DISEÑO DE UN PLAN DE TRABAJO PARA LA IMPLEMENTACIÓN DE LA ISO 27001: SEGURIDAD INFORMÁTICA EN LA CORPORACIÓN UNIVERSITARIA ANTONIO JOSÉ DE SUCRE - CORPOSUCRE

PRESENTADO POR:

ALEXANDRA CHARTUNI BARRIOS
YEISON MIGUEL CONTRERAS CHICO
SEBASTIAN ROMERO HERNANDEZ

CORPORACIÓN UNIVERSITARIA ANTONIO JOSÉ DE SUCRE
CORPOSUCRE

FACULTAD DE CIENCIAS DE LA INGENIERÍA

PROGRAMA DE INGENIERÍA DE SISTEMAS

2020

Tabla de contenido

Índice de tablas y figuras

Resumen

Se propone diseñar un plan de trabajo para la implementación de los Sistema de Gestión de Seguridad de la Información (SGSI), basado en la norma ISO 27001, en la Corporación Universitaria Antonio José de Sucre. Se desarrollarán las actividades requeridas para cumplir con el objetivo final de poder diseñar un plan de trabajo que sea acorde a la estructura de la corporación, representando este un aporte muy fundamental y de gran ayuda al momento de realizar dicha implementación.

Palabras claves: Implementación, Plan, Diseño, Seguridad, Información, Sistemas, Gestión

Abstract:

It is proposed to design a work plan for the implementation of the Information Security Management System (ISMS), based on the ISO 27001 standard, at the Antonio José de Sucre University Corporation. The activities required to meet the final objective of being able to design a work plan that is in accordance with the structure of the corporation will be developed, representing this a very fundamental and helpful report at the time of carrying out said implementation..

Keywords: Implementation, Plan, Design, Security, Information, Systems, Management.

Introducción.

El avance tecnológico ha traído consigo un reto mayor para quienes se dedican al combate de programa con características maliciosas, la difusión de nuevas técnicas y metodologías de ataques y amenazas informáticas cada vez más sofisticadas y eficaces. No es un secreto la cantidad de recursos que invierten las organizaciones para evitar intrusiones y manipulaciones que pongan en riesgo, desde la integridad de la data hasta las operaciones propias de la entidad (Galdaméz, 2017)

Hoy en día, las organizaciones son más dependientes de sus redes informáticas y un problema que las afecte, por pequeño que sea, puede llegar a comprometer la continuidad de las operaciones, situación que inevitablemente se traduce en pérdida económica, retraso en las operaciones y crisis de confianza por parte de los usuarios. Aunado a lo anterior se encuentra la ausencia de una adecuada política de seguridad de las redes (Huseyin, Mishra, & Raghunathan, 2004). Este es un problema que está presente por el sólo hecho de subestimarse las fallas que a nivel interno se producen, considerando sobre todo que la propia complejidad de la red es una dificultad para la detección y corrección de múltiples y variados problemas de seguridad que van siendo detectados. (Schilling & B, 2015).

La seguridad de la información es una disciplina asociada tradicionalmente a la gestión de TIC, cuyo propósito es mantener niveles aceptables de riesgo de la información organizacional y de los dispositivos tecnológicos que permiten su recolección, procesamiento, acceso, intercambio, almacenamiento, transformación y adecuada presentación. Ha sido definida por la

norma ISO/IEC 27000 como la preservación de la confidencialidad, integridad y disponibilidad de la información (ICONTEC, 2009)

La adopción temprana de la ISO 27001 en todo el mundo en comparación con otros estándares de gestión (Freixo & Rocha, 2014), pone de manifiesto la importancia que ha tomado la seguridad de la información, lo cual se ratifica a partir del número de certificaciones otorgadas por la Organización Internacional para la Estandarización (ISO) en los últimos años, presentando un crecimiento exponencial, al pasar de un total de 5797 certificaciones en el año 2006, a 27536 en 2015, siendo Japón y el Reino Unido los países con mayor número de empresas certificadas, de acuerdo al último informe de la entidad (Magerit, 2017). No obstante, las normas establecen el *deber ser*, y no la forma como se logra, de allí la importancia de establecer metodologías que permitan orientar a las organizaciones en la forma como se debe abordar este tipo de procesos, con el respaldo de las normas internacionales promulgadas para tal fin.

Teniendo en cuenta lo anterior, la gestión administrativa de las universidades implica un tratamiento de datos fundamentalmente de alumnos (incluidos los exalumnos y pre-alumnos), de profesores y personal docente, así como de investigadores. El área de investigación, los departamentos de recursos humanos e informática, también gestionan información que puede llegar a ser sensible, además, se maneja un gran volumen de datos de cada persona, puesto que el tratamiento puede ir desde los resultados académicos de los alumnos, datos curriculares del personal docente e investigador, datos de control de presencia y horario, datos económicos y financieros, hasta datos de salud para control de bajas laborales o certificados médicos del alumnado para justificación de faltas. (Valenzuela, 2019)

Las nuevas tecnologías han permitido que las universidades desarrollen gran parte de su actividad en la red a través de campus virtuales, uso de soportes informáticos, constante uso de internet**,** lo que también supone un aumento considerable del riesgo y una gran responsabilidad en la aplicación de medidas organizativas y técnicas.

En la siguiente monografía, se realizará el diseño de un plan de trabajo para la implementación de un sistema de seguridad informática bajo ISO 27001 en la Corporación Universitaria Antonio José de Sucre-Corposucre, a fin de mejorar la seguridad informática y gestión de datos tanto de estudiantes como del personal docente y administrativo, considerando los siguientes objetivos:

Objetivo general:

Diseñar un plan de trabajo para la implementación de la ISO 27001: Seguridad Informática en la Corporación Universitaria Antonio José de Sucre-Corposucre.

