DISEÑO DE UN PROTOTIPO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA INSTITUCIONES EDUCATIVAS

ALEX MAURICIO AVILA QUICENO

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA DE INGENIERÍA

FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MAESTRÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MEDELLÍN

2016

DISEÑO DE UN PROTOTIPO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA INSTITUCIONES EDUCATIVAS

ALEX MAURICIO AVILA QUICENO

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA DE INGENIERÍA

FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MAESTRÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MEDELLÍN

2016

DISEÑO DE UN PROTOTIPO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA INSTITUCIONES EDUCATIVAS

ALEX MAURICIO AVILA QUICENO

Trabajo de grado para optar al título de Magíster en Tecnologías de la Información y la Comunicación

Asesor

REINALDO MAYOL ARNAO

PhDc.

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA DE INGENIERÍA

FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MAESTRÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MEDELLÍN

2016

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____
Firma
Nombre
Presidente del jurado

_____
Firma
Nombre
Presidente del jurado

_____
Firma
Nombre
Presidente del jurado

Medellín, 28 de junio de 2016

A la memoria de mi hermano Marlon Andrés Avila Quiceno…

AGRADECIMIENTOS

Doy gracias a Dios por darme la fuerza, el tiempo y las condiciones físicas y mentales para el desarrollo de este trabajo.

A mi hija Luciana, mi inspiración en todo lo que hago, quien con su dulce voz siempre me animó a seguir estudiando.

Un agradecimiento especial a mi asesor el Doctor Reinaldo Mayol, por enseñarme que siempre se deben hacer las cosas bien y que cuando son difíciles, se valoran mucho más.

CONTENIDO

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

GLOSARIO

Proyecto de SGSI: Actividades estructuradas llevadas a cabo por la organización, con el fin de implementar un sistema de gestión de seguridad de la información.

Amenaza: Un principio viable de un incidente no-deseado, el cual puede afectar a un sistema.

Vulnerabilidad: La debilidad de un activo o conjunto de ellos que puede ser explotada por una o varias amenazas.

Riesgo: Es la mezcla de la posibilidad de un evento y su posible ocurrencia.

Análisis de riesgo: Sistema ordenado que busca, realizar inventario de los activos más valiosos para las organizaciones, identificarlos, clasificarlos y definir las metodologías para evaluar y proteger los mismos.

Tratamiento del riesgo: Proceso de tratamiento de los riesgos identificados y la implementación de controles para minimizar dichos riesgos

RESUMEN

Resumen: El presente trabajo tiene como finalidad presentar un prototipo de Sistema de Gestión de Seguridad de la Información (SGSI) para instituciones educativas, el cual posibilite ayudar a que la seguridad de la información sea gestionada correctamente por medio de un proceso metódico, argumentado y conocido por todas las áreas de la organización. Dicho proceso será desarrollado y evaluado basado en el estándar ISO27001:2013.

Objetivo: Definir la estructura general que debe contener un prototipo para la implementación de un SGSI en instituciones educativas.

Metodología: Para su desarrollo se proponen cuatro etapas:
Etapa 1. Encuesta de seguridad Informática en Colombia.
Etapa 2. Construcción del prototipo de SGSI.
Etapa 3. Marco legal.
Etapa 4. Validación del prototipo.

Resultados: Construir un prototipo de un SGSI que pueda ser aplicado en instituciones del sector educativo.

Conclusiones: En la actualidad, la creciente aparición de riesgos relacionados con los procesos de misión crítica de TIC (utilizados para la administración de la información), ha obligado a las instituciones a implantar sistemas que permitan proteger sus datos. En este sentido, el SGSI propuesto en la NTC-ISO-IEC 27001:2013 es la elección más factible para conservar la confidencialidad, integridad y disponibilidad de la información.

PALABRAS CLAVE: Sistema de Gestión de Seguridad de la Información, estándar ISO27001, Seguridad de la información, prototipo, modelo PHVA.

ABSTRACTS

Abstract: This paper aims to present a prototype of information security management system for educational institutions. Which allows help the security of information to be managed properly, through a systematic, documented and known throughout the organization. This process will be developed and evaluated based on the standard for the safety of the ISO27001:2013.

Objective: To define the general structure must contain a prototype for the implementation of an ISMS in educational institutions.

Methods: For its development four stages are proposed:
Step 1. Information Security Survey in Colombia.
Step 2. Construction of the prototype stage ISMS.
Step 3. Legal Framework
Step 4. Validation of the prototype.

Results: Building a prototype of an ISMS, which can be applied in education sector institutions.

Conclusion: Currently, the growing emergence of risks related to mission-critical processes of TIC's (used for information management), has forced institutions to implement systems to protect your data. In this sense, the proposed ISMS in the NTC-ISO-IEC 27001: 2013 is the most viable to maintain the confidentiality, integrity and availability of information option.

KEY WORDS: Information security management system, ISO27001 standard, Information Security, prototype, model PHVA

INTRODUCCIÓN

El acelerado crecimiento de las tecnologías de la información y comunicación ha impactado directamente en las organizaciones, por lo tanto, la seguridad de la información tiene que ser gestionada y controlada adecuadamente, [1] esta maratónica tarea se puede lograr utilizando algunas de las mejores prácticas desarrolladas a nivel mundial como pueden ser COBIT, ITIL e ISO27000. Hoy en día los datos de las empresas son el activo más valioso e incalculable, la información tiene una relevancia vital para el desarrollo y quizá incluso sea concluyente para la persistencia de las empresas [2].

Las instituciones educativas, al igual que las demás empresas no son ajenas a esta problemática, sus sistemas de información están expuestos a un número cada vez más elevado de amenazas [3]. Los virus informáticos o los ataques de denegación de servicio (DOS) son algunos de patrones más populares, pero igualmente se deben tener en cuenta los peligros de sufrir eventos de seguridad causados voluntaria o involuntariamente desde el interior de la entidad o aquellos inducidos accidentalmente por desastres naturales o fallas técnicas.

El propósito principal de SGSI no es garantizar la seguridad [4] que en ningún podrá ser total, sino avalar que los riesgos de la seguridad de la información son conocidos, apropiados, tratados y reducidos por la organización de una forma documentada y estructurada, revisada continuamente y adaptable a los cambios que se produzcan al interior de la organización.

El SGSI salvaguarda los activos de información de las empresas, sin diferenciar el medio en que se encuentren; por citar algunos ejemplos; correos electrónicos, informes de diferentes tipos, páginas web, imágenes en diferentes formatos, hojas de cálculo, información confidencial de empleados, entre otros.

La seguridad de la información como disciplina que defiende los activos de una organización, ha venido presentando una alta demanda, debido a los grandes alcances informáticos. Es constante recibir reportes de las diferentes vulnerabilidades en sistemas de información, que de alguna manera son aprovechadas; esto consecuencia de fallas

procedimentales o tecnológicas, o lo que en estos tiempos es más común fallas humanas. [5]

En el ámbito organizacional, la información se ha convertido en un insumo de la mayoría de las tareas que se realizan al interior de ellas. Cada día, las organizaciones adquieren sistemas de información y herramientas para facilitar el procesamiento de los datos con el fin de generar informes y estadísticas, las cuales se utilizan como guía para el desempeño y/o cumplimiento de los objetivos estratégicos trazados por cada organización.

Las compañías, en la búsqueda de la protección de la información, se encuentran en procesos de implementación y adopción de lineamientos y/o directrices de seguridad de la información. Dichos lineamientos son plasmados en un documento de política de seguridad de la Información. Para dar cumplimiento a la política se requiere de un proceso de culturización y sensibilización de seguridad de la información de los integrantes de las organizaciones, que se ve reflejado en las campañas de sensibilización que emprenden las instituciones. [6][7][8].

Con la llegada de la sociedad de la información [9] y con esto el aumento en el uso de las diferentes tecnologías de la información y las comunicaciones (TIC) [10], hace que la información y los medios informáticos que la administran posean un rol primordial en las actividades financieras, sociales y culturales. [11] Asociado a este aumento, es igualmente cada vez mayor la suma de amenazas y ataques que se producen a las aplicaciones y recursos informáticos. [3]

Es así como la información se trasforma en un recurso primordial que se debe preservar. La seguridad informática se torna necesaria como forma de mejorar, madurar e incrementar la integridad, disponibilidad y confidencialidad de los datos. [12]

Los sistemas de información de las instituciones académicas se encuentran entre los más atacados del mundo [13]. Su infraestructura descentralizada y la necesidad de combinar la experimentación y los controles, hacen difícil en muchos casos, garantizar unas medidas de seguridad fiables a través de sus redes.

1. DESCRIPCIÓN DEL PROBLEMA Y PROPUESTA DE SOLUCIÓN

1.1. Descripción del problema

Los SGSI, juegan un papel fundamental para proteger a la organización y su capacidad de llevar a cabo su misión empresarial. [4] No solo estamos hablando de los activos de la empresa, también abarca todos los procesos de gestión de riesgos de las organizaciones.

Es común que las empresas sientan que sus sistemas están “blindados” porque cuentan con un firewall y antivirus en todas sus estaciones de trabajo, generando en ellas un estado de tranquilidad y confianza que las convierte en blanco fácil para un ataque.

La administración de la seguridad en las instituciones educativas es una tarea de alta complejidad que demanda un considerable nivel de conocimiento. Los requerimientos por parte del personal de las instituciones y su comunidad de alumnos son cada vez mayores.

Por un lado, debe considerarse que el acceso a la información disponible en Internet, constituye un requerimiento fundamental para el diario funcionamiento de cualquier institución educativa, por lo cual contar con una infraestructura que contribuya a la correcta administración de la información y una alta disponibilidad, es primordial.

De igual forma, los aplicativos académicos y administrativos para el correcto funcionamiento de las instituciones son vitales para el desarrollo diario de las actividades y requieren de diferentes competencias para su administración y para mantener los niveles de seguridad propios de estas instituciones.

Del mismo modo podemos observar que las instituciones educativas en su gran mayoría tienen digitalizada su información. Hoy en día, las bases de datos tienen almacenados los datos personales e históricos de matrículas de cientos de personas, pero entonces, ¿qué sucede si un hacker aprovecha alguna debilidad en la seguridad, accede a la base de datos y roba todos estos registros para vendérselos a la competencia? La institución puede sufrir un descenso representativo en la demanda de estudiantes.

Igualmente ¿qué sucede si un empleado por desconocimiento de las buenas prácticas de seguridad, conecta a un equipo de la red interna, una memoria USB con un virus malicioso que infecta los servidores, destruyendo los registros de la base de datos? Al

depender completamente de su información, las instituciones educativas tendrían que interrumpir sus actividades de manera temporal, mientras se trata de restablecer los datos eliminados o modificados y cada minuto de interrupción representa decenas de matrículas que dejarán de realizarse (dinero que la institución dejará de percibir).

Y ¿qué pasa si la institución no tiene un buen sistema de Backup y la información no puede ser recuperada? la institución educativa no tendrá bases para operar, no podrá generar certificados, ni matricular estudiantes antiguos porque no habrá nada que legitime los cursos realizados, lo que traerá consigo consecuencias legales y una carga reputacional puesto que los usuarios perjudicados no tendrán una buena imagen de la institución. Sería muy difícil superar un problema de estas magnitudes.

