Trabajadores temporales
	Consultores externos
	Asesores especialistas

Nota. Elaboración propia sobre la fuente de información (ISOTools Excellence, 2017)

10. El sistema de gestión de seguridad de la información

Un SGSI se define como un conjunto de prácticas encaminadas a garantizar la integridad, seguridad y confidencialidad de la información de las organizaciones (ISO Tools, 2016). Al ser un grupo de datos que aportan valor a las organizaciones, recopila los criterios más relevantes para la evaluación de los riesgos asociados a la administración de la información independientemente del área o sector donde se desenvuelva.

Un SGSI está basado en la preservación de tres principios fundamentales: Confidencialidad, integridad y disponibilidad. Grupo también conocido como Triada CID, definidos a continuación:

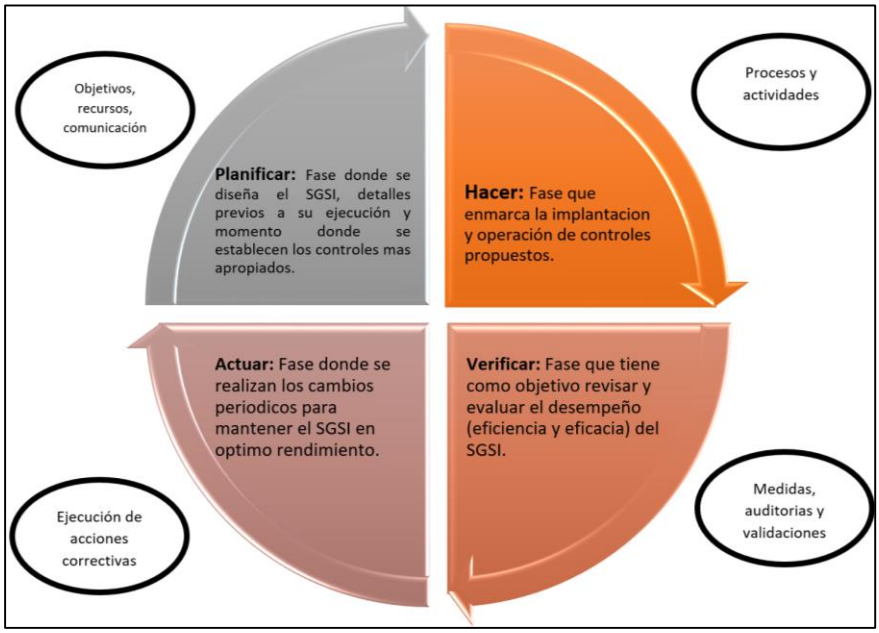
Confidencialidad: La información sensible solo debe estar al alcance de los usuarios autorizados, evitando la desviación y uso inapropiado de la misma.

Integridad: La información debe ser correcta y completa. Se debe garantizar que no se permitan modificaciones de datos por personas no autorizadas.

Disponibilidad: La información tiene que ser accesible de forma oportuna para los usuarios autorizados.

Para lograr la preservación de la información se debe establecer, desarrollar y perfeccionar un SGSI, el cual se ejecuta según el enfoque de mejora continua más conocido como Ciclo Deming concebido así:

Figura 3. *Ciclo Deming, método de mejor continua.*



Nota. Elaboración propia

11. ISO/IEC 27001

La serie de normas ISO/IEC 27000 proferidas por el International Organization for Standardization y el International Electrotechnical Commission (20 guías), son un conjunto de buenas prácticas relacionadas a la implantación, mantenimiento y gestión de un SGSI orientadas, a la mejora continua del sistema y mitigación de riesgos.

La ISO/IEC 27001 es la única norma certificable de la familia la cual según (ICONTEC, 2022) permite el control y la gestión de los riesgos para las cuales la información y la tecnología son uno de los activos importantes. Mediante la implementación de mejores prácticas de seguridad de la información, las empresas que certifican su SGSI demuestran ante sus stakeholders la debida diligencia en la ejecución de esfuerzos en materia de seguridad.

