Beneficios de utilizar metodologías para la implantación de Sistemas de Gestión de Seguridad de la Información

Wendy Yomar Sarmiento Martínez
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
yomara_sm12@hotmail.com

***Resumen*—Hoy en día uno de los activos más importantes dentro de toda institución es la información, la misma debe ser protegida de amenazas del entorno durante su transición y almacenamiento, el presente artículo pretende demostrar la importancia de utilizar las metodologías para la implementación de sistemas de gestión de seguridad de la información (SGSI), de esta manera mitigar los riesgos y preservar la confidencialidad, integridad y disponibilidad de la información. Se analizan diferentes normas, con el fin de dar a conocer los beneficios de implementar metodologías para los SGSI, dentro de las misma se puede evidenciar que algunas normas son más generales, algunos centrados en la gestión de riesgos y otros incluso tendientes a desarrollar un modelo de madurez de la seguridad de la información. Finalmente, se analiza la aplicación de la metodología para implementar un SGSI, a un caso real, en el mismo se verifica las particularidades del objeto de estudio: las normas y recomendaciones internacionales, el modelo organizacional aplicable al negocio, y los beneficios que estas brindan.**

Palabras clave—metodología, normas, riesgo, sistema de gestión de seguridad de la información.

I. Introducción

En la actualidad se conoce que la mayoría de los procesos de negocios e industriales son automatizados y gestionados por sistemas informáticos, a lo que nos lleva a la pregunta ¿estos procesos están seguros?, cada día se conoce de los diferentes riesgos y amenazas tecnológicas las cuales varían desde diversas formas de virus, pasando por los recientes ataques de ransomware o simples fallas humanas, todo esto requiere de la implementación de controles que puedan ser gestionados a través de un adecuado enfoque de seguridad de la información.

El interés de esta investigación surgió por lo anteriormente descrito, muchas veces se cree que la seguridad que se tiene que implementar en un sistema]a informático es solo al código y no nos enfocamos al contexto en general como son los sistemas de información, esto genera un gran problema en las instituciones ya que al no tener conocimiento de los riesgos que se presentan puede llevar a grandes pérdidas económicas, que muchas ocasiones son irremediables.

Los riesgos más comunes a los que están expuestos los sistemas de información según Alejandro Pinzón [1] son:

Riesgos físicos:

- Accesos no autorizados
- Catástrofes naturales: incendios, inundaciones, terremotos tormentas, descargas atmosféricas
- Vandalismo en infraestructura
- Fallas en el flujo eléctrico
- Daños causados por humanos con o sin intención

Riesgos lógicos

- Software malicioso: virus, gusanos, caballos de Troya y spyware
- Errores o vulnerabilidades en el software
- Ataques de denegación de servicio

Para proteger a las instituciones de todas estas amenazas es necesario conocerlas y afrontarlas de una manera apropiada. Para ello debemos establecer unos procedimientos adecuados e implementar controles de seguridad basados en la evaluación de los riesgos y en una medición de su eficacia.

A. Seguridad de la Información:

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las instituciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos [2].

El Sistema de Gestión de Seguridad de la Información SGSI, según la ISO 27001 consiste en preservar la confidencialidad, integridad y disponibilidad, además de todos los sistemas implicados en el tratamiento dentro la institución [3]:

- Confidencialidad: la información no se pone a disposición de nadie, ni se revela a individuos o entidades no autorizadas.

Para referenciar este artículo (IEEE):

[N] W. Sarmiento, «Beneficios de utilizar metodologías para la implantación de Sistemas de Gestión de Seguridad de la Información» *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 7, pp. 104-107, 2020.

- Integridad: mantener de forma completa y exacta la información y los métodos de proceso.
- Disponibilidad: acceder y utilizar la información y los sistemas de tratamiento por parte de los individuos, entidades o proceso autorizados cuando lo requieran.

B. Proceso de los Sistemas de Gestión de Seguridad de la Información

Dentro del desarrollo de los SGSI es necesario la implementación de una metodología que promueva la adopción de un enfoque basado en procesos, con el fin de establecer, implementar, operar, dar seguimiento, mantener y mejorar el SGSI de las instituciones, por este sentido se adopta el modelo de procesos: Planificar-Hacer-Verificar-Actuar (PHVA) el mismo significa actuar sobre el proceso, resolviendo continuamente las desviaciones a los resultados esperados. El mantenimiento y la mejora continua de la capacidad del proceso pueden lograrse aplicando este modelo en cualquier nivel de las instituciones tanto públicas como privadas y en cualquier tipo de proceso ya que se encuentra asociada con la planificación, implementación, control y mejora del desempeño de los procesos.