Como se puede observar, la incorrecta administración de la seguridad de la información puede generar perjuicios representativos para la organización. Teniendo en cuenta las mejores prácticas planteadas por estándares internacionales como COBIT 5 e ISO27001:2013, que recomiendan la creación de políticas de seguridad claras para los empleados en la administración de los datos, la estandarización en los procesos que se llevan a cabo y la capacitación del personal sobre la cantidad y variedad de amenazas a las que se expone un sistema de información, sumado a la acelerada multiplicación y evolución de los riesgos de manera permanente en el medio, hacen que la implementación de un SGSI sea una oportunidad de mejora con gran trascendencia para las instituciones educativas.

Bajo este contexto, el presente trabajo de grado brinda como alternativa, el diseño estructural que debe contener un modelo para la implementación de un SGSI en instituciones educativas, además de una serie de herramientas que les permitirán madurar la seguridad al interior de las mismas, basados en el estándar ISO27001:2013.

1.2. Propuesta de solución

Para ayudar a las instituciones educativas en su camino de creación de un SGSI, se presentarán una serie de etapas desarrolladas a través de un prototipo, necesarias para pensar en la implementación de este tipo de sistemas al interior de sus empresas, dichas etapas están conformadas de la siguiente manera:

Etapa 1: Inicialmente se realizará una revisión exhaustiva del estado de la seguridad informática en el país a partir de la encuesta Nacional de Seguridad de la Información del año 2014.

Etapa 2: En esta etapa se construirá un prototipo para la implementación en organizaciones del sector educación, el cual será instalado en diferentes instituciones.

Etapa 3: Se ajustará el prototipo creado según la normatividad legal que es aplicable al trabajo de grado.

Etapa 4: Para la validación del prototipo se utilizarán como datos sintéticos de pruebas dos instituciones educativas, que para este caso serán el Centro Colombo Americano de Medellín y la Institución Universitaria Escolme.

2. OBJETIVOS

2.1. Objetivo General

Definir la estructura general que debe contener un prototipo para la implementación de un SGSI en instituciones educativas.

2.2. Objetivos Específicos

- Revisar a partir de la encuesta Nacional de Seguridad de la Información del año 2014, el estado actual de los SGSI en las instituciones educativas en Colombia.

- Proponer las metas mínimas que cualquier institución educativa tiene que cumplir a nivel internacional para la implementación de un SGSI.

- Construir un prototipo para la implementación de un Sistema de Gestión de Seguridad en organizaciones del sector educación.

3. MARCO TEÓRICO

3.1. Inseguridad de la información

En los últimos años, la información ha llegado a ser considerada “el activo más valioso de una organización”, puesto que gracias a nuevos modelos estratégicos implementados de manera masiva, se ha convertido en un elemento clave en la toma de decisiones, aportando un alto nivel de competitividad que se traduce en mayor desarrollo empresarial.

Antes de la aparición y masificación del uso de sistemas informáticos, la información de las organizaciones era recopilada en papel y se almacenaba en grandes archivadores, lo que representaba una gran complejidad para su gestión.

Los sistemas informáticos han permitido que toda esta información sea digitalizada, simplificando su almacenamiento, administración y transporte. Pero con las nuevas facilidades, también han aparecido nuevos desafíos que amenazan la seguridad de la información alterándola o eliminándola, por lo que “la inseguridad informática es la característica propia de los sistemas de información actuales.” [14]

Como menciona Jeimy J. Cano en su artículo *Entendiendo la inseguridad de la información*, “pareciera que mientras más nos esforzamos en controlar y avanzar en el entendimiento de la inseguridad, nuevas y más desafiantes vulnerabilidades aparecen.” [14]

3.2. Seguridad de la información

El panorama actual de inseguridad de la información ha obligado a las organizaciones a implementar modelos que protejan sus sistemas de información y mejoren su seguridad.

La seguridad de la información, por consiguiente, se podría precisar como la defensa de la confidencialidad, integridad y disponibilidad de los activos de información de las organizaciones según sea preciso, para lograr los objetivos del negocio de la organización. [15]

La función de la seguridad de la información tradicional se concentra en la información y cómo ésta debe ser protegida. Es decir, estudian sus detalles y sus medios de difusión o almacenamiento para establecer las medidas tecnológicas requeridas que permitan un acceso confiable y controlado. [16]

Actualmente, la seguridad de la información, debido al incremento en la utilización de estándares como COBIT, ITIL e ISO27000, hacen que se convierta en un elemento fundamental para todo tipo de organización, no solo es pensada para organizaciones como bancos o financieras sino que se amplía a todo tipo y tamaño de empresa. [17]

La seguridad de la información se alcanza realizando un apropiado conjunto de revisiones donde están incluidas las políticas, métodos, operaciones, estructuras organizacionales y procedimientos de software y hardware.

Al hablar de seguridad de la información se manejan los conceptos de evento de seguridad de la información e incidente de seguridad de la información, los cuales están estrechamente relacionados y pueden llegar a confundirse:

3.1.1. Evento de seguridad de la información

Según la norma ISO 27035, un evento de seguridad de la información, es la presencia reconocida de una condición de un sistema, servicio o inclusive red, que indica una potencial violación de la política de seguridad de la información o la falla de las contramedidas. [18]

Algunos ejemplos de eventos de Seguridad de la Información son: Un empleado que se enlaza a un sistema, un intento errado de un empleado para acceder a un aplicativo, un firewall que aprueba o bloquea un ingreso, una alerta de cambio de contraseña de un usuario, etc. [19]

3.1.2. Incidente de seguridad de la información

Por otro lado, un incidente de Seguridad de la Información se caracteriza por ser un evento o una serie de eventos de seguridad de la información, no esperados, que tienen una posibilidad mayor de comprometer las operaciones de la empresa y de comprometer la seguridad de la información. [18]

Cuando un **evento** comienza a registrar cualquier grado de impacto operativo, se convierte en un **incidente**. Por tanto, un incidente podría calificarse como un evento de cierta importancia, reportable y que genera un efecto significativo en los procesos del negocio. [19]

Algunos casos de Incidentes de Seguridad de la Información podrían ser; Un acceso no permitido, el robo de contraseñas por parte de alguno de los usuarios, las diferentes prácticas de Ingeniería Social que se puedan presentar, la explotación de fallas en los procesos de autenticación para lograr accesos ilícitos, el robo de información, el borrado de información de terceros, la alteración de la información de terceros, el abuso y/o mal uso de los servicios informáticos internos o externos de una organización. [18]

3.1.3. Diferencia entre seguridad informática y seguridad de la información

Es importante tener clara la diferencia entre la seguridad de la información y la seguridad informática, la primera abarca muchas más áreas, debido a que la información puede encontrarse en diferentes medios y formas, mientras la segunda se dedica exclusivamente de la protección de las infraestructuras de tecnologías de la información y la comunicación que soportan las organizaciones. Por consiguiente la seguridad de la información cubre la seguridad informática. [15]

3.1.4. Seguridad informática

Expresado de otra manera, la seguridad informática son las estrategias implementadas para preservar todos los equipos informáticos personales y acoplados en una red, frente a perjuicios accidentales o mal intencionados. Estos daños incluyen el mal funcionamiento del hardware y software, la pérdida de datos y el ingreso a datos de la organización de personal no autorizado. [20]

3.1.4.1. Principios de la seguridad informática

Existen diferentes servicios de seguridad, por medio de los cuales se avala que los recursos del sistema de información sean utilizados de la manera establecida y el acceso y modificación de la información sólo sea posible a las personas acreditadas para tal fin. Estos son:

Disponibilidad: Es la propiedad, forma o condición que tiene la información de presentarse a disposición de quienes necesiten acceder a ella, ya sean personas, procesos o aplicativos. En otras palabras, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran. [20]

La falta de disponibilidad se asume como una interrupción a los servicios, por lo que perjudica directamente a la producción de la organización**.** [21]

Confidencialidad: Es el atributo o característica consistente en que la información no se coloca a disposición, ni se presenta a individuos, entidades o procesos no autorizados. [22] De acuerdo a esto, la información debe llegar solamente a las personas autorizadas; para un usuario que no tiene permiso de acceso a la información, ésta debe ser ininteligible.

En contra la confidencialidad pueden presentarse salidas y filtraciones de información, así como accesos no permitidos. La confidencialidad es una propiedad difícil de recuperar, lo que representa un aspecto delicado en la organización, y su violación podría generar desconfianza y suponer el incumplimiento de leyes referentes a la custodia de los datos. [22]

Integridad: Consiste en mantener las cualidades de un documento o archivo sin alteraciones no autorizadas. La integridad de un dato puede ser obtenido agregándole un conjunto de información de identificación de la integridad, en este enfoque, la firma digital es una de las herramientas transcendentales para lograrlo.

En detrimento de la integridad, los datos podrían ser manipulados, corruptos o incompletos. La integridad perjudica directamente el adecuado desempeño de las operaciones de una organización. [22]

Autenticación: Es la propiedad que permite verificar que un documento pertenece a quien el documento lo dice. La autenticación en los sistemas informáticos habitualmente se realiza mediante un usuario o login y una contraseña o password.

El sistema debe ser capaz de verificar que un usuario identificado que accede o genera una determinada información, es quien dice ser. Solo cuando un usuario o entidad ha sido autenticado, podrá tener autorización de acceso.

Se puede exigir autenticación en la entidad origen de la información, en la entidad destino o en ambas. [23]

No repudio: También conocido como irrenunciabilidad, es una facultad de seguridad de la información, estrechamente relacionada con la autenticación, que es utilizada para comprobar la participación del emisor y el receptor en una comunicación. [23]

Ahora bien, la autenticidad verifica quién es el emisor de un documento y cuál es su receptor, el “no repudio” verifica que el emisor envió la comunicación y que el receptor la recibió. Existen dos posibilidades:

- No repudio en el origen, cuando el emisor no puede negar el envío. La prueba la crea el propio emisor y la recibe el receptor.

- No repudio en el destino, cuando el receptor no puede negar que recibió el mensaje. La prueba la crea el receptor y la recibe el emisor.