La norma se basa en el ciclo Deming (PDCA) anteriormente mencionado, donde establecen las actividades relacionadas con la implantación y gestión en una organización del SGSI, su estructura contempla 10 secciones: Objeto y campo de aplicación, normativa, definiciones, contexto de la empresa, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora.

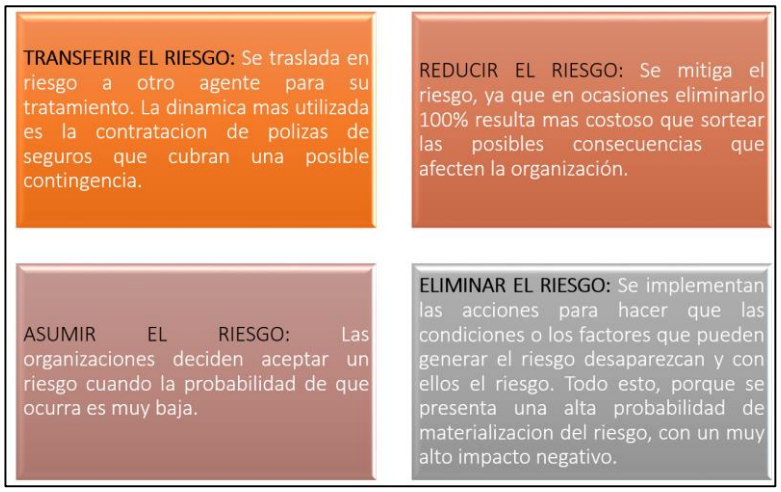
Lo anterior, se soporta en varios procesos de control los cuales permiten el monitoreo oportuno del desempeño del SGSI en una empresa.

Actualmente, las organizaciones sortean diariamente riesgos asociados a la seguridad de sus datos y a tecnología emergente. Es por esto, que la norma ISO 27001 establece el marco de referencia para evaluar los riesgos, establecer controles y diseñar estrategias que permitan suministrar protección a todos sus flujos de información. Es pertinente aclarar que, si bien la certificación en ISO 27001 aumenta el grado de confianza de las organizaciones frente al manejo de su información, los riesgos son inherentes, en un mundo tan dinámico no existe un blindaje total.

12. Riesgos

Es importante definir políticas relacionadas con el tratamiento del riesgo en función de la probabilidad de que las amenazas propias de los activos de la información se materialicen y provoquen un daño parcial o total de estos activos. Todo lo anterior, debe estar alineado con la triada CID. Los esfuerzos de las organizaciones deben estar encaminados a:

Figura 4. Tratamiento de riesgos



Nota. elaboración propia

Entre los riesgos asociados más conocidos en materia de seguridad de información están:

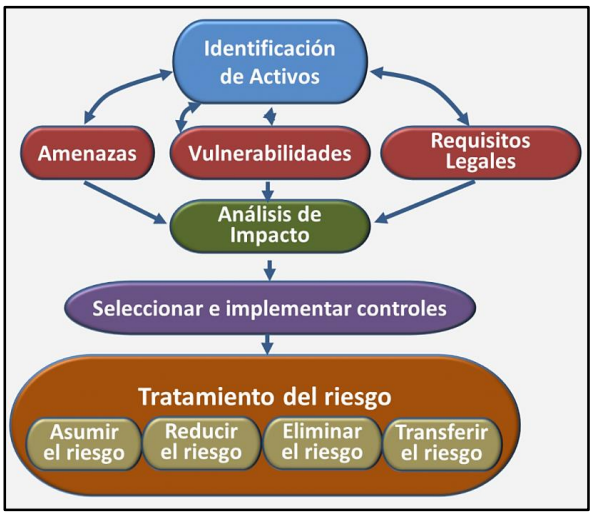
Tabla 1. *Riesgos asociados a un SGSI*

1. Permisos de administrador en los dispositivos electrónicos.
2. Correos maliciosos o no deseados.
3. No realizar copias de seguridad.
4. Uso de contraseñas.
5. Uso de aplicaciones de almacenamiento on-line.