A continuación, se describe el modelo PHVA aplicado a los procesos de SGSI.

- Planificar: (Establecer el SGSI) se debe establecer las políticas, los objetivos, procesos y procedimientos de seguridad necesarios para gestionar el riesgo y mejorar la seguridad de la información.
- Hacer: (Implementar y operar el SGSI) en esta etapa se debe garantizar una adecuada implementación de los controles seleccionados y la correcta aplicación de los mismos.
- Verificar: (Revisar y dar seguimiento al SGSI) se debe evaluar y verificar el desempeño de los procesos contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.
- Actuar: (Mantener y mejorar el SGSI) emprender acciones correctivas y preventivas basadas en los resultados de la verificación y la revisión por la dirección, para lograr la mejora continua del SGSI.

Diferentes instituciones internacionales han definido estándares y normas que apoyan en diferente medida el cumplimiento de los requerimientos indicados anteriormente. A continuación, se detallan los de mayor utilización a nivel mundial, y que fueron tomados como base para el modelo propuesto.

ISO 17799

Es un estándar para la administración de la seguridad de la información, e implica la implementación de toda una estructura documental que debe contar con un fuerte apoyo de la alta dirección de cualquier organización.

Este estándar fue publicado, con el objeto de desarrollar un marco de seguridad sobre el cual trabajen las instituciones. Esta norma internacional ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización [4].

COBIT

Es un estándar desarrollado por la *Information Systems Audit and Control Foundation* (ISACA), la cual fue fundada en 1969 en EE.UU., y que se preocupa de temas como gobernabilidad, control, aseguramiento y auditorias para TIC.

COBIT es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los Interesados, permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas [5].

ITIL

(*IT Infrastructure Library*, biblioteca de infraestructura de TI) Marco de referencia que describe un conjunto de mejores prácticas y recomendaciones para la administración de servicios de TI, con un enfoque de administración de procesos [6].

COSO

La normativa COSO, acrónimo de *The Committee of Sponsoring Organizations of the Treadway Commission's Internal Control - Integrated Framework*, está principalmente orientada al control de la administración financiera y contable de las instituciones. Sin embargo, dada la gran cercanía que hoy existe entre esta área y los sistemas de información computarizados, es que resulta importante entender el alcance y uso de esta norma. Junto a esto son muchas otras las normas que están directa o indirectamente relacionadas con ésta como por ejemplo COBIT.

El Informe COSO es un documento que contiene directivas e indicaciones para la implantación, gestión y control de un sistema de Control Interno, con alcances al área informática.

ISO Serie 27000

A semejanza de otras normas ISO, la 27000 es una serie de estándares, para identificar requisitos para sistemas de gestión de seguridad de la información [7].

- ISO 27001, guía de buenas prácticas en objetivos de control y controles recomendables de seguridad de la información.
- ISO 27002, una guía de implementación de SGSI (Sistema de Gestión en Seguridad de la Información) junto a información de uso del esquema PHVA.
- ISO 27003, especificación de métricas para determinar la eficacia de SGSI.
- ISO 27004, una guía de técnicas de gestión de riesgo.
- ISO 27005, especificación de requisitos para acreditación de entidades de auditoría y certificación de SGSI.
- ISO 27006, una guía de auditoria de SGSI.
- ISO 27007, una guía de gestión de seguridad de la información para telecomunicaciones.
- ISO 27011, una guía de continuidad de negocio en cuanto a TIC.
- ISO 27031, una guía de ciber-seguridad.

- ISO 27032, una guía de seguridad en redes.
- ISO 27033, una guía de seguridad en aplicaciones.