Objetivos específicos:

- Realizar un diagnóstico que permita conocer el estado de la institución frente a la implementación del sistema de gestión bajo ISO 27001
- Construir un plan de trabajo con las directrices que faciliten la implementación de un sistema de gestión bajo ISO 27001 en la institución.

1. Contenido:

1.1. Seguridad Informática

La seguridad informática se encarga de mantener al mínimo los riesgos sobre los recursos informáticos, –todos los recursos– y garantizar así la continuidad de las operaciones de la organización al tiempo que se administra ese riesgo informático a un cierto costo aceptable. (Voutssas, 2010)

Teniendo en cuenta la importancia que hoy en día han adquirido las nuevas tecnologías dentro de las entidades, es fundamental que los sistemas informáticos con los que contamos en nuestras instituciones estén dotados de unas buenas medidas de seguridad. En los últimos tiempos los hackers o ciberdelincuentes se han dedicado a introducirse de forma ilegal en dichos sistemas para poder hacerse con todos los datos confidenciales que almacenamos en ellos o también para bloquearlos, entre otros actos delictivos. (Administrador, 2018)

La seguridad informática siempre busca la gestión de riesgos, es decir que se tenga siempre un mecanismo para evitarlo o prevenirlo y que se pueda realizar ciertas acciones para evitar esas situaciones de la mejor forma ya que esto garantiza que los documentos, registros y archivos informáticos de la organización mantengan siempre su confiabilidad total.

Según (Romero & Grase, 2018) La seguridad informática es la ciencia encargada de los procesos, técnicas y 14 métodos que buscan procesar almacenar y transmitir la información, mientras tanto la seguridad de la información no se preocupa sólo por el medio informático, se preocupa por todo aquello que pueda contener información; es decir, que se preocupa por casi

todo, lo que conlleva a afirmar que existen varias diferencias, pero lo más relevante es el universo que manejan cada uno de los conceptos en el medio informático

Las herramientas de seguridad informática deben estar dirigidas al análisis constante y a la ejecución proactiva para detectar vulnerabilidades en los ambientes TI de las empresas, realizándose mediciones desde una plataforma digital en la que se puedan visualizar los distintos procesos de la organización. La detección de vulnerabilidades y la seguridad informática es fundamental para mantener siempre segura e intacta la información privada de las entidades.

1.1. Importancia de la seguridad informática

Hoy en día si una entidad quiere ser competitiva debe contar con sistemas, recursos y plataformas TIC con un alto nivel de disponibilidad, lo que exige una gestión efectiva y un amplio proceso de transformación digital. En este proceso de transformación digital en el que están inmersas la mayoría de organizaciones y la sociedad en general, permite que se puedan cometer ataques contra la seguridad informática de las organizaciones desde cualquier parte del mundo utilizando como herramienta tan solo un ordenador. Es por esto que las organizaciones tienen que estar atentas para protegerse de posibles ataques eventuales ya que nadie está a salvo de los malware. (Tuyu technology, 2017) es decir, que la seguridad informática es muy importante porque limita los riesgos de ciberataques y al momento de implementar la ISO 27001 las entidades quedan en condiciones de manejar cualquier tipo de ataque ya que las personas encargadas de los sistemas informáticos y seguridad de la información tiene las condiciones en gestionar con tranquilidad cualquier ataque o el buen manejo de la información.

Algunas de las medidas recomendadas para evitar los ciberataques son:

- ✓ Externalizar servicios: al no tener tantos activos disminuye el riesgo de ataques.
- ✓ Contar con un buen antivirus que nos garantice protección.
- ✓ Capacitación de los usuarios: formar a los usuarios de los sistemas de seguridad informática en materia de ciberseguridad.
- ✓ Mantener actualizado el software.
- ✓ Prestar atención a las contraseñas.
- ✓ Realizar auditorías de software.
- ✓ Posibilidad de contratar un ciberseguro.

Cuando los sistemas informáticos de una organización reciben el ataque de un malware, se inicia un proceso de recuperación por parte de los sistemas informáticos de la organización muy difícil de conseguir. Es un proceso difícil ya que es muy complicado investigar qué ha pasado realmente, cuáles son las causas de que ese ataque haya podido penetrar en nuestros sistemas informáticos. Este ciberataque se puede investigar, pero se debe invertir tiempo y dinero ya que supone muchos costes. Lo más aconsejable para las organizaciones es reinstalar de nuevo todo y restaurar los ficheros críticos de la copia de seguridad. (Technology, 2017)

1.2. Sistemas de Gestión de la Seguridad de la Información

El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad será actualizado periódicamente; reuniendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información. (Modelo de seguridad, 2015)

La implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, en la Entidad está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos. (Modelo de seguridad, 2015)

Mediante la adopción del Modelo de Seguridad y Privacidad por parte de las Entidades del Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital. (Modelo de seguridad, 2015)

1.3. Marco Legal de la Seguridad informática en Colombia (Habeas Data)

Siempre que se desea implementar un Sistema de Gestión, toda organización debe obligatoriamente cumplir con todas las leyes, normas, decretos, etc que sean aplicables en el desarrollo de sus actividades. De manera general puedo mencionar el tema de seguridad social, cumplir con la Cámara de Comercio, permisos, licencias de construcción, etc, pero en lo que se refiere específicamente a Seguridad de la Información, estas son las Leyes vigentes al día de hoy: (Camelo, 2010)

1.3.1. Ley 603 de 2000.

Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales. (Camelo, 2010)

1.3.2. Ley estatutaria 1266 del 31 de diciembre de 2008.

Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

1.3.3. Ley 1273 del 5 de enero de 2009.

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. (Camelo, 2010)

1.3.4. Ley 1341 del 30 de julio de 2009

Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones. (Camelo, 2010)

1.3.5. Ley estatutaria 1581 de 2012

Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional. (Camelo, 2010)

Como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma. (Camelo, 2010)

Aspectos claves de la normatividad:

- Cualquier ciudadano tendrá la posibilidad de acceder a su información personal y solicitar la supresión o corrección de la misma frente a toda base de datos en que se encuentre registrado.
- Establece los principios que deben ser obligatoriamente observados por quienes hagan uso, de alguna manera realicen el tratamiento o mantengan una base de datos con información personal, cualquiera que sea su finalidad.