Nota. Elaboración propia sobre la base de información de (ISO Tools, 2016)

En el momento de implantar un SGSI según esta norma ISO, se considera como eje principal la evaluación de riesgos**.** Esto, permitirá a la dirección de la empresa tener una visión que le permita definir el alcance, políticas y medidas a implantar, soportándose en el ciclo PHVA, común para todas estas normas ISO.

Figura 5. Método de Evaluación y Tratamiento del Riesgo



Nota. Ciclo de mejora continua propuesto para un SGSI, Fuente (NORMAS-ISO .COM, s.f.)

Pasos:

- Identificar Activos de Información y responsables.
- Identificar Vulnerabilidades de cada activo (aquellas susceptibles de sufrir ataques o daños).
- Identificar amenazas: Todo aspecto o situación que represente peligro frente a los activos de la información.
- Identificar requisitos legales y contractuales que tiene la organización.
- Identificar riesgos: Definir la probabilidad de que las amenazas puedan causar un daño total o parcial al activo de la información.
- Cálculo de riesgo: probabilidad de ocurrencia e impacto.
- Plan de tratamiento del riesgo: Definición de la política de tratamiento de los riesgos en con base en los aspectos anteriores. Estas políticas están orientadas para asumir, reducir, eliminar o transferir el riesgo.

13. Modelo COBIT

Este modelo de objetivos de control para TI, establece un conglomerado de mejores prácticas para la gestión de los sistemas de Información de las empresas. Su objetivo está enfocado más al control que a la ejecución misma, el cual es básicamente administrar la aplicación de TI en las empresas, presentando las actividades que se interrelacionan entre si de una manera manejable y lógica.

En su más reciente versión número 5 del año 2012, las TIC son protagonistas en la creación de valor para las organizaciones. Esto, soportado a través de un modelo con 5 principios:

1. Satisfacer las necesidades de los stakeholders: aumento de su rendimiento y alcance de objetivos.
2. Cubrir la empresa de manera integral: Partiendo de una perspectiva global, se cubren las necesidades corporativas.
3. Aplicar un solo marco integrado: Este modelo considera los mejores marcos de asociación de auditoría y control de sistemas de información orientados a encontrar un balance entre los riesgos identificados con los beneficios buscados.
4. Habilitar un enfoque integral: La propuesta del modelo, está diseñada para que el gobierno de TI y su administración, operen alineadas con los objetivos generales del negocio.
5. Separar el Gobierno de la Administración: El modelo diferencia el campo de acción del gobierno de TI (Evalúa, dirige, monitorea) y la gestión de tecnologías de la información (planifica, construye, ejecuta y monitorea). (Universidad ESAN, 2016)

Se puede establecer que las tecnologías de información y comunicación son un aspecto fundamental que permite para manejar las transacciones y su información. Estas actividades cada vez son más dinámicas y requieren de la unión de distintas fuerzas para ser efectivas.

Este modelo está estructurado en 34 procesos agrupados en 4 dominios:

1. **Planificación y organización:** Aprovechamiento de las TI para la consecución de objetivos.
2. **Adquisición e Implementación:** Implantación de nuevas tecnologías asociadas con los procesos de la empresa.
3. **Entrega y soporte:** efectividad y eficiencia de los sistemas tecnológicos
4. **Monitoreo:** Vigilancia a las soluciones estratégicas que han sido implantadas a raíz de las necesidades cambiantes de la organización.

El modelo COBIT ofrece un marco que permite respaldar las decisiones, generando cadenas de valor, teniendo en cuenta las necesidades y expectativas de los stackeholders. A través del modelo, se alinea la seguridad de la información con los objetivos del negocio.

14. Modelo ITIL

Este modelo, comprende una serie de documentos que exponen recomendaciones y mejores prácticas para la gestión de los servicios de TI. Este, se utiliza como un marco de referencia en materia de administración de procesos de TI.