En general, los distintos servicios de seguridad dependen jerárquicamente unos de otros. Es imprescindible que exista el nivel inferior para poder aplicar el siguiente, en la *Figura 1 Jerarquía Principios de la Seguridad de la Información,* se puede apreciar mejor este concepto:

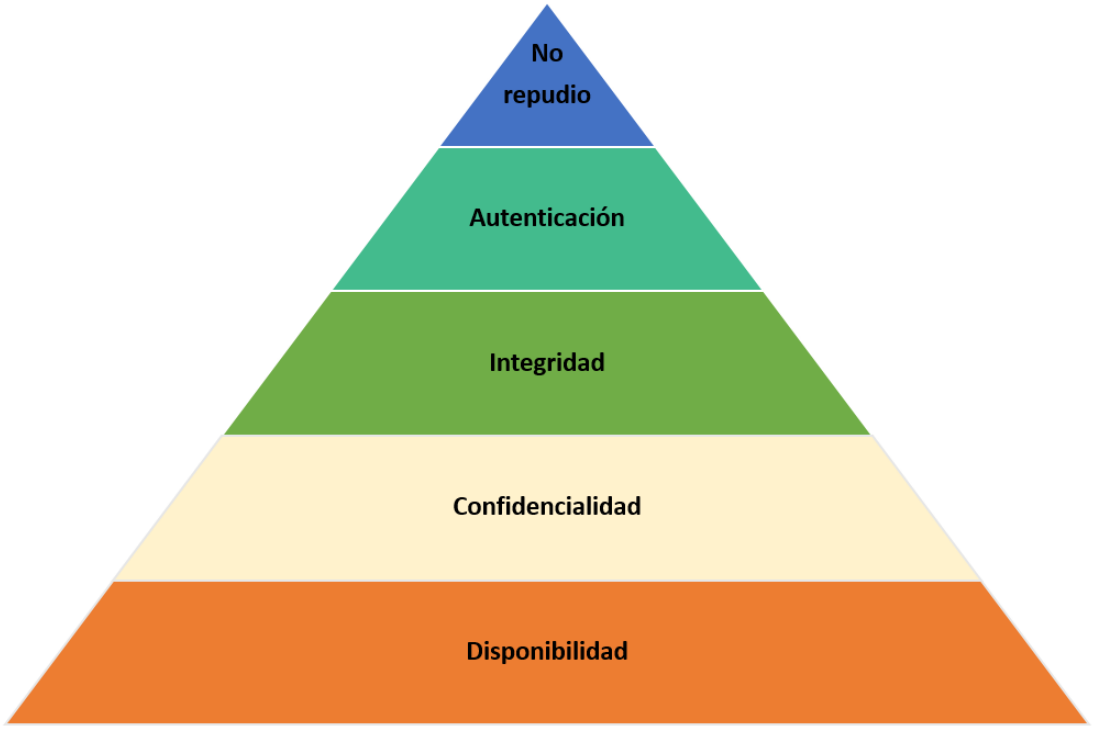


Figura 1 Jerarquía Principios de la Seguridad de la Información.

La seguridad de un sistema informático depende de diversos factores, entre los que se puede destacar: [24]

- La sensibilización de los directivos y responsables de la organización.
- Los conocimientos, capacidades e implicación de los responsables del sistema informático.
- La mentalización, formación y asunción de responsabilidades de todos los usuarios del sistema.

- La correcta instalación, configuración y mantenimiento de los equipos.
- La administración de los permisos y privilegios asignados a los usuarios.
- El soporte de los proveedores, con la publicación de parches y actualizaciones que permitan corregir fallos o vulnerabilidades.
- Contemplar no sólo la seguridad frente a las amenazas del exterior, sino también las amenazas procedentes del interior de la organización, aplicando el principio de "Defensa en Profundidad".

3.1.4.2. Elementos vulnerables en el sistema informático

La seguridad es un problema integral. Los problemas de seguridad informática no pueden ser tratados aisladamente ya que la seguridad de todo el sistema es igual a su punto más débil. [23]

Los tres elementos fundamentales a proteger en todo sistema informático son el software, el hardware y los datos. Estos tres elementos deben admitir tres operaciones primordiales: almacenamiento, procesamiento y transmisión de la información. Estas tres operaciones pueden ser víctimas de múltiples ataques, los cuales pueden dividirse en cuatro grandes tipos: Acceso, modificación, interrupción y generación.

Normalmente, los datos de las organizaciones componen el principal factor de los tres a proteger, esto obedece a que es el más amenazado y presenta un grado mayor de recuperación.

Hoy en día por medio de programas mal intencionados como sniffers, keyloggers, virus informáticos, los cuales atentan contra los servicios fundamentales de la seguridad de la información mencionados anteriormente, una persona, un aplicativo o hasta un proceso pueden ingresar a un segmento del sistema al cual no están autorizados, siendo difíciles de detectar.

Además de ingresar, el ataque puede causar la modificación, pérdida, o reemplazo de los datos o el sistema.

Un ataque, también puede bloquear que la información llegue a su receptor. En este caso, el ataque es fácil de detectar pero difícil de impedir.

Un ataque a los datos puede agregar campos determinados y registros adicionales en un sistema de base de datos, agregar determinadas líneas de código a los aplicativos, añadir programas en su totalidad en un sistema (virus), e implantar mensajes no acreditados por una línea de datos.

En relación a los ataques contra el hardware, se pueden dar de manera intencional o de forma accidental, estos ataques pueden ir desde incendios a los diferentes sistemas, fallas físicas, daños en el cableado estructurado entre otros.

Finalmente, los ataques en contra del software se pueden concentrar en los sistemas operativos de la empresa, programas de ofimática, en aplicativos desarrollados por la empresa, o a los programas descargados e instalados por el usuario. Existe gran variedad de ataques software como:

- La bomba lógica, donde el programa incluye comandos que al cumplirse una condición provocan una distorsión del funcionamiento normal del sistema.
- Virus que normalmente reemplazan archivos ejecutables por otros infectados con el código de éste.
- Gusanos que se replican, alojándose en diferentes ubicaciones del ordenador con el objetivo de colapsar los ordenadores y las redes informáticas.
- Backdoors que son puertas traseras que producen la entrada en el sistema de modo que el usuario usual del mismo no tiene noción del ataque.
- Caballos de Troya que se utilizan regularmente para situar Backdoors.
- Ataques al personal que suelen conocerse más como ingeniería social y consiste en mantener un trato social con las personas que custodian datos, indagar en sus costumbres o conocerlas más profundamente para perpetrar posteriormente un ataque más elaborado.[25]

3.1.5. Sistema de Gestión de Seguridad de la Información (SGSI)

Si una organización es víctima de alguno de estos ataques, su estabilidad y el cumplimiento de sus objetivos corporativos podrían verse afectados de manera significativa, por lo que es necesario adaptar un método que garantice que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. [26]

Para lograr este fin, se implementa un SGSI, el cual fomenta que una organización conozca los riesgos a los que está expuesta su información y los trate mediante una metodología definida, documentada y conocida por todos, que se revisa y mejora constantemente. [15]

El SGSI salvaguarda la confidencialidad, la integridad y la disponibilidad de la información, por medio de la aplicación de un proceso de gestión del riesgo, y brinda confianza a las partes interesadas al gestionar adecuadamente los riesgos. [27]

El objetivo principal de un SGSI es que las diferentes actividades afines con la gestión de la seguridad de la información, como pueden ser la declaración de objetivos, la planificación de actividades relacionadas al mejoramiento de la seguridad de la información, la implantación de controles, que pueden ser adaptados de normas como son ISO27001:2013 ITIL O COBIT, el análisis y la reacción ante incidentes y eventos, se puedan definir, repetir, medir y optimizar, implantando un proceso de mejora continua y dotando a las organizaciones del concepto de calidad a la Seguridad. [28]

Es un error considerar que el aseguramiento de los sistemas de información de una organización es función del área de TI, debido a que las acciones de todos los miembros que la componen pueden afectar de manera representativa la seguridad. Es por ello que la implementación exitosa de un SGSI requiere el compromiso de todos, especialmente la alta dirección, comprendiendo y aceptando sus responsabilidades. [29] Adicionalmente, es

necesario tener en cuenta el alcance y la planificación temporal requeridos por el SGSI, el nivel de seguridad deseado, tamaño y complejidad de la organización.

La implementación de un SGSI en una empresa puede fluctuar entre seis meses y un año. Está condicionado al ámbito, el tamaño y complejidad de la empresa.

Es recomendable que el proceso de implementación no sea mayor a que un año, ya que si se prolonga demasiado el tiempo puede causar que toda la labor realizada al principio del proyecto, quede obsoleta antes de llegar a su finalización. [15]

3.1.5.1. Modelo PHVA

La seguridad absoluta no es posible y no existe un sistema totalmente seguro, por lo que el factor de riesgo siempre es latente sin importar las medidas que se tomen. [29] Para tratar de mitigar esa realidad, la seguridad de la información se ha definido como un proceso continuo que se debe actualizar, refinar y mejorar constantemente, permitiendo a cada organización utilizar los instrumentos que considere oportunos para medir y controlar la mejora del sistema. Por eso, la familia ISO 27000 adopta el modelo de mejora continua PHVA (Planificar, Hacer, Verificar y Actuar) aplicado a toda la estructura de procesos del SGSI.

En la fase de Planificación se realiza una evaluación de la organización donde se evalúa el estado en seguridad, el resultado de este estudio definirá las medidas que se deben implementar en respuesta a las necesidades detectadas. La información tiene diferentes valores y diferentes tipos de riesgos, lo cual conlleva a que se deba realizar un Análisis de Riesgos que valore los activos de la información. De igual forma este estudio permitirá entender las vulnerabilidades a las que la organización está expuesta. [30]

Así mismo es necesario realizar una gestión de los riesgos detectados y reducirlos en la medida de lo posible, el resultado final después de aplicar el análisis y la gestión de riesgo, son una seria de controles necesarios para reducir los riesgos.

En la fase de Hacer del Modelo PHVA se realiza la implementación de los controles de seguridad seleccionados por la organización en la fase anterior, estos controles hacen referencia a fenómenos más técnicos como son la documentación necesaria. De igual forma en esta fase se realiza uno de los elementos vitales en el proceso y son las campañas de concientización y formación que permite dar a conocer a todos los actores de la organización qué se está haciendo y por qué. [30]

Siguiendo el Modelo PHVA, la siguiente es la fase de Verificar. En ella se valora la validez de los controles implementados, de ahí radica la importancia de contar con todos los registros e indicadores desarrollados al momento de definir y desarrollar los controles en las fases anteriores.

El Modelo PHVA se finaliza con la fase de Actuar en ella se realizan las actividades relacionadas con el mantenimiento del sistema, si en el desarrollo de la fase anterior, la fase de verificar se detectó algún problema, ese problema es mejorado y corregido en esta fase del proceso. [30]

Al terminar la ejecución de las cuatros fases se tienen en cuenta los resultados de la última fase y se inicia nuevamente con la primera.

En la etapa del diseño metodológico del presente trabajo de grado, se amplía la información referente a la implementación del SGSI mediante el modelo PHVA.

3.1.6. Conceptos básicos de seguridad

Para comprender los procesos que involucra la implementación de un SGSI, antes es necesario aclarar algunos conceptos:

3.1.6.1. Activo

El principal activo que tienen las organizaciones es la información, la cual debe ser protegida frente a riesgos y amenazas para asegurar el adecuado funcionamiento de la empresa. Esta información que es necesaria asegurar se denomina activo de seguridad de la información. Para identificación completa de los activos es necesario ampliar la visión y tener en cuenta más elementos que sólo hardware y software, puesto que

contiene información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [22]

Los activos pueden dividirse en diferentes tipos según su naturaleza:

Servicios: Se refiere a la función que satisface una necesidad de los usuarios (del servicio). [31]

Datos/Información: Los datos son el corazón que permite a una organización prestar sus servicios. La información es un activo abstracto que es almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o es transferido de un lugar a otro por los medios de transmisión de datos. [22]

Aplicaciones: Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este tipo se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios. [31]

Equipos informáticos: Son los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, convirtiéndose en depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos. [31]

Redes de comunicación: Incluye tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro. [22]

Soportes de información: Aquí se encuentran los dispositivos físicos que permiten almacenar información de forma permanente o al menos, durante largos periodos de tiempo. [31]

Equipamiento auxiliar: Se refiere a otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos. [22]

Instalaciones: Son los lugares donde se hospedan los sistemas de información y comunicaciones. [31]

Personal: Son las personas que explotan u operan los elementos anteriores.