Es importante concluir que un modelo no será mejor que otro, debido a que inicialmente hay que evaluar la pertinencia, la cobertura (áreas) y ante todo que cada organización, cada empresa tiene su particularidad, por ende, lo importante será adoptar un modelo pertinente, tomar los elementos que sean aplicables y adaptar el modelo de referencia para generar un modelo propio para la empresa. En este sentido el objetivo de la investigación es mostrar la Importancia de Utilizar Metodologías para la implementación de Sistemas de Gestión de Seguridad de la Información en todos los procesos del negocio para así poder garantizar la confidencialidad, integridad, disponibilidad de la información.

II. Métodos

La presente es una investigación con alcance exploratorio y descriptivo, la primera se utilizó para encontrar el objeto de estudio y el segundo para caracterizarla, los mismos pretenden dar a conocer los beneficios que se tiene al implementar metodologías para la gestión de seguridad de la información en las diferentes instituciones,

Se determinó el objeto de estudio el cual es: beneficios de las metodologías para la implementación de sistemas de gestión de seguridad de la información.

El ámbito donde se enfoca la investigación fue en la ciudad de La Paz, Bolivia tomando en cuenta 25 empresas entre públicas y privadas.

Se aplicaron instrumentos de medición documental, para lo cual se diseñó una encuesta y entrevistas no estructuradas, de acuerdo al contexto de estudio.

El proceso de la investigación no tuvo inconvenientes, se realizó 2 etapas de recolección de información en las empresas, las cuales se describe a continuación:

Primera Etapa:

- Después de preparar la encuesta se pasó a aplicarla.

Segunda Etapa:

- Una vez terminada la encuesta se pasó a explicar en qué consiste y cuáles serían los beneficios que tendría la empresa aplicando metodologías para aplicar sistemas de gestión de seguridad de la información en todos los procesos de la empresa.

Terminada la explicación se les realizo dos preguntas más:

- ¿Utilizaría usted las metodologías para la implementación de sistemas de gestión de seguridad de la información en su empresa?
- ¿Después de la explicación, que norma utilizaría en su empresa como SGSI?

III. Resultados

Como se mencionó anteriormente se realizó la investigación a 25 instituciones a continuación se describe:

TABLA I. Cantidad de empresas tomadas como muestra entre públicas y privadas.

Tipo de Institución	
Privada	*Pública*
17	8

La siguiente tabla describe las preguntas más resaltantes de la primera etapa como se puede observar que existe desconocimiento sobre normas de seguridad.

TABLA II. Peguntas relevantes de la investigación

Preguntas		Tipo de institución	
		Privada	*Pública*
		Recuento	*Recuento*
¿Los principales procesos de negocio de la compañía están soportados por Tecnologías de la Información?	si	14	7
	no	3	1
¿La organización administra datos externos?	si	6	6
	no	11	2
¿La organización cuenta con un servicio externo de procesamiento de datos?	si	3	0
	no	14	8
¿Se tienen copias de los archivos en lugar diferente al de la computadora?	si	4	0
	no	13	8
¿Está su empresa protegida a nivel informático?	si	4	0
	no	13	8
¿Conoce algunas normas para la seguridad de la información?	si	7	0
	no	10	8

TABLA III. Niveles de preocupación en cuanto a la seguridad de la información en la empresa

Tipo de Institución	Niveles de preocupación en cuanto a la seguridad de la información en la empresa			
	muy preocupado	*algo preocupado*	*no muy preocupado*	*nada preocupado*
Privada	1	2	4	10
Publica	2	1	0	5

IV. Discusión

En la primera etapa se consultó sobre que normas conocían para implementar en su institución, pero la respuesta fue que el 88% no conocía sobre las normas y que el 12% sí.

TABLA IV. Conocimiento sobre normas

Tipo de Institución	¿Cuál es la norma de la cual escucho hablar o que usted conozca?					
	ISO 17799	*COBIT*	*ITIL*	*COSO*	*ISO Serie 27000*	*NINGUNA*
privada	0	1	0	0	2	14
pública	0	0	0	0	0	8

En la segunda etapa se procedió a realizar una explicación sobre las normas de seguridad los beneficios que estas brindan al aplicar metodologías para implementar sistemas de gestión de seguridad de la información SGSI en las instituciones y como pueden minimizar los riesgos de las mismas brindando así la confiabilidad integridad y disponibilidad de la información.

La siguiente tabla muestra la satisfacción de las empresas al saber de estos beneficios.