Como se mencionó anteriormente, esta metodología permite garantizar los niveles de servicios informáticos establecidos donde participa la organización y sus clientes. Este

modelo está orientado a la reducción de costos en el desarrollo y soporte de las TIC y simultáneamente garantiza el cubrimiento de las necesidades de seguridad. El modelo ITIL ofrece a través de sus libros, las recomendaciones que contemplan desde listas de verificación hasta la asignación de responsabilidades que se adhieren a la naturaleza de cualquier empresa.

Los 5 libros que comprenden este modelo en su más reciente versión V3 son:

1. Estrategia de servicio: Diseño del plan de acción para el desarrollo de una estrategia en materia de tecnologías de la información.

2. Diseño de servicio: Conceptos relativos al diseño de Servicios TI.

3. Operación del servicio: Mejores prácticas orientadas a ofrecer un nivel de servicio que atienda las necesidades de los clientes.

4. Mejora continua del servicio: Se concibe como la fuente principal de desarrollo del servicio se tecnologías de la información.

5. Transición del servicio: Cambios que se han de producir el trabajo diario de las organizaciones. (HUÉRCANO, 2011)

15. SGSI y su relación con Control interno

Reglamentado por la Ley 87 de 1993, el ejercicio de control interno (CI) se define como un sistema integrado de planes, métodos, principios, normas, procedimientos de verificación y evaluación en una organización, cuyo objetivo es asegurar la ejecución de todas sus actividades en el marco de la legalidad y cumplimiento de las políticas establecidas.

Uno de los objetivos de CI que se encuentra más estrechamente relacionado con el SGSI es el de asegurar la oportunidad y confiabilidad de la información y registros generados, pese a que, sobre este, se soporten todas las labores de control. Las oficinas de control interno con el fin de verificar el cumplimiento de las políticas relacionadas, realiza la evaluación del SGSI con el objetivo de evaluar los controles establecidos, los cuales se soportan en la estrategia de mejora continua (Ciclo PHVA) y el cumplimiento de las 3 bases de seguridad de la información (Triada CID).

15.1 Componente de Información y Comunicación

El componente de información y comunicación de COSO, el cual apoya los otros componentes del control interno, cuenta con un enfoque sistemático que asegura el flujo de información en todas las direcciones con calidad y oportunidad. Este componente verifica que las políticas, directrices y mecanismos de consecución, captura, procesamiento y generación de datos dentro y en el entorno de cada entidad, satisfagan la necesidad de divulgar los resultados, de mostrar mejoras en la gestión administrativa y procurar que la información y la comunicación de una entidad y de cada proceso sea adecuada a las necesidades específicas de los grupos de valor y grupos de interés. Se requiere que todos los servidores de la entidad reciban un claro mensaje de la Alta Dirección sobre las responsabilidades de control. Deben comprender su función frente al Sistema de Control Interno.

Resalta de ese componente la comunicación interna y externa, así como los canales de comunicación de la información.

Los datos al interior de una organización deben ser: captados, identificados, seleccionados, registrados, estructurados y comunicados en tiempo y forma oportuna. Por

esto, la calidad y suficiencia de la información toma una importancia fundamental. Puesto que la organización debe asegurar que la información sea confiable, valida, suficiente, pertinente y oportuna. Para esto, es necesario diseñar, implementar y evaluar los mecanismos que aseguren

con las que debe contar toda información útil como parte del sistema de control interno.

Por lo anterior, los sistemas de información junto con los canales de comunicación implementados en la organización construyen una herramienta fundamental para la formulación de las estrategias organizacionales y por ende para el logro de los objetivos, es por esto, que su diseño debe responder a las necesidades y naturaleza de la organización. También resulta fundamental la efectividad del sistema de gestión del desempeño de esta herramienta, donde se garantice la solidez y efectividad de respuesta de la organización ante las posibles contingencias que se presenten.