Intangibles: Junto a los demás activos, hay que tener en cuenta aquellos intangibles como la imagen y la reputación de una empresa.

3.1.6.2. Vulnerabilidad

Los Activos de Seguridad de la Información pueden tener vulnerabilidades, es decir, circunstancias o características que representan una debilidad, permitiendo la materialización de ataques que comprometan la confidencialidad, integridad o disponibilidad del mismo. [32]

Dicho de otra manera, la incapacidad de resistencia cuando se presenta un fenómeno amenazante es conocida como vulnerabilidad. Por ejemplo, un equipo será vulnerable a los virus si no tiene un programa antivirus instalado. [15]

Las vulnerabilidades pueden estar ligadas a aspectos organizativos (procedimientos mal definidos o sin actualizar, ausencia de políticas de seguridad), al factor humano (falta de formación y/o de sensibilización del personal con acceso a los recursos del sistema), a los propios equipos, a los programas y herramientas lógicas del sistema, a los locales y las condiciones ambientales del sistema (deficientes medidas de seguridad física, escasa protección contra incendios, mala ubicación de los locales con recursos críticos para el sistema, etc.) [32]

3.1.6.3. Amenaza

Aclarando el término de amenaza mencionado en la definición de vulnerabilidad, una amenaza es un evento o incidente provocado por una entidad natural, humana o artificial que aprovechando una o varias vulnerabilidades de un activo, pone en peligro la confidencialidad, la integridad o la disponibilidad de ese activo. Por tal motivo, se puede afirmar que una amenaza explota la vulnerabilidad del activo. [15]

Una amenaza actúa de formas inesperadas para aprovecharse de las vulnerabilidades de los sistemas, servicios o redes de información y tiene el potencial de causar incidentes no deseados a los activos expuestos por las vulnerabilidades. [18]

Las amenazas pueden ser clasificadas de acuerdo al elemento que las provoca, bien sean personas, amenazas lógicas o amenazas físicas.

De manera intencionada o accidental, las personas son las responsables de la mayoría de ataques a los sistemas, causando cuantiosas pérdidas.

Al hablar de personas, las amenazas suelen relacionarse con piratas informáticos que intentan conseguir el máximo nivel de privilegios aprovechando riesgos lógicos del sistema, pero pocas organizaciones tienen en cuenta a la hora de diseñar una política de seguridad otros mortíferos factores.

El personal de la compañía puede comprometer significativamente la seguridad de la información, ya sea con ataques intencionados pasando por alto la confianza que se le ha dado, o accidentalmente por un error o por desconocimiento de las normas básicas de seguridad. [23]

Ex-empleados disgustados con la organización también pueden aprovechar sus conocimientos del sistema para violentar la seguridad y realizar acciones indebidas al interior de éste, poniendo en jaque la continuidad del negocio.

Los curiosos son los atacantes más habituales del sistema y en la mayoría de las ocasiones solo tienen como objetivo enterarse de información que no se les ha comunicado. Aunque este tipo de ataques no suelen ser destructivos, violan el principio de confidencialidad de la información.

También existen amenazas provocadas por hackers, personas que utilizan sus amplios conocimientos informáticos para descubrir las debilidades de la red informática y acceder de manera ilegítima.

Muy similar a los hackers, los cracker también acceden a la red de manera ilegítima utilizando sus conocimientos, sólo que en éste caso con la intensión de destrozar, robar o modificar los elementos del sistema informático.

Por la misma línea existen intrusos remunerados, los cuales son piratas con gran experiencia en seguridad que son contratados por una persona externa para robar información o simplemente desprestigiar la compañía.

En cuanto a las amenazas lógicas, se pueden encontrar todo tipo de programas que de una forma u otra pueden dañar el sistema, son creados de forma intencionada o simplemente por un error. [23]

Un software puede tener errores de programación (llamados bugs), que pueden ser aprovechados por programas maliciosos (llamados exploits) para atacar el sistema.

La implementación de herramientas de seguridad, representan un arma de doble filo, ya que así como se utilizan para detectar y solucionar fallos en el sistema, de la misma manera un intruso las puede utilizar para identificar esos fallos y atacar.
Pueden aparecer canales cubiertos, los cuales son canales de comunicación que transmiten la información a otros (locales o remotos) que no están autorizados para acceder a esa información.

Otros elementos como puertas traseras, bombas lógicas, virus, gusanos y caballos de Troya mencionados en el tema de los elementos vulnerables en el sistema informático, también representan una amenaza lógica.

Finalmente, las amenazas físicas que pueden afectar el funcionamiento de los sistemas son robos, sabotajes, destrucción de los sistemas, cambios fluctuaciones bruscas en el suministro eléctrico, condiciones atmosféricas que afecten el comportamiento de los componentes informáticos y catástrofes bien sea naturales o artificiales. [23]

3.1.6.4. Riesgo

Si una amenaza aprovecha una vulnerabilidad en los sistemas de información para causar daño, se habla de riesgo. Un riesgo es la apreciación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.
Por lo tanto, el riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. [22]

Para una empresa que cuente con un SGSI, es de vital importancia gestionar los riesgos, para evitar que se materialicen y afecten el normal funcionamiento de la compañía.

Gestión de riesgos: Alienados con los objetivos y estrategias de la organización las actividades propias del tratamiento de los riesgos permiten desarrollar un plan de seguridad que implementado y en ejecución cumpla con los objetivos propuestos con el nivel de riesgos asumido y aceptado por la alta gerencia. A este conjunto de actividades se le conoce como Proceso de Gestión de Riesgos.

En su libro Seguridad de la Información, Redes, Informática y Sistemas de Información, Javier Areitio define la gestión de riesgos como "*el proceso que se encarga de identificar y cuantificar la probabilidad de que se produzcan amenazas y de establecer un nivel aceptable de riesgo para la organización, considerando el impacto potencial de un incidente no deseado*." [33]

En la *Figura 2 Gestión de Riesgos*, la cual es presentada a continuación, resume las actividades de gestión del riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso del SGSI:

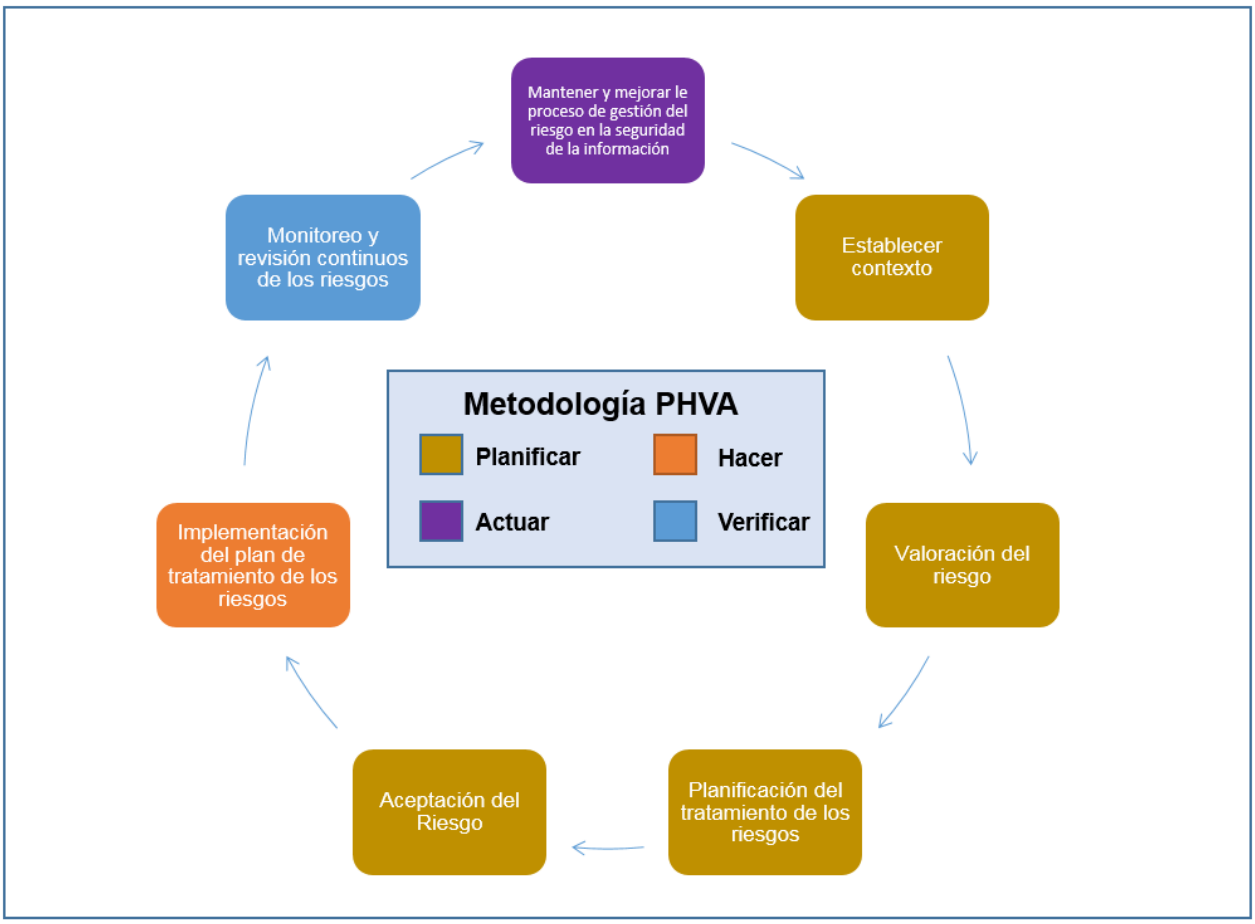


Figura 2 Gestión de Riesgos.

La gestión de riesgos contiene los siguientes procesos:

Análisis y valoración: El análisis es un proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización. [22]

El análisis de riesgos: Permite establecer cómo es, cuánto vale y el nivel de protección del sistema, además de suministrar un modelo del sistema en términos de activos, amenazas y salvaguardas, y es la piedra angular para controlar todas las actividades con fundamento. [22]

La valoración del riesgo: Determina el valor de los activos de información, identifica las amenazas y vulnerabilidades aplicables que existen (o que podrían existir), identifica los

controles existentes y sus efectos en el riesgo identificado, determina las consecuencias potenciales y, finalmente, prioriza los riesgos derivados y los clasifica frente a los criterios de evaluación del riesgo determinados en el contexto establecido. [34]

En este proceso es adecuada la implementación de posibles controles para reducir los riesgos [35]

Por tanto, la valoración de riesgo consiste en identificar los problemas antes de que aparezcan.