- Aclara la diferencia entre clases de datos personales construyendo las bases para la instauración de los diversos grados de protección que deben presentar si son públicos o privados, así como las finalidades permitidas para su utilización.
- Crea una especial protección a los datos de menores de edad.
- Establece los lineamientos para la cesión de datos entre entidades y los procesos de importación y exportación de información personal que se realicen en adelante.
- Define las obligaciones y responsabilidades que empresas de servicios tercerizados tales como Call y Contact Center, entidades de cobranza y, en general, todos aquellos que manejen datos personales por cuenta de un tercero, deben cumplir en adelante.
- Asigna la vigilancia y control de las bases de datos personales a la ya creada Superintendencia Delegada para la Protección de Datos Personales, de la Superintendencia de Industria y Comercio.
- Crea el Registro Nacional de Bases de Datos.
- Establece una serie de sanciones de carácter personal e institucional dirigidas a entidades y funcionarios responsables del cumplimiento de sus lineamientos.

1.3.6. Decreto 1377 de 2013.

Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012.

1.3.7. Decreto 886 de 2014.

Ley 1712 de 6 de marzo de 2014, por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información Pública Nacional y se dictan otras disposiciones

1.3.8. Decreto 1759 de 2016.

Procuraduría General de la Nación, para el cumplimiento de las obligaciones de la Procuraduría General de la Nación como sujeto obligado de la Ley 1712 de 2014 y demás normas reglamentarias (Camelo, 2010)

1.3.9. Decreto 90 de 2018.

- Ley 1915 de 12 de julio de 2018, por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de Derecho de Autor y Derechos Conexos.
- Ley 1928 de 24 de julio de 2018, por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest.

1.3.10. Decreto 2019.

Circular externa nº 1, de 16 de enero de 2019, de la Superintendencia de Industria y Comercio de Colombia, sobre la obligación de registro de bases de datos. (Cuervo, 2020)

1.3.11. Decreto 2020.

Ley nº 2015 de 31 de enero de 2020, por medio de la cual se crea la Historia Clínica Electrónica Interoperable (HCEI) y se dictan otras disposiciones. (Cuervo, 2020). Proyecto de Ley 300 de 2020, de 11 de marzo de 2020, por medio de la cual se dictan disposiciones generales para el fortalecimiento de la protección de datos personales, con relación al reconocimiento de las garantías de los derechos digitales, y se dictan otras disposiciones. (Cuervo, 2020)

2. Norma ISO 27000: Seguridad Informática

Es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

El estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

La aplicación de ISO-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización. La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002**.**

2.1 Estructura de la norma ISO 27001

1. Objeto y campo de aplicación: La norma comienza aportando unas orientaciones sobre el uso, finalidad y modo de aplicación de este estándar.
2. Referencias Normativas: Recomienda la consulta de ciertos documentos indispensables para la aplicación de ISO27001**.**
3. Términos y Definiciones: Describe la terminología aplicable a este estándar.
4. Contexto de la Organización: Este es el primer requisito de la norma, el cual recoge indicaciones sobre el conocimiento de la organización y su contexto, la comprensión de las necesidades y expectativas de las partes interesadas y la determinación del alcance del SGSI**.**
5. Liderazgo: Este apartado destaca la necesidad de que todos los empleados de la organización han de contribuir al establecimiento de la norma. Para ello la alta dirección ha de demostrar su liderazgo y compromiso, ha de elaborar una política de seguridad que

conozca toda la organización y ha de asignar roles, responsabilidades y autoridades dentro de la misma.

6. Planificación: Esta es una sección que pone de manifiesto la importancia de la determinación de riesgos y oportunidades a la hora de planificar un Sistema de Gestión de Seguridad de la Información**,** así como de establecer objetivos de Seguridad de la Información y el modo de lograrlos.
7. Soporte: En esta cláusula la norma señala que para el buen funcionamiento del SGSI la organización debe contar con los recursos, competencias, conciencia, comunicación e información documentada pertinente en cada caso.
8. Operación: Para cumplir con los requisitos de Seguridad de la Información**,** esta parte de la norma indica que se debe planificar, implementar y controlar los procesos de la organización, hacer una valoración de los riesgos de la Seguridad de la Información y un tratamiento de ellos.
9. Evaluación del Desempeño: En este punto se establece la necesidad y forma de llevar a cabo el seguimiento, la medición, el análisis, la evaluación, la auditoría interna y la revisión por la dirección del Sistema de Gestión de Seguridad de la Información, para asegurar que funciona según lo planificado.
10. Mejora: Por último, en la sección décima vamos a encontrar las obligaciones que tendrá una organización cuando encuentre una no conformidad y la importancia de mejorar continuamente la conveniencia, adecuación y eficacia del SGSI**.**

3. Resultados

3.1. Diseño de plan de trabajo.

Existen diversas formas de llevar a cabo una implementación de un SGSI en una organización, no obstante, para lograr cierto nivel de éxito y disminuir la incertidumbre en sus resultados, se debe adoptar un enfoque que permita abordar, desde una perspectiva sistémica, la forma de cumplir con los elementos que hacen parte de éste.

La metodología contempla cinco (5) fases secuenciales, las cuales serán detalladas con la suficiente granularidad como para poder comprender los pasos a desarrollar no sólo desde el punto de vista conceptual sino metodológico, a partir de un proyecto que incorpore personas, tiempos y recursos, así como el respaldo de la alta Dirección, como un requisito fundamental para cumplir los objetivos previstos.