TABLA V. INTERÉS DE LA UTILIZACIÓN DE SGSI

¿Utilizaría usted las metodologías de sistemas de gestión de seguridad de la información en su empresa?	
SI	NO
21	4

La tabla VI muestra el interés de utilizar norma de sistemas de gestión de seguridad en las instituciones, donde el 84% de las instituciones estarían interesadas en aplicarlas, el otro 16% alegaron que si bien estarían interesados no cuentan con el presupuesto necesario.

TABLA VI. UTILIZACIÓN DE NORMAS SGSI

Tipo de Institución	¿Después de la explicación que norma utilizaría en su empresa como SGSI?					
	ISO 17.799	*COBIT*	*ITIL*	*COSO*	*ISO Serie 27000*	*NINGUNA*
privada	1	0	2	4	6	4
pública	1	4	0	2	1	0

V. CONCLUSIONES

Como se mencionó al principio es importante tomar en cuenta diferentes mecanismos de seguridad tanto físicas como lógicas e implementarlas en las instituciones.

La inexistencia de normas, políticas, procedimiento referidos a los procesos de la información constituye el principal riesgo al que está expuesta toda institución u organización, de esta manera es necesario que las mismas estén apegadas a las normativas de seguridad de la información.

Se analizó la situación actual de los estándares y normas más utilizadas a nivel mundial, con lo que se ha podido comprobar que cada norma tiene un campo de aplicación específico dependiendo del sector, tamaño de la empresa, tipo de tecnología de comunicación que utilizan, aplicaciones y servicios que ofrecen.

Implementando procesos de sistemas de gestión de seguridad de la información tomando en cuenta metodologías como también las fases del método PHVA de forma correcta, debe permitir resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

El desconocimiento de los beneficios que conllevan la implantación de metodologías para los sistemas de gestión de seguridad de la información en las instituciones hace que las personas no las apliquen al grado de tampoco contar con normas internas.

A medida que se realizó la investigación se dio una explicación a cada empresa sobre cuán importante es que tengan normas internas y mucho más contar con normas y estándares referidas a la seguridad de la información, al conocer sobre estos estándares el 84% de las instituciones estarían interesadas en aplicarlas, el otro 16% alegaron que si bien estarían interesados no cuentan con el presupuesto necesario pero que si comenzarían con implementar normar internas en su institución, de esta manera se pudo cumplir con el objetivo planteado en esta investigación.

REFERENCIAS

[1] A. P. Roberto, Sistemas de gestión de la seguridad de la información, 2016.

[2] I. security, «security,» 04 08 2017. [En línea]. Available: https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n. [Último acceso: 07 - 01 - 2020].

[3] SGSI, «Blog especializado en Sistemas de Gestión,» 28 07 2015. [En línea]. Available: http://www.pmg-ssi.com/2015/07/que-es-sgsi/. [Último acceso: 06 -01 - 2020].

[4] C. D. Argentero, «ISO 17799. La Seguridad Informática no es un producto sino un Proceso,» 12 09 2006. [En línea]. Available: http://www.monografias.com/trabajos42/iso-informatica/iso-informatica2.shtml. [Último acceso: 10- 11- 2019].

[5] ISACA, «COBIT 4.1 IT Governance Institute, 1-29,» 2007. [En línea]. Available: http://www.sciencedirect.com/science/article/pii/S0167404897846755?via%3Dihub. [Último acceso: 19- 12- 2019].

[6] H. A. Juárez, «ITIL: ¿qué es y para qué sirve?,» 2017. [En línea]. Available: http://www.magazcitum.com.mx/?p=50#.WelQxY_9TIU. [Último acceso: 12- 02- 2020].

[7] ISOtools, «La familia de normas ISO 27000,» 2015. [En línea]. Available: https://www.isotools.org/2015/01/21/familia-normas-iso-27000/. [Último acceso: 11- 01- 2020].

Breve CV de la autora

Wendy Yomar Sarmiento Martínez es Licenciada en Informática, mención: Ingeniería en Sistemas Informáticos por la Universidad Mayor de San Andrés. Diplomada en Educación Superior, Diplomada en Metodología de la Investigación mediante Tecnologías de la Información y Comunicación. Es docente universitaria. Actualmente realiza la Maestría en Informática Forense, Seguridad de la Información y Auditoria Informática en el Postgrado en Informática UMSA. Email: yomara_sm12@hotmail.com.