3.1.6.5. Metodologías de análisis de riesgos

Es importante para las organizaciones capacitarse para estar preparados en el desafío de proteger sus activos de información, esto conlleva conocer y aplicar en detalle la terminología, las metodologías, los estándares, la normatividad y las diferentes herramientas, para lograr el objetivo de seguridad. [17] Existen diferentes organizaciones internacionales que se han dado a la tarea de diseñar metodologías que le permitan a las organizaciones analizar sus riesgos. Algunas metodologías son:

MAGERIT: Es una metodología española para la gestión y análisis de riesgos de los sistemas de la información que en sus tres libros “Método”, “Catalogo de elementos” y “Guía de técnicas” sirve como fuente de revisión de definiciones y lo correspondiente a la estimación de riesgos. [35]

Elaborado por el Ministerio de Administraciones Públicas español, MAGERIT realiza el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información, [22] detallando los pasos para realizar un análisis del estado de riesgo y para gestionar su mitigación, detalla las tareas para llevarlo a cabo de manera que el proceso esté bajo control en todo momento y contempla aspectos prácticos para la realización de un análisis y una gestión realmente efectivos.

ISO/IEC 27005: Es una norma ISO Internacional que no especifica ningún método de análisis de riesgo concreto sino que, contiene recomendaciones y directrices generales para la gestión de riesgos, por tanto, puede utilizarse como guía para elaborar una metodología de gestión de riesgos propia. [36]

ISO 27005 es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que puedan complicar la seguridad de la información de la organización.

A pesar de que ISO 27005 pertenece a la serie 27000 al igual que ISO27001, esta metodología no se adentra realmente en la gestión de los riesgos, sino que se centra en el marco declarativo de determinados riesgos y no toma en cuenta un análisis de vulnerabilidades.

OCTAVE: Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE), desarrollado en EEUU por el Instituto de Ingeniería de Software (SEI) de la Universidad Carnegie Mellon, es una metodología para identificar y evaluar los riesgos de seguridad de la información.

Tiene como objetivo ayudar a la organización a desarrollar criterios de evaluación de riesgos cualitativos que describan el riesgo operacional de la organización, identificar los activos que son importantes para la misión de la organización, identificar las vulnerabilidades y amenazas a los activos, y finalmente determinar y evaluar las consecuencias potenciales para la organización si se materializan amenazas.[37]

Hay dos versiones, una para grandes organizaciones y otra para pequeñas, de menos de 100 empleados. [15]

Algunos puntos en contra de ésta metodología es que su uso interno es gratuito, pero el uso externo está limitado por el pago de la licencia para su utilización. Además requiere de profundos conocimientos técnicos y no es compatible con los estándares ISO/IEC.

NIST SP 800-30: Es una guía realizada por el Instituto Nacional de Estándares y Tecnología para la gestión de riesgos de sistemas de tecnología de la información de

Estados Unidos, [35] que proporciona una base para el desarrollo de un programa eficaz de gestión de riesgos. Contiene las definiciones y la orientación práctica necesarias para evaluar y mitigar los riesgos identificados dentro de los sistemas de TI. El objetivo final es ayudar a las organizaciones a gestionar mejor los riesgos relacionados con TI. [38]

La Metodología NIST SP 800-30 está compuesta por 9 pasos básicos para el análisis de riesgo: [38]

1. Caracterización del sistema.
2. Identificación de amenaza.
3. Identificación de vulnerabilidades.
4. Control de análisis.
5. Determinación del riesgo.
6. Análisis de impacto.
7. Determinación del riesgo.
8. Recomendaciones de control.
9. Resultado de la implementación o documentación.

CRAMM: (CCTA Risk Analysis and Management Method) es una metodología desarrollada por la agencia CCTA (Central Computer and Telecommunications Agency) del gobierno del Reino Unido. [32]

Está basada en las mejores prácticas de la administración pública británica, por lo que es más adecuada para organizaciones grandes, tanto públicas como privadas. [15]

Cramm realiza un análisis de riesgos cualitativos asociados con una herramienta de gestión. Los elementos esenciales de la recolección de datos, análisis y los resultados de salida que deben estar presentes en una herramienta automatizada de análisis de riesgos están cubiertos en las tres etapas de una revisión Cramm:

1. Identificar y evaluar los bienes.
2. Identificar las amenazas y vulnerabilidades calculando sus riesgos.
3. Identificar y priorizar las medidas de defensa o contramedidas.

Con respecto a esto, Cramm calcula los riesgos para cada grupo de activos contra las amenazas a las que es vulnerable en una escala de 1 a 7, utilizando una matriz de riesgo con valores predefinidos, comparando los valores de activos a las amenazas y niveles de vulnerabilidad. En esta escala, "1" indica una línea de base de bajo nivel de exigencia de seguridad y el “7 " indica un requisito de seguridad muy alto.

Basándose en los resultados del análisis de riesgos, Cramm produce una serie de contramedidas aplicables al sistema o red que se consideran necesarias para gestionar los riesgos identificados. [39]

Para utilizar Cramm, se debe pagar el costo de la licencia (más allá del costo de la implementación del análisis y del mantenimiento). Otro punto en contra es que no promueve la mejora continua, por lo que no representa una opción viable para las instituciones educativas.

MEHARI: La metodología MEHARI se diseñó para ayudar a los CISO (Chief Information Security Officers) en la gestión de las actividades de la seguridad de la información. [40]

El objetivo de MEHARI es proporcionar un método para la evaluación y gestión de riesgos, concretamente en el dominio de la seguridad de la información, conforme a los requerimientos de la ISO/IECE 27005:2008, proporcionando el conjunto de herramientas y elementos necesarios con su implementación. [40]

NTC 5254: Es la Norma Técnica Colombiana de Gestión del Riesgo 5254 la cual es una traducción equivalente de la norma técnica Australiana AS/NZ 4360:2004 de ancha aceptación y reconocimiento a nivel mundial para la gestión de riesgos, independiente de la industria o el negocio que desea utilizada.

La NTC 5254 tiene como objetivo proporcionar una guía para permitir que las empresas públicas, privadas o comunitarias, los grupos y los individuos logren:

1. Una base más rigurosa y confiable para la toma de decisiones y la planificación.
2. Mejor identificación de las oportunidades y las amenazas.

3. Ganar valor a partir de la incertidumbre y la variabilidad.
4. Una gestión proactiva y no reactiva.
5. Asignación y uso más eficiente de los recursos.
6. Mejorar la gestión de incidentes y la reducción en las pérdidas y el costo del riesgo. [41]

3.1.6.6. Gestión y tratamiento

El tratamiento es el proceso que buscar modificar los riesgos, existen diferentes formas de tratar los riesgos: Se pueden prevenir las características que lo provocan, disminuir las posibilidades de que suceda, reducir sus consecuencias tomando seguros con terceros o en última instancia, aceptando que pudiera suceder, destinado recursos y herramientas para actuar adecuadamente cuando sea necesario.[22]

Los cuatro tipos de tratamiento son:

Eliminar el riesgo: Aunque no revista ser la opción más factible, ya que su costo puede ser elevado o en algunos casos complicado, si se cree posible o necesario, habrá que constituir los pasos para conseguirlo: eliminar el activo, eliminar el proceso o incluso el área de negocio que es la fuente del riesgo. [15]

Transferir el riesgo: Este proceso se puede conseguir asegurando el activo que presenta el riesgo o contratando con un tercero el servicio que es afectado. Se deben evaluar las opciones y desarrollar las acciones necesarias ligadas a la opción seleccionada, es necesario tener en cuenta el costo de la solución, no solo el costo económico sino también los posibles riesgos que puede acarrear la trasferencia a un tercero. [15]

Asumir el riesgo: La alta gerencia, asume el riesgo que puede estar por debajo del valor de riesgo aceptable, es necesario dejar documentado que la dirección conoce y acepta estos riesgos. Los riesgos que se han asumido han de ser controlados y supervisados con frecuencia en miras a evitar que avancen y se conviertan en riesgos mayores. [15]

Mitigar el riesgo: Consiste en disminuirlo por medio de la implementación de controles que reduzcan el riesgo o lo lleven a un nivel mínimo, esto implica seleccionar los controles, definir los métodos de implementación y documentarlos para después aplicarlos y gestionarlos. [15]

3.1.6.7. Seguimiento y monitorización

En esta fase el control de cambios es el elemento fundamental, por lo tanto el monitoreo se debe realizar sobre todos los elementos documentados que pueden ser procesos, vulnerabilidades o amenazas con el fin de constituir acciones a seguir ante cambios (tales como agregar activos, riesgos o amenazas nuevas o que algo se modifique o requiera ser eliminado) y lograr que la gestión este continuamente actualizada para lograr evaluar indicadores de cumplimiento de los planes. [35]

Inmersos en el tema de gestión de riesgos, existen algunos conceptos adicionales que se deben tener en cuenta:

3.1.6.8. Salvaguarda

También llamadas contramedidas, son aquellos procedimientos o mecanismos tecnológicos que persiguen conocer, prevenir, impedir, reducir y controlar el daño que podría tener un sistema a causa de los riesgos. [30]

Las salvaguardas pueden actuar contra la amenaza, la vulnerabilidad, el impacto o el propio riesgo y varían con el avance tecnológico. [33]

Las salvaguardas se pueden clasificar según distintas categorías: [30]

Salvaguardas preventivas o proactivas, que persiguen anticiparse a la ocurrencia del incidente.

Salvaguardas reactivas, que persiguen reducir el daño una vez ocurre el incidente.

Salvaguarda de “no hacer nada”, o de aceptar el riesgo existente para los equipos (cuando se cumplan los criterios de aceptación de riesgo de la empresa, y sólo cuando esta decisión sea autorizada por la Dirección).

3.1.6.9. Riesgo residual

Es el riesgo resultante después de aplicar las salvaguardas o contramedidas. Por mucho que se desee proteger nuestros activos, es casi imposible eliminar todos los riesgos a un 100%, por esta circunstancia se presentan los riesgos residuales en los sistemas que deben ser asumidos y vigilados por la organización [43]

La dirección de las compañías debe ser consciente de todos los riesgos residuales, en términos de impacto y de la probabilidad de que ocurra una agresión. La decisión de asumirlos, debe adoptarse por quienes están en posición de aceptar las consecuencias de los impactos debidos a la materialización de las amenazas y por quienes pueden autorizar la implantación de salvaguardas adicionales, en caso de que los riesgos residuales no sean aceptables. [33]

3.1.6.10. Riesgo intrínseco

Es una medida del daño probable sobre un sistema sin considerar las salvaguardas que pudieran protegerlo. Se calcula para cada Situación de Riesgo, el resultado se toma de unas tablas de Impacto vs. Probabilidad, diferentes para los riesgos físicos y lógicos. [43]

En la *Figura 3 Relación Entre Elementos de Seguridad*, se muestra la relación entre los elementos de seguridad que se han mencionado hasta ahora:

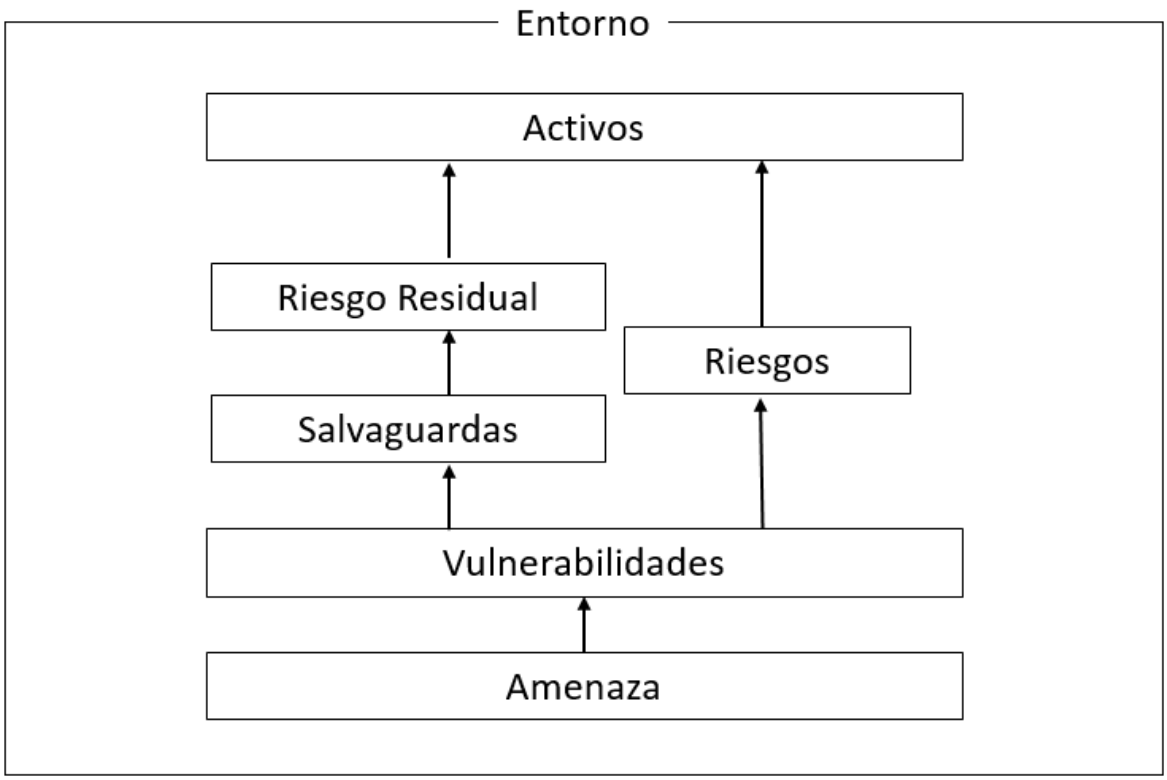


Figura 3 Relación Entre Elementos de Seguridad.

Como podemos notar en la *Figura 3 Relación Entre Elementos de Seguridad*, el nivel inferior “Amenaza” es nuestro punto de partida y como ya fue mencionado anteriormente, puede ser provocada y materializada por una entidad natural, humana o artificial, esta Amenaza se puede convertir en una Vulnerabilidad, es decir, un eslabón débil que puede permitir la ejecución de un ataque.

En el nivel siguiente podemos ver que si la Amenaza, aprovecha una Vulnerabilidad, se llega a un riesgo que podría comprometer los activos de la empresa, estos riesgos se pueden manejar con Salvaguardas (contramedidas) para conocer, prevenir, impedir, reducir y controlar el daño. Posterior a esto, podrían transformase en un Riesgo Residual y es el resultado después de aplicar todas las Salvaguardas, este puede ser asumido o no por la empresa.

Por otro lado si los riesgos no son tratados con Salvaguardas y concientizados y asumidos como Riesgos Residuales, tendrían la facultad de comprometer los activos de la

empresa de forma directa, lo cual puede ser mucho más impactante para la continuidad del negocio.

3.1.6.11. Probabilidad

En la gestión de riesgos, es muy importante el concepto de probabilidad, ya que le permite a la organización determinar cuál de los escenarios de riesgos son más proclives a materializarse dado su entorno. Este aspecto resulta de gran utilidad posteriormente cuando la organización comienza el proceso de priorización de sus actividades de mitigación de riesgos. [36]

Dependiendo del método utilizado en la gestión de riesgos, la probabilidad puede ser clasificada en diferentes escalas. A continuación se presenta un ejemplo:

- **Seguro**: No existen o no se realizan actividades de control que permitan mitigar o administrar el riesgo frente a la materialización del mismo.
- **Probable**: Se realizan algunas actividades informales pero éstas no son suficientes para mitigar o administrar el riesgo frente a la materialización del mismo.
- **Factible**: Se realizan actividades formales e informales que permiten mitigar o administrar parcialmente (no de manera preventiva) el riesgo frente a la materialización del mismo.
- **Poco probable:** Se realizan actividades formales que permiten mitigar o administrar parcialmente el riesgo frente a la materialización del mismo.
- **Remoto**: Se realizan suficientes actividades que permiten mitigar o administrar totalmente el riesgo frente a la materialización del mismo.

3.1.6.12. Impacto

Junto con la probabilidad, el impacto es un elemento fundamental en la gestión de riesgos. La NTC-ISO/IEC 27005, define el impacto como "*el cambio adverso en el nivel de los objetivos del negocio logrados*" [34]
El impacto se refiere a la medición y valoración del daño que podría producir a la organización un incidente de seguridad.

Para valorar el impacto es necesario tener en cuenta tanto los daños tangibles como la estimación de los daños intangibles**.** [32]

Al igual que la probabilidad, dependiendo del método utilizado en la gestión de riesgos, el impacto puede ser clasificado en diferentes escalas. A continuación se presenta un ejemplo:

- **Significativo**: Un riesgo que conduce a la compañía a tener inhabilidad permanente y/o generalizada para cumplir con los objetivos del plan estratégico establecido.
- **Mayor**: Un riesgo que conduce a la compañía a tener inhabilidad transitoria y/o parcial para cumplir con los objetivos del plan estratégico establecido.
- **Moderado**: Un riesgo que conduce a la compañía a tener inhabilidad esporádica y/o en ciertas áreas que le impida cumplir con los objetivos del plan estratégico establecido.
- **Menor**: Un riesgo que conduce a la compañía a tener ciertas inhabilidades que aunque existan no le impidan cumplir con los objetivos del plan estratégico establecido.
- **Insignificante**: Interrupciones puntuales en los procesos de la compañía, sin impacto en el cumplimiento del plan estratégico.

3.1.7. Estándares y Frameworks relacionados con la seguridad de la Tecnología de Información

Existen varios estándares internacionales que pueden ser utilizados como guía para la implementación de un SGSI:

3.1.7.1. COBIT

Según ISACA las siglas COBIT significan Objetivos de Control para Tecnología de Información y Tecnologías relacionadas (Control Objectives for Information Systems and related Technology). COBIT es un marco de referencia para cumplir los objetivos de control sobre la información y recursos tecnológicos asociados. [44]

Fue creado por ISACA (Information System Control Standard) la cual es una organización sin ánimo de lucro enfocada en el Gobierno y control de IT. La función principal de COBIT es ayudar a las organizaciones a mapear sus procesos de acuerdo a las mejores prácticas recopiladas por ISACA. Este marco de referencia usualmente es implementado por compañías que realizan auditorías de sistemas de información, ya sea relacionadas

Estructura de COBIT 5: COBIT 5 se basa en cinco principios claves para el gobierno y la gestión de las TI empresariales: [45]

Principio 1. **Satisfacer las Necesidades de las Partes Interesadas:** Las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos.

COBIT 5 provee todos los procesos necesarios y otros catalizadores para permitir la creación de valor del negocio mediante el uso de TI. Dado que toda empresa tiene objetivos diferentes, una empresa puede personalizar COBIT 5 para adaptarlo a su propio contexto mediante la cascada de metas, traduciendo metas corporativas de alto nivel en otras metas más manejables, específicas, relacionadas con TI y mapeándolas con procesos y prácticas específicos. [45]

Principio 2: **Cubrir la Empresa Extremo-a-Extremo:** COBIT 5 integra el gobierno y la gestión de TI en el gobierno corporativo:

Cubre todas las funciones y procesos dentro de la empresa; COBIT 5 no se enfoca sólo en la “función de TI”, sino que trata la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la empresa.

Considera que los catalizadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin, es decir, incluyendo a todo y todos – internos y externos – los que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionadas.[45]

Principio 3: **Aplicar un Marco de Referencia único integrado**: COBIT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las TIC de la empresa. [45]

Principio 4: Hacer Posible un Enfoque Holístico: Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. COBIT 5 define un conjunto de catalizadores (habilitadores) para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa. Los catalizadores se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la empresa. El marco de trabajo COBIT 5 define siete categorías de catalizadores: [45]

Catalizador 1 - Principios, Políticas y Frameworks

Catalizador 2 - Procesos

Catalizador 3 - Estructuras Organizacionales

Catalizador 4 - Culta, Ética y Comportamiento

Catalizador 5 - Información

Catalizador 6 - Servicios, Infraestructura y aplicaciones

Catalizador 7 - Personas, Habilidades y Competencias

Principio 5: Separar el Gobierno de la Gestión: El marco de trabajo COBIT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes

tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos. La visión de COBIT 5 en esta distinción clave entre gobierno y gestión es:

Gobierno*: "El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas."[44]*

Gestión: "*La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales."* [44]

El Modelo de Referencia de Procesos COBIT 5:

Procesos de Gobierno y Gestión [45]

Una de las directivas en COBIT es la distinción hecha entre gobierno y gestión. En línea con este principio, se espera que todas las empresas implementen varios procesos de gobierno y varios procesos de gestión para proporcionar un gobierno y una gestión del entorno IT exhaustivos.

Al considerar los procesos para gobierno y gestión en el contexto de la empresa, la diferencia entre los tipos de procesos se encuentra en los objetivos:

Procesos de Gobierno: Los procesos de gobierno tratan de los objetivos de gobierno de las partes interesadas, entrega de valor, optimización del riesgo y de recursos e incluye prácticas y actividades orientadas a evaluar opciones estratégicas, proporcionando la dirección de TI y supervisando la salida (Evaluar, orientar y supervisar [EDM], en línea con los conceptos del estándar ISO/IEC 38500).