Estas cinco fases con sus respectivas etapas están distribuidas en función de la norma ISO/IEC 27001, tal como se puede apreciar en la tabla 1 y cuyo cumplimiento es obligatorio, si se quiere cumplir con los requisitos exigidos para obtener la certificación internacional.

A continuación, se explicará en detalle cada una de estas fases, tratando de incorporar una serie de elementos prácticos que permitan poner en contexto su implementación.

3.1.1. Fase 1: Aprobación de la Dirección para iniciar el proyecto

Uno de los aspectos que se deben tener en cuenta y que no es a menudo claramente comprendido, es que un proyecto de SGSI no es un proyecto del área de Tecnologías de Información, es un proyecto organizacional y como tal requiere la aprobación y el apoyo de la Dirección para avanzar en su adecuada implementación. Para cumplir con este propósito se deben llevar a cabo las siguientes actividades:

Establecimiento de las prioridades de la organización para desarrollar un SGSI: Para llevar a cabo esta actividad es necesario conocer a fondo las prioridades que

Tabla 1 - Fases de implementación de un SGSI y su relación con los numerales de la norma ISO/ IEC 27001:2013.

Fases 27003:2010	Etapas	Numerales de la norma ISO/ IEC 27001:2013 relacionados
Obtener la aprobación de la Dirección para iniciar el proyecto	Establecimiento de las prioridades de la organización para desarrollar un SGSI	4.1. Conocimiento de la organización y de su contexto.
	Definir el alcance preliminar del SGSI	4.2. Comprensión de las necesidades y expectativas de las partes interesadas.
	Creación del plan del proyecto para ser aprobado por la Dirección.	5.1. Liderazgo y compromiso 7.1. Recursos
Definir el alcance, los límites y la política del SGSI	Definir el alcance y los límites del SGSI.	4.3. Determinación del alcance del sistema de gestión de seguridad de la información.
	Definir el alcance y los límites de las Tecnologías de Información y Comunicaciones.	
	Definir el alcance y los límites físicos.	
	Integrar cada alcance y los límites para obtener el alcance y los límites del SGSI.	
	Desarrollar la política del SGSI y obtener la aprobación de la Dirección.	5.1. Liderazgo y compromiso 5.2. Política 6.2. Objetivos de seguridad de la información y planes para lograrlos.
	Definición de roles, responsabilidades del SGSI	5.3. Roles, responsabilidades y autoridades en la organización. 7.2. Competencia 7.3. Toma de conciencia
Realizar el análisis de los requisitos de seguridad de la información	Definir los requisitos de seguridad de la información para el proceso SGSI	4.2. b) La organización debe determinar los requisitos de las partes interesadas pertinentes a la seguridad de la información.
	Identificar los activos dentro del alcance del SGSI	
	Realizar una evaluación de la seguridad de la información	6.1.2. Valoración de riesgos de seguridad de la información.
	Realizar la valoración de riesgos	

Realizar la valoración de riesgos y planificar el tratamiento de riesgos		6.1.2. Valoración de riesgos de seguridad de la información.
	Seleccionar los objetivos de control y los Controles	6.1.3. Tratamiento de riesgos de la seguridad de la información. 6.2. Objetivos de seguridad de la información y planes para lograrlo.
	Obtener la autorización de la Dirección para implementar y operar el SGSI	5.1. Liderazgo y compromiso
	Diseñar la seguridad de la información de la organización	7.4. Comunicación
Diseñar el SGSI	Diseñar la seguridad física y de las Tecnologías de Información y Comunicaciones	7.5. Información documentada
	Diseñar la seguridad específica de un SGSI	8.1. Planificación y control operacional
	Producir el plan del proyecto final del SGSI	8.2. Valoración de riesgos de seguridad de la información. 8.3. Tratamiento de riesgos de seguridad de la información. 9.1. Seguimiento, medición, análisis y evaluación 9.2. Auditoría interna 9.3. Revisión por la Dirección

Fuente: Propia

Se recomienda a Corposucre, que debe contar con los siguientes elementos como mínimo:

Objetivos estratégicos de la organización: este elemento permitirá determinar la forma como un SGSI puede aportar a los diferentes objetivos de la organización y justificar aún más su necesidad como parte de la estrategia organizacional. Una vez identificados los objetivos estratégicos a los cuales podría aportar el SGSI, se pueden establecer las líneas de negocio y los procesos involucrados que dependen de estos objetivos estratégicos.

Requisitos normativos o de terceros relacionados con la seguridad de la información: es necesario identificar los requerimientos normativos que tenga la entidad, o los requerimientos que en materia de información se tengan de terceros y que requieran cumplir con criterios de confidencialidad, integridad y disponibilidad de la información. Estos requisitos son fundamentales para complementar la necesidad de justificar un SGSI.

Sistemas de gestión existentes: con el fin de poder aprovechar la base instalada con que cuenta la organización en relación a otras normas de sistemas de gestión ya incorporadas en la organización, es necesario identificarlas si se tiene en cuenta que por lo general todas las normas de gestión basadas en las normas ISO cuentan con algunos elementos estructurales idénticos y como tal pueden ser compatibles con los requerimientos establecidos en la norma ISO/IEC 27001:2013. Se ha podido establecer de acuerdo a (Mesquida, Mas, Feliu, & Arcilla, 2014) que, en la mayoría de los casos, cuando una empresa decide implantar una norma de gestión de seguridad de la información, ya ha tenido otras experiencias en la incorporación de sistema de gestión basados en ISO. Es importante que el SGSI sea parte de la estructura de gestión de la organización, y se incorpore como parte de los procesos, en aquellas actividades que requieren adecuados niveles de protección de la información.