16. Conclusiones

A raíz de la evolución a pasos agigantados de la tecnología en la actualidad, surgen a la misma velocidad nuevos métodos creados por los delincuentes que comprometen la integridad y seguridad de la información. De allí nace la necesidad de implementar una estrategia orientada a la seguridad de los Sistemas de Información con los que se está interactuando día a día en la organización, con el fin de prevenir y administrar los riesgos informáticos a los que se puede ver expuesta.

Desde la fase inicial de implantación y parametrización inicial de los sistemas de información es fundamental conocer las necesidades y exigencias en materia de seguridad

de datos de la organización, pues constituye un punto de partida importante en el diseño de un SGSI para la identificación de vulnerabilidades que afectarían el funcionamiento de los sistemas. Sin embargo, esto no es garantía de que las amenazas no se presenten, pues siempre estará expuesta ya que el aseguramiento se verá afectado por factores externos o quizá internos.

Los marcos de referencia ISO 27001, COBIT E ITIL han sido creados con el propósito de sumar valor a la gobernanza de los activos de la información, a través de buenas prácticas en planeación, organización, dirigir y controlar los SI que participan en todos los procesos de la organización,

La implementación del SGSI constituye en una herramienta fundamental para lograr una comunicación eficaz entre la alta dirección empresarial, los responsables de la gestión y custodia de la información y los clientes y demás interesados (Comunicación transversal).

Un SGSI reduce la probabilidad e impacto de los incidentes en materia de seguridad, mediante la implantación de los controles adecuados; de este modo, prepara a la organización ante posibles emergencias y garantiza la continuidad del negocio (debido cuidado y diligencia).

Los trabajos de auditoría Interna deben coadyuvar a que el control interno en TI brinde una garantía razonable del cumplimiento de los objetivos de la entidad.

17. Referencias

CEPAL. (26 de NOVIEMBRE de 2020). *Séptima Conferencia Ministerial sobre la Sociedad de la Información de América Latina y el Caribe*. Obtenido de https://conferenciaelac.cepal.org/

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. (11 de abril de 2016). *Documento Conpes 3854.* Recuperado el 26 de 02 de 2022, de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

HUÉRCANO, S. R. (18 de 07 de 2011). *Manual ITIL v3 Integro.* Recuperado el 03 de 03 de 2022, de https://docs.supersalud.gov.co/portalweb/planeacion/administracionsig/gsde01.pdf

ICONTEC. (2022). *Certificación ISO 27001, Sistemas de Gestión de seguridad de la información*. Obtenido de https://www.icontec.org/eval_conformidad/certificacion-iso-27001-sistemas-de-gestion-de-seguridad-de-la-informacion-2/#:~:text=El%20SGSI%20basado%20en%20ISO,activos%20importantes%20de%20su%20negocio.

ISO Tools. (16 de febrero de 2016). *Blog Calidad y Excelencia*. Recuperado el 15 de 02 de 2022, de Descubre qué es un SGSI y cuáles son sus elementos esenciales: https://www.isotools.org/2016/02/16/descubre-que-es-un-sgsi-y-cuales-son-sus-elementos-esenciales/

ISOTools Excellence. (23 de 02 de 2017). *isotools.org*. Recuperado el 03 de 06 de 2022, de ¿Cómo realizar un inventario de activos de información?: https://www.pmg-ssi.com/2017/02/realizar-inventario-activos-de-informacion/

MINTIC. (11 de ABRIL de 2016). *Política Nacional de Seguridad Digital en Colombia.* Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

NORMAS-ISO .COM. (s.f.). *Normas ISO*. Recuperado el 06 de 03 de 2022, de https://www.normas-iso.com/iso-27001/

The World Economic Forum. (2021). *The Global Risks Report 2020.* Switzerland. Recuperado el 15 de 02 de 2022

Universidad ESAN. (01 de 06 de 2016). *Los cinco principios de COBIT 5*. Recuperado el 01 de 03 de 2022, de https://www.esan.edu.pe/conexion-esan/los-cinco-principios-de-cobit-5