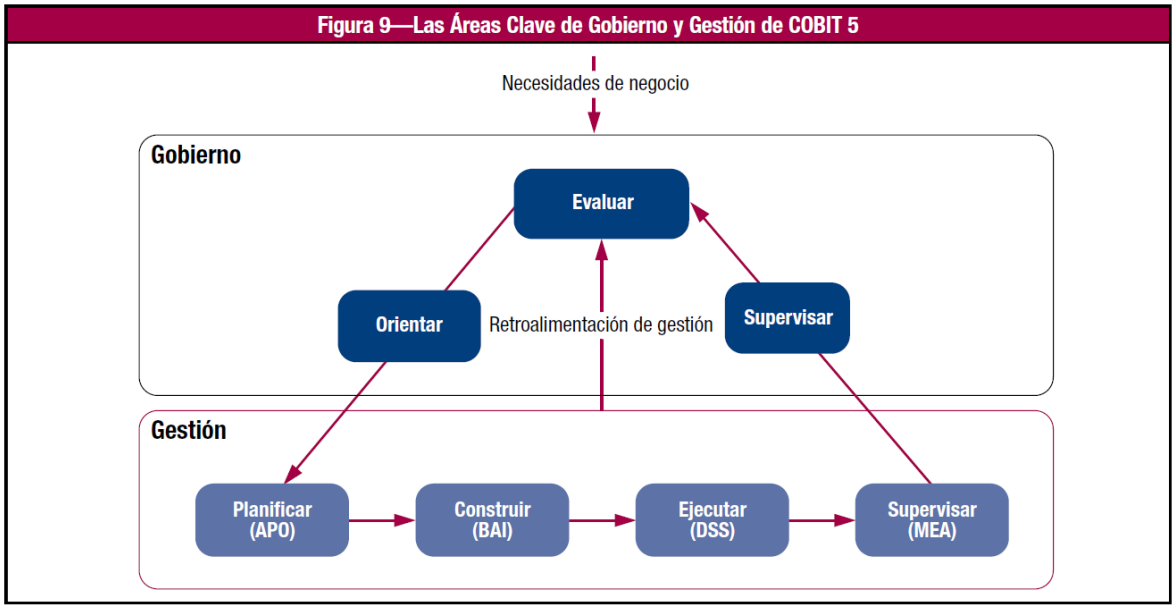
Procesos de Gestión: En línea con la definición de gestión las prácticas y actividades de los procesos de gestión cubren las áreas de responsabilidad de PBRM de TI de la empresa y tienen que proporcionar cobertura de TI extremo a extremo. [45]

Aunque las salidas de ambos tipos de procesos es diferente y está destinada a distinta audiencia, internamente, en el contexto del proceso, todos los procesos requieren

actividades de ‘planificación’, ‘construcción o implementación’,’ ejecución’ y ‘supervisión’ del proceso.

Modelo

COBIT 5 no es preceptivo, pero por lo mencionado anteriormente está claro que aboga por que las empresas implementen un gobierno y una gestión de los procesos de forma que las áreas claves estén cubiertas, como se muestra en la *Figura 4 Las Áreas Claves de Gobierno Gestión de COBIT 5*. En teoría, una empresa puede organizar sus procesos como estime conveniente siempre y cuando los objetivos básicos de gobierno y gestión estén cubiertos. Las pequeñas empresas quizás tengan menos procesos; empresas más grandes y complejas quizás tengan más procesos, todos para cubrir los mismos objetivos.



Figuran 4 Las Áreas Claves de Gobierno Gestión de COBIT 5.

COBIT 5 incluye un modelo de referencia de procesos que define y describe en detalle varios procesos de gobierno y de gestión. Esto proporciona un modelo de referencia de procesos que representa todos los procesos encontrados normalmente en una empresa respecto a las actividades de IT, ofreciendo un modelo de referencia común entendible para gerentes de operativa TI y de negocio. El modelo de procesos propuesto es

completo, exhaustivo, pero no es el único modelo posible. Cada empresa debe definir su propio conjunto de procesos, teniendo en cuenta su situación específica.

La incorporación de un modelo operacional y un lenguaje común a todas las partes de la empresa involucradas en actividades de TI es uno de los pasos más importantes y críticos hacia el buen gobierno. Esto también proporciona un marco para medir y supervisar el desempeño IT, comunicar con proveedores de servicio e integrar las mejores prácticas de gestión.

El modelo de referencia de procesos de COBIT 5 subdivide los procesos de gobierno y de gestión de TI de la empresa en dos principales áreas de actividad; gobierno y gestión, divididas en dominios de procesos:

Gobierno: Este dominio contiene cinco procesos de gobierno; dentro de cada proceso, se han definido las prácticas de evaluación, orientación y supervisión (EDM). Se tiene el ciclo de monitoreo, seguimiento, dirigir y evaluar. Aquí los procesos se centran en mantener el rumbo de la corporación, asimismo se mantiene un proceso de evaluación para validar que se persigan los objetivos propuestos.

Gestión Aquí el centro es toda la parte de seguimiento, donde se preocupa por construir, hacer, ejecutar y hacer seguimiento, es decir monitorear. Aquí se hace un manejo adecuado de los recursos, bajo el uso de las buenas prácticas. Contiene 4 dominios, en consonancia con las áreas de responsabilidad de planificar, construir, ejecutar y supervisar (Plan, Build, Run and Monitor – PBRM), y proporciona cobertura extremo a extremo de las TI. Estos dominios son una evolución de los procesos y dominios de COBIT 4.1.

Los nombres de estos dominios son:

(Align, Plan and Organise, APO) 13 Procesos

(Build, Acquire and Implement, BAI) 10 Procesos

(Deliver, Service and Support, DSS) 6 Procesos

(Monitor, Evaluate and Assess, MEA) 3 Procesos

En la Figura *5 Modelo de Referencia de procesos de COBIT 5*, se muestra el conjunto completo de los 37 procesos de gobierno y gestión dentro de COBIT 5. [45]

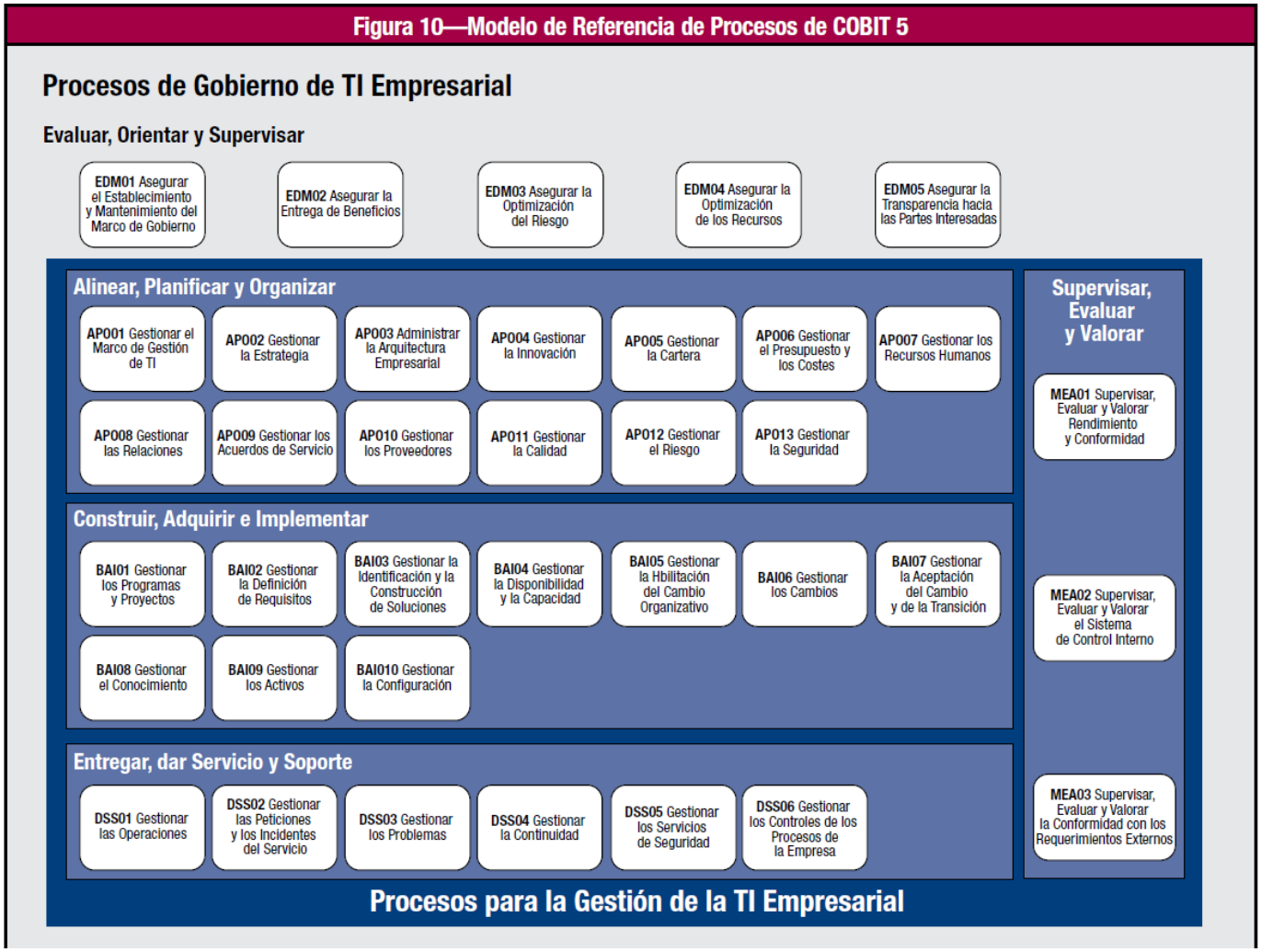


Figura 5 Modelo de Referencia de procesos de COBIT 5.

Relación de COBIT y la seguridad de la Información : En relación a la seguridad de la información en 2010, ISACA preocupado en resolver los problemas que de forma común afectan la seguridad de la información, decidió emitir una guía completa que aborda aspectos de personas, procesos de la organización y la tecnología de la seguridad de información, esta guía es el resultado de dos años de investigación y se denomina el

Modelo de Negocio para la Seguridad de Información (Business Model for Information Security, BMIS), disponible como un descargado de forma gratis en www.isaca.org/bmis.

El BMIS es adaptable a empresas de diferentes tamaños y tiene compatibilidad con otros marcos de seguridad ya existentes, puede ser adaptado en cualquier país sin importar sus regulaciones normativas, además cubre desde la privacidad y seguridad tradicional de la información hasta proporcionar vínculos a diferentes riesgos, seguridad física y cumplimiento.

Como ya fue mencionado el BMIS está orientado a la empresa, centrándose en las personas y procesos, además de la tecnología. Este modelo puede ser descargado de forma gratuita y de igual forma se pueden obtener guías introductorias en el link antes mencionado.

3.1.7.2. ITIL

Desarrollada a finales de 1980, la Biblioteca de Infraestructura de Tecnologías de la Información (ITIL) se ha convertido en el estándar mundial de utilizado en la Gestión de Servicios Informáticos. Iniciado como una guía para el gobierno de UK, la estructura base ha demostrado ser útil para las organizaciones en todos los sectores a través de su adopción por innumerables compañías como base para consulta, educación y soporte de herramientas de software. Hoy, ITIL es conocido y utilizado mundialmente. Pertenece a la OGC[1], pero es de libre utilización. [46]

ITIL fue desarrollada al reconocer que las organizaciones dependen cada vez más de la Informática para alcanzar sus objetivos corporativos. Esta dependencia en aumento ha dado como resultado una necesidad creciente de servicios informáticos de calidad que se correspondan con los objetivos del negocio, y que satisfagan los requisitos y las expectativas del cliente. A través de los años, el énfasis pasó de estar sobre el desarrollo de las aplicaciones TI a la gestión de servicios TI. La aplicación TI (a veces nombrada como un sistema de información) sólo contribuye a realizar los objetivos corporativos si el

[1] Open GeoSpatial Consortium (OGC) El OGC es un consorcio internacional fundado en 1994, sin ánimo de lucro, líder en el desarrollo de estándares para servicios geoespaciales.

sistema está a disposición de los usuarios y, en caso de fallos o modificaciones necesarias, es soportado por los procesos de mantenimiento y operaciones.