Definir el alcance preliminar del SGSI: El punto de partida para desarrollar un SGSI es definir qué se quiere proteger y con base en ello se determina de manera preliminar el alcance. De acuerdo a lo establecido en la norma ISO/IEC 27003, el alcance preliminar incluye un resumen de los requisitos establecidos por la Dirección y las obligaciones impuestas externamente a la organización.

Creación del plan del proyecto para ser aprobado por la Dirección: Si bien la incorporación de un SGSI en la organización es una tarea permanente, el primer paso para impulsar su diseño e implementación parte de la elaboración de un proyecto que permita definir con certeza los tiempos, recursos y personal requerido, utilizando para ello las diferentes herramientas de gestión de proyectos existentes en el mercado. Una vez formulado el proyecto es necesario e importante involucrar a la alta Dirección de la organización, si se tiene en cuenta que es allí donde inicia el proyecto y es ella, en últimas, la que autoriza la implementación y operación del SGSI. Adicionalmente, es allí donde se aprueba el presupuesto del plan de mitigación de riesgos resultante del análisis de riesgos. Es necesario que la Dirección proporcione evidencias de su compromiso con los procesos y actividades que están involucrados en el establecimiento, implantación, operación, monitoreo, evaluación, mantenimiento y mejora permanente del SGSI de acuerdo con la cláusula 5 de la norma ISO 27001:2013; estableciendo la política de seguridad de la información, fijando los objetivos, asignando los papeles y las responsabilidades, la comunicación de la importancia de la gestión de seguridad de la información para el negocio, la provisión de recursos para el SGSI y la decisión sobre el nivel aceptable del riesgo.

3.1.2. Fase 2: Definir el alcance, los límites y la política del SGSI

Esta fase contempla los siguientes elementos:

Definición del alcance: La importancia que tiene el establecimiento del alcance está fundamentada en que permite delimitar el proceso de gestión de riesgos y, por ende, pone foco a todo el proceso de implementación del SGSI.

El alcance se establece en función del negocio y/o en función de su ubicación en el caso de aquellas entidades que cuentan con varias sedes y puede ir desde un proceso, un conjunto de procesos, una sede, un servicio o un conjunto de servicios y debe ser adecuadamente definido para evitar ambigüedades, teniendo presente que su definición no conlleve a un proyecto inalcanzable en términos de tiempo y recursos. Se recomienda establecer el alcance, desarrollando previamente matrices que permitan cruzar los procesos de la organización con los requisitos, o con los dominios de la norma ISO 27001:2013 relacionados en el anexo A y que son aplicables a la organización. El producto final del alcance, por lo general, es un párrafo que resume lo que se está protegiendo en la organización y hace parte del documento de certificación entregado a aquellas entidades que logran cumplir con los requisitos exigidos.

Definición de la política y objetivos de seguridad: De acuerdo a Diaz (2010) la política de seguridad refleja lo que la organización quiere hacer con respecto a la seguridad de la información, los objetivos que pretende conseguir, contemplando los requisitos legales y reglamentarios aplicables y teniendo en cuenta el compromiso de la Dirección para conseguirlos.

Una política es una directriz que ayuda al cumplimiento de los objetivos, definida en función del alcance, y se encuentra contemplada como el primer control de la norma ISO/IEC 27002. Es importante tener en cuenta que la política general de seguridad de la información es una sola, y a partir de allí se pueden definir las diferentes políticas específicas en los diferentes niveles, tales como: política de acceso, política de uso de dispositivos móviles, política de backups, entre otros. En cuanto a los objetivos de seguridad, es importante delimitar los dos tipos de objetivos que contempla un SGSI: los objetivos generales del sistema y los objetivos de

control resultantes del proceso de análisis y valoración de riesgos. Al menos en esta primera parte se deben definir los objetivos generales que busca la implementación del SGSI, articulándolos con las políticas y dentro del alcance previsto.

Aprobación de la Dirección: Una de las formas de demostrar el apoyo de la Dirección de manera inicial, es la aprobación que ella da a las políticas y objetivos del SGSI dentro del alcance. De allí que el numeral 5.1. Literal a) de la norma ISO/IEC 27001:2013 establece, como parte del compromiso de la Dirección, el aseguramiento que ésta hace del establecimiento de la política y los objetivos de la seguridad de la información de modo que estos sean compatibles con la dirección estratégica de la organización.

3.1.3. Fase 3: Análisis de los requisitos de seguridad de la información

De acuerdo a lo establecido en la norma ISO/IEC 27003:2010 para establecer los requisitos de seguridad de la información se deben tener en cuenta cinco (5) elementos: Identificar (a) los activos de información importantes; (b) la visión de la organización y sus efectos sobre los requisitos futuros de procesamiento de información; (c) las formas actuales de procesamiento de información (aplicaciones, redes, la ubicación de las actividades y recursos de TI); (d) requisitos legales, reglamentarios, obligaciones contractuales, normas de la industria, acuerdos con clientes y proveedores, condiciones de pólizas de seguros, etc.; (e) el nivel de toma de conciencia sobre seguridad de la información y los requisitos de formación y educación en seguridad. Estos requisitos justifican la necesidad de contar con un SGSI en la organización.

Identificar los activos dentro del alcance del SGSI: Las organizaciones cuentan con una gran cantidad y variedad de activos tecnológicos, y tratar de establecer y clasificar estos activos puede ser una tarea de grandes proporciones, sobre todo en aquellas grandes organizaciones, ya que es probable que existan terabytes de datos electrónicos, almacenes de documentos y miles de personas y dispositivos que hacen parte de los activos tecnológicos (ISACA, 2012). Los activos en el contexto del SGSI, según la norma ISO/IEC 13335-1:2002, son cualquier activo de información físico o lógico que tiene valor para la organización.

La norma ISO/IEC 27005 diferencia dos tipos de activos: primarios y de soporte. Los activos primarios son los procesos de negocio y la información, mientras que los activos de soporte, son aquellos de los cuales dependen los activos primarios y se clasifican en: hardware, software, redes, personal, ubicación y estructura de la organización.

La Dirección General de Modernización Administrativa Procedimientos e Impulso de la Administración Electrónica (2012) a través de MAGERIT establece una clasificación basada en capas tecnológicas interdependientes, teniendo presente que existen relaciones entre activos, formando grafos, a través de los cuales se puede observar el nivel de dependencia entre los diferentes activos tecnológicos. Es necesario tener en cuenta que el valor de los activos se concentra generalmente en unos pocos, en especial en aquellos activos terminales (información, servicios, procesos) dadas las relaciones de dependencia que existen entre los activos primarios o terminales y los activos de soporte (Jiménez-martín, Vicente, & Mateos, 2015).

Se deben identificar y clasificar los activos de acuerdo a los requerimientos de seguridad y el nivel de criticidad para el negocio, así como establecer quién es el propietario de ese activo y quien debería ser el responsable de su seguridad (Pallas, 2009).

3.1.4. Fase 4: Valoración de riesgos y planificar el tratamiento de riesgos

Sin duda éste es el eje principal del SGSI, cuyo principal referente es la norma ISO/IEC 27005, no obstante, existen otros modelos que pueden ser utilizados para tal fin, entre los que se destacan: OCTAVE, CRAMM, NIST SP 800-30, MAGERIT, MEHARI, FAIR, RISK FOR COBIT 5.0. Al respecto se debe tener en cuenta:

Establecimiento de contexto: Esta fase contempla la preparación de los diferentes elementos que requiere el proceso de gestión de riesgos de seguridad de la información, partiendo del contexto, alcance, políticas, objetivos y parámetros de evaluación del riesgo. Para llevar a cabo la actividad de evaluación se requiere el establecimiento de parámetros para evaluar los riesgos, los cuales deben ser racionales y fáciles de utilizar a lo largo del proceso de implementación del SGSI. Estos parámetros de referencia son los siguientes: parámetros de probabilidad, parámetros de impacto, vulnerabilidad y criterios de aceptación del riesgo.

Parámetros de probabilidad: Debe establecerse una tabla de frecuencias de la posible ocurrencia de las amenazas, con los niveles requeridos de acuerdo a las necesidades de la organización. Generalmente, se utilizan tablas con un rango de entre tres (3) y cinco (5) niveles. A cada nivel se le asigna un valor de referencia en una escala lineal, cuyo único requisito es que a

mayor frecuencia dicho valor sea más alto. A cada nivel se le asigna un nombre que facilite su aplicación y adicionalmente se establecen criterios de valoración basados en número de veces que ha ocurrido o puede llegar a ocurrir, por lo general en el periodo de un año.

Parámetros de impacto: La gravedad de una amenaza no solo está en función de la cantidad de dinero que se pierde, sino en cómo los diferentes eventos que surgen en la organización y que están relacionados con la información pueden llegar a afectarla en su conjunto o en algunos procesos o a ciertas áreas.

Los parámetros de impacto se definen en función de las consecuencias que podría tener cualquier amenaza sobre la información o los activos de información en lo relacionado con confidencialidad, integridad y disponibilidad, tal como se ha explicado en los apartados anteriores.

Determinación de la vulnerabilidad: Para determinar qué tan importante es el riesgo, se ha establecido una nueva medida para estimar el impacto que una amenaza podría tener sobre la organización. Esta medida establece cuán grave sería para la organización que una amenaza ocurriera y afectara la información empresarial en términos de confidencialidad, integridad y disponibilidad. Esta medida genérica se conoce como vulnerabilidad, y corresponde a la sensibilidad de la organización frente a la posible materialización de una amenaza sobre la información empresarial.

La vulnerabilidad se mide en términos porcentuales y en función de los dos parámetros definidos previamente (probabilidad e impacto), y para ello se utiliza la siguiente formula: VX =(P × I)/ max (P × I); Donde VX es la vulnerabilidad del escenario de riesgo X, P es la probabilidad de ocurrencia e I es el impacto.

Criterios de aceptabilidad del riesgo: Los criterios de aceptación de riesgo permiten establecer el apetito de riesgo que tiene la organización y corresponde a los parámetros que define una organización para determinar si un riesgo es aceptable. La determinación por parte de la organización de lo que es suficientemente seguro, es lo que delimita el nivel de seguridad de la empresa y los principales recursos y esfuerzos a desarrollar para mantenerse en este estado. La mayor dificultad que existe para determinar las condiciones de seguridad de una organización, se fundamenta en el hecho de establecer los parámetros de aceptabilidad del riesgo, debido a la coincidencia de múltiples intereses, así como la evaluación hecha por personas con diferentes niveles de conocimientos, experiencia y "emotividad", lo que genera diversas percepciones sobre el mismo (Duque, 2017). Con el fin de compatibilizar todos los intereses existentes en la organización, es necesario que el equipo del SGSI en compañía de la alta dirección, determine la aceptabilidad del riesgo en forma coherente (Vanegas & Pardo, 2014).

Valoración del riesgo: La valoración del riesgo, de acuerdo a lo establecido en la norma ISO/IEC 27005:2009 contempla tres fases: identificación de los escenarios de riesgo, estimación del riesgo y evaluación del riesgo.

Identificación de escenarios de riesgo: El propósito de la identificación de riesgos es determinar qué podría suceder que cause una pérdida potencial, y llegar a comprender el cómo, dónde y por qué podría ocurrir esta pérdida (ICONTEC, 2009). Si partimos del concepto de riesgo, tal como lo plantea la norma ISO/IEC 27000, como la incertidumbre sobre los objetivos, dicha incertidumbre se materializa a través de la identificación de los eventos que pueden llevar al incumplimiento de objetivos, estos eventos son tradicionalmente definidos como amenazas. Algunos ejemplos de amenazas se pueden observar en las encuestas y estudios de seguridad de la información que cada año elaboran diferentes entidades tales como CISCO, IBM, Deloitte, Ernst & Young, PwC, entre otros.

Una buena práctica para delimitar las amenazas específicas que tiene una organización es la construcción de un catálogo de amenazas que permita a los responsables identificar aquéllas que en su concepto se podrían materializar. Entre los referentes para tal fin se encuentran MAGERIT, el repositorio de vulnerabilidades del gobierno de los Estados Unidos y el repositorio de vulnerabilidades del Instituto de Ingeniería de Software (SEI). La exposición de un recurso de información a una amenaza específica configura la "Unidad de Análisis Básica", y recibe el nombre de ESCENARIO DE RIESGO. La construcción de los escenarios de riesgo se realiza en función de las amenazas que pueden llegar a afectar a cualquier activo identificado dentro del alcance del SGSI.

Estimación del riesgo: Para estimar el riesgo, se pueden llevar a cabo análisis cualitativo, semicuantitativo o cuantitativo, o bien, una combinación de los tres (Shameli-Sendi, Aghababaei-Barzegar, & Cheriet, 2016). En cualquier caso, el tipo de análisis que se lleve a cabo debe ser

congruente con los criterios desarrollados en el establecimiento del contexto. Como se mencionó en párrafos anteriores, para estimar el riesgo se acudirá a la estimación de la vulnerabilidad: en este caso la vulnerabilidad inherente y la vulnerabilidad residual, entendida la primera como la estimación de la vulnerabilidad, sin tener en cuenta los controles existentes, mientras que la segunda representa la estimación de la vulnerabilidad, teniendo en cuenta el efecto que tienen los controles sobre la disminución de la probabilidad o el impacto.

Evaluación del riesgo: La evaluación del riesgo consiste en realizar una comparación de las vulnerabilidades resultantes de cada riesgo y confrontarlas contra el nivel de aceptación de riesgo. De acuerdo con este concepto, deberán existir dos tipos de evaluaciones: antes de controles y después de controles, acorde a la estimación resultante en la fase anterior. Los resultados arrojados de la evaluación de riesgos permiten diseñar mapas de riesgos, o mapas de calor, informes de vulnerabilidad por cada criterio de seguridad de la información y diversos indicadores que permiten monitorear el nivel de avance en la gestión del riesgo.

Tratamiento del riesgo: La fase de tratamiento de riesgos establece las acciones a desarrollar, a través de controles propuestos, para lograr llevar el riesgo a un nivel aceptable en la organización. Para ello se deben priorizar los riesgos residuales en función de los criterios de aceptabilidad, siendo prioritarios aquellos que se encuentran en el más alto nivel de vulnerabilidad.

Es importante tener en cuenta que la elaboración del plan de tratamiento de riesgos requiere un análisis de costo-beneficio de los controles a implementar y los techos presupuestales

asignados para su elaboración, de allí la importancia de priorizar aquellos escenarios de riesgo que son más críticos para la organización.

Para su tratamiento se encuentran diversas opciones, las cuales han sido clasificadas por la norma ISO/IEC 27005 en cuatro alternativas: reducción del riesgo, retención del riesgo, evitar el riesgo, transferencia del riesgo.

Un plan de tratamiento de riesgos, por lo general contempla la siguiente estructura: escenario de riesgo, riesgo residual, alternativa de tratamiento, controles a implementar, responsable de su implementación (rol), valor estimado, fechas estimadas de implementación, efecto esperado del control en función de la disminución de la probabilidad o impacto, riesgo residual esperado después del plan de mitigación.

Tabla 2 - Resumen de la información documentada que debe tener un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001

Numeral ISO/IEC 27001		Documentación
4.3	Determinación del alcance del SGSI	El alcance debe estar disponible como información Documentada
5.2	Política de seguridad	e) La política de seguridad debe estar disponible como información documentada
6.1.2	Valoración de riesgos de seguridad de la información	Información documentada acerca del proceso de valoración de riesgos de la seguridad de la información
6.1.3	Tratamiento de riesgos de seguridad de la información	Información documentada acerca del proceso de tratamiento de los riesgos de seguridad de la información
6.1.3	Declaración de aplicabilidad	d) Declaración de aplicabilidad
6.2	Objetivos de seguridad de la información y planes para lograrlos	Objetivos de la seguridad de la información

7.2	Competencia	Evidencia de la competencia de las personas relacionadas con la seguridad de la información
7.5	Información documentada	b) La que la empresa ha determinado que es necesaria para la eficacia del SGSI
7.5.3	Control de la información Documentada	La información documentada de origen externo
8.1	Planificación y control Operacional	Información documentada para tener confianza de que los procesos se han llevado a cabo de acuerdo a lo planificado
8.2	Valoración de la seguridad de la información	Resultados de las valoraciones de riesgos de la seguridad de la información
8.3	Tratamiento de riesgos de seguridad de la información	Resultados de los tratamientos de riesgos de la seguridad de la información
9.1	Seguimiento, medición, análisis y evaluación	Evidencia de los resultados del monitoreo y de la medición
9.2	Auditoría interna	g) conservar la información documentada como evidencia de la implementación del programa de auditoría y de los resultados de ésta.
9.3	Revisión por la dirección	Evidencia de los resultados de la revisión por la Dirección
10.1	No conformidades y acciones correctivas	Naturaleza de las no conformidades y cualquier acción posterior tomada
10.1	No conformidades y acciones correctivas	Resultados de cualquier acción correctiva

3.1.5. Fase 5: Diseñar el SGSI

El diseño del SGSI contempla básicamente tres componentes: La documentación que debe tener el sistema, la implementación de los controles previstos en el plan de tratamiento de riesgos y el monitoreo constante de la seguridad de la información.

Documentación del sistema: La información documentada que debe tener un SGSI comprende los requisitos contemplados en la norma ISO/IEC 27001, los cuales surgen a partir de

la implementación de sus diferentes fases. Un resumen de la información a documentar como parte del SGSI se muestra en la tabla 2.

Implementar el plan de tratamiento de riesgos: La implementación del plan de tratamiento de riesgos aprobado por la alta dirección con los recursos asignados para tal fin, y el mantenimiento de los controles existentes, es lo que permite garantizar niveles aceptables de seguridad de la información en la organización.

De allí que debe existir un monitoreo permanente de los controles y de los nuevos escenarios de riesgos que surgen para mantener un SGSI pertinente y ajustado a la realidad de la organización.

Monitoreo de la seguridad de la información: Tal como lo establece el numeral 9, de la norma ISO/IEC 27001:2013, la evaluación del desempeño del SGSI se realiza a través de la supervisión, medición, análisis y evaluación del sistema; las auditorías periódicas y la revisión por la Dirección. La supervisión, medición, análisis y evaluación del SGSI se realiza, por lo general, a través de la definición de indicadores. Estos indicadores son comúnmente desarrollados a nivel general del SGSI, a nivel de indicadores de gestión de riesgos y de los indicadores que permiten evaluar la eficacia y eficiencia de los controles que hacen parte de la declaración de aplicabilidad definida para el sistema.

En lo relacionado con las auditorías al SGSI existen tres (3) normas específicas que deben ser tenidas en cuenta al momento de desarrollar un proceso de auditoría: las normas ISO

19011:2011, ISO/IEC 27007:2011 e ISO/IEC TR-27008. Por último, la revisión de la dirección corresponde a la alta Dirección, con el fin de asegurar la suficiencia del sistema para dar respuesta a los objetivos y la eficacia en su implementación. Esta revisión se desarrolla por lo general cada año y está basado en las mediciones y las auditorías internas desarrolladas durante el periodo.

Conclusión.

La cantidad de normas con que cuenta actualmente la familia ISO/IEC 27000 para llevar a cabo la implementación de un sistema de gestión de seguridad de la información, pone de manifiesto una complejidad adicional al proceso de desarrollo de un sistema de gestión de seguridad de la información. El presente trabajo aporta en la construcción de un proceso metodológico para la Corporación Universitaria Antonio José de Sucre, a partir de la interrelación de cuatro de las principales normas que la conforman, allanando el camino para emprender un proyecto de este tipo y dar respuesta de esta forma a una necesidad sentida de la comunidad profesional de desarrollar metodologías ajustadas a los estándares internacionales, y en contexto con la organización. En futuras investigaciones, se espera aplicar la metodología a distintas organizaciones colombianas para dar cumplimiento a las diferentes regulaciones existentes actualmente.

Referencias

27005, N. T.-I. (2009). *Tecnología de Información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información*. Recuperado el 25 de Julio de 2020

Administrador. (08 de 11 de 2018). *Tipos de seguridad informatica*. Obtenido de Importancia de la implementacion en las e-mpresas: https://profitline.com.co/tipos-de-seguridad-informatica-importancia-de-la-implementacion-en-las-empresas/

Camelo, L. (23 de 02 de 2010). *Seguridad de la informacion en Coliombia*. Obtenido de Seguridad de la informacion en Coliombia: http://seguridadinformacioncolombia.blogspot.com/2010/02/marco-legal-de-seguridad-de-la.html

Cuervo, J. (2020). *Informatica juridica*. Obtenido de Informatica juridica: http://www.informatica-juridica.com/legislacion/colombia/

Electrónica., D. G. (2017). *MAGERIT - versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de Hacienda y Administraciones Pùblicas, Ed.

Freixo, J., & Rocha, A. (2014). Arquitetura de informação de suporte à gestão da qualidade em uniades hospitalares. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, 14*, 1-15. doi:http://dx.doi.org/10.17013/risti.14.1-15

Galdaméz, P. (2017). *Seguridad Informática.* Actualidad TIC.

Huseyin, C., Mishra, B., & Raghunathan, S. (2004). A Model for Evaluating IT Security Investments. *Commun ACM, 47*(1), 87-92.

Modelo de seguridad. (2015). Obtenido de Modelo de seguridad: https://www.mintic.gov.co/gestionti/615/w3-article-5482.html?_noredirect=1

Romero, m., & Grase, F. (01 de Octubre de 2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMATICA.* Obtenido de https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Schilling, A., & B, W. (2015). Optimal selection of IT security safeguards from an existing knowledge base. *Eur. J. Oper. Res.,, 248*(1), 318-327.

Technology. (11 de 07 de 2017). *Technology*. Obtenido de CIBERATAQUES: https://www.tuyu.es/importancia-seguridad-informatica/#:~:text=Por%20seguridad%20inform%C3%A1tica%20entendemos%20el,que%20contienen%20sus%20sistemas%20inform%C3%A1ticos.

Tuyu technology. (11 de 07 de 2017). Obtenido de Importancia de la seguridad informatica: https://www.tuyu.es/importancia-seguridad-

informatica/#:~:text=Por%20seguridad%20inform%C3%A1tica%20entendemos%20el,que%20contienen%20sus%20sistemas%20inform%C3%A1ticos.

Valenzuela, L. (16 de Abril de 2019). *Legal Today*. Recuperado el 25 de Julio de 2020, de https://www.legaltoday.com/practica-juridica/derecho-publico/proteccion-datos/que-deben-hacer-las-universidades-para-respetar-la-proteccion-de-datos-2019-04-16/

Voutssas, J. (06 de 04 de 2010). *Preservación documental digital y seguridad informática*. Obtenido de Preservación documental digital y seguridad informática: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008