A lo largo de todo el ciclo de los productos TI, la fase de operaciones alcanza cerca del 70-80% del total del tiempo y del costo, y el resto se invierte en el desarrollo del producto (u obtención). De esta manera, los procesos eficaces y eficientes de la Gestión de Servicios TI se convierten en esenciales para el éxito de los departamentos de TI. Esto se aplica a cualquier tipo de organización, grande o pequeña, pública o privada, con servicios TI centralizados o descentralizados, con servicios TI internos o suministrados por terceros. En todos los casos, el servicio debe ser fiable, consistente, de alta calidad, y de costo aceptable. [46]

ITIL y buena práctica en la Gestión del Servicio: ITIL es una fuente de buenas prácticas en la Gestión del Servicio. Se aplica en organizaciones de todo el mundo para establecer y mejorar las capacidades en la gestión del servicio. ISO/IEC 20000 proporciona un estándar formal y universal para las organizaciones que deseen auditar y certificar sus capacidades de Gestión del Servicio. [46]

Mientras que ISO/IEC 20000 es un estándar a cumplir y mantener, ITIL ofrece una estructura de conocimiento útil para cumplir el estándar.

La Biblioteca ITIL incluye los siguientes componentes:

El Núcleo de ITIL: Guía de la mejor práctica aplicable a todos los tipos de organizaciones que proporcionan servicios para un negocio.

El Núcleo de ITIL se compone de cinco publicaciones, tal cual como se puede observar en la *Figura 6 Núcleo de ITIL*, cada una de ellas proporciona la guía necesaria para un método integrado, tal y como requiere la especificación del estándar ISO/IEC 20000:

- Estrategia del Servicio.
- Diseño del Servicio.
- Transición del Servicio.
- Operación del Servicio.

- Mejora Continua del Servicio.

A continuación se explicarán brevemente cada una de ellas: [46]

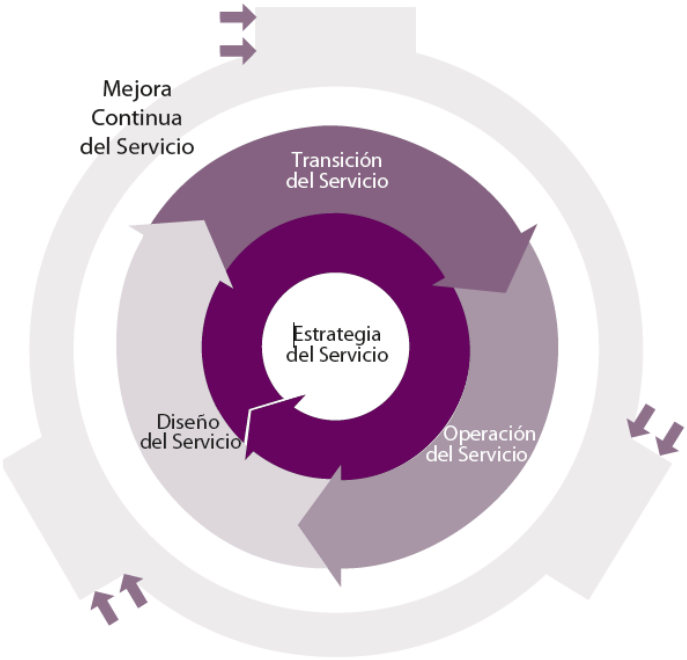


Figura 6 Núcleo de ITIL.

Estrategia del Servicio: La publicación Estrategia del Servicio proporciona la guía para diseñar, desarrollar e implementar la Gestión del Servicio, no sólo como una capacidad organizativa, sino también como un activo estratégico. Se proporciona una orientación sobre los principios que sustentan la práctica de la Gestión del Servicio y que resultan útiles para el desarrollo de las políticas, guías y procesos de Gestión del Servicio durante todo el Ciclo de Vida del Servicio de ITIL. La guía Estrategia del Servicio resulta útil en el contexto de Diseño del Servicio, Transición del Servicio, Operación del Servicio y Mejora Continua del Servicio. Los temas incluidos en Estrategia del Servicio incluyen

Diseño del Servicio: La publicación Diseño del Servicio proporciona una guía para el diseño y el desarrollo de servicios y procesos de Gestión del Servicio. Recoge los principios y métodos de diseño que permiten transformar los objetivos estratégicos en

portfolios de servicios y activos del servicio. El ámbito de Diseño del Servicio no se limita a nuevos servicios.

Transición del Servicio: La publicación Transición del Servicio proporciona una guía para el desarrollo y mejora de capacidades que permitan transformar servicios nuevos y modificados en operaciones. Esta publicación pone a disposición una guía sobre cómo los requisitos de la Estrategia del Servicio que se codifican en el Diseño del servicio se materializan de forma eficaz en operaciones del servicio mientras se controlan los riesgos de fallo y discontinuidad.

Operación del Servicio: La publicación contiene prácticas sobre la gestión de Operación del Servicio. Incluye una guía para lograr eficacia y eficiencia en la entrega y el soporte de servicios que garanticen el valor para el cliente y el proveedor de servicio. Los objetivos estratégicos se materializan en última instancia a través de Operación del Servicio, por lo que se convierte en una capacidad crítica. Se da una orientación para saber cómo mantener la estabilidad de las operaciones del servicio, mientras se permiten cambios en el diseño, escala, ámbito y niveles de servicio.

Mejora Continua del Servicio: Esta publicación proporciona una guía instrumental sobre la creación y mantenimiento del valor que se ofrece a los clientes a través de la mejora del diseño, transición y operación de los servicios. Combina principios, prácticas y métodos a partir de la gestión de la calidad, Gestión de Cambios y mejora de la capacidad. Las organizaciones aprenden a realizar mejoras graduales y a gran escala en la calidad del servicio, en la eficiencia operativa y en la continuidad del negocio.

La Guía complementaria de ITIL: Un conjunto complementario de publicaciones con una guía específica para sectores industriales, tipos de organizaciones, modelos operativos y arquitecturas tecnológicas. [46]

La guía que se incluye en ITIL puede adaptarse para que pueda ser empleada en diversos entornos de negocio y estrategias organizativas. La Guía Complementaria de ITIL proporciona flexibilidad para implementar el Núcleo en un rango diverso de entornos. Los profesionales pueden seleccionar la Guía complementaria en función de sus

necesidades para impulsar el Núcleo en un contexto de negocio dado, de igual forma que se seleccionan los neumáticos según el tipo de automóvil, el propósito y las condiciones de la carretera. Esto permite ampliar la duración y la portabilidad de los activos del conocimiento y proteger las inversiones en las capacidades de Gestión del Servicio.

3.1.7.3. Serie ISO 27000

La Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC), aprobaron y publicaron como estándar internacional un conjunto de normas que sirven como guía en la implementación de un SGSI, con rangos de numeración reservados que van desde la 27000 hasta la 27017 y desde la 27030 hasta la 27044.[47]

El Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), adaptó algunas normas de ésta serie de acuerdo a la legislación Colombiana, facilitando a las empresas nacionales adoptar las medidas necesarias y certificar en ISO27001.

A continuación se describe brevemente el alcance de las principales normas:

- ISO 27000: (Términos, definiciones y visión general)
- ISO 27001: Especificaciones de un SGSI (Certificable)
- ISO 27002: Código de buenas prácticas
- ISO 27003: Guía de implantación
- ISO 27004: Métricas e Indicadores
- ISO 27005: Guía para el Análisis y Gestión del Riesgo
- ISO 27006: Especificaciones para organismos certificadores
- ISO 27007: Guía de requisitos para entidades auditoría y certificación
- ISO 27035: Gestión de incidentes de seguridad.

A través del uso de la familia ISO 27000 sobre SGSI, las organizaciones pueden desarrollar e implementar un marco para la gestión de la seguridad de sus activos de información incluyendo información financiera, propiedad intelectual y detalles de los empleados, o la información confiada a ellos por los clientes o terceros. [48]

Para el desarrollo del presente trabajo de grado, se toman como guía las siguientes normas:

ISO/IEC 27000:2014: Contiene cláusulas y definiciones que se emplean en toda la serie 27000 y proporciona una visión general de SGSI. La aplicación de cualquier estándar necesita de un vocabulario claramente definido que evite distintas interpretaciones de conceptos técnicos y de gestión. [46]

Esta Norma Internacional es aplicable a todos los tipos y tamaños de organización. [47]

La versión más reciente de esta norma fue publicada en 2014 y aún no ha sido adoptada por ICONTEC. Por tal motivo, para el presente trabajo de grado se emplea la versión original publicada por ISO e IEC.

ISO/IEC 27001:2013: ISO/IEC 27001 es el estándar internacional para la gestión de la seguridad de la información. Define cómo poner en práctica un SGSI evaluado independientemente y certificado. Esto le permite asegurar más eficientemente toda la información confidencial de manera que reduzca la posibilidad de acceder a la misma de manera ilegal o sin autorización. [49]

ISO 27001 es la norma más utilizada y extendida que sienta las bases para el establecimiento de un SGSI. Incluye los diferentes requisitos necesarios para la evaluación y el tratamiento de los riesgos de seguridad de la información. Los requisitos establecidos en la norma ISO / IEC 27001: 2013 son genéricos y se pretende que sean aplicables a todas las organizaciones, sin importar su tipo, tamaño o naturaleza. [50]

El Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) realizó una adopción idéntica de este estándar internacional, titulándolo NTC-ISO-IEC 27001 TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. REQUISITOS [27].

Siguiendo el modelo PHVA, la NTC-ISO-IEC 27001 recomienda abordar los siguientes ítems en la elaboración de un SGSI:

Contexto de la organización: La organización debe conocer y comprender las características actuales del negocio, sus necesidades, expectativas y el alcance de la aplicabilidad del SGSI.

Liderazgo: La alta dirección debe demostrar liderazgo y compromiso con respecto al SGSI, estableciendo las políticas adecuadas y asegurándose de que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen. [27]

Planificación: La organización debe planificar el SGSI de acuerdo a las necesidades y expectativas inicialmente definidas, así como determinar los riesgos y oportunidades que es necesario tratar.

También debe definir y aplicar un proceso de valoración y tratamiento de riesgos de la seguridad de la información. [27]

Soporte: La organización debe definir y suministrar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continúa del SGSI, definiendo personal competente para su implementación. [27]

Es deber de la organización comunicar y generar conciencia en el recurso humano, sobre las políticas definidas y su importancia para la organización.

Asimismo, debe documentar y actualizar la información referente al SGSI implementado.

Operación: La organización debe implementar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información y para implementar las acciones determinadas en la etapa de planeación. [27]

Evaluación de desempeño: La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información. Para ello debe llevar a cabo auditorías internas a intervalos planificados.

La alta dirección debe revisar el sistema de gestión de la seguridad de la información de la organización, para asegurarse de su conveniencia, adecuación y eficacia continuas. [27]

Los elementos de salida de la revisión por la dirección deben incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio en el sistema de gestión de la seguridad de la información. [27]

Mejora: La organización debe mejorar continuamente la conveniencia, adecuación y eficacia del sistema de gestión de la seguridad de la información.

Cuando ocurra una no conformidad, la organización debe reaccionar y tomar las acciones necesarias para controlarla y corregirla.

La aplicación de la ISO27001 permite:

- Reducir la incertidumbre por el conocimiento de los riesgos e impactos asociados,
- La mejora continua en la gestión de la seguridad de la información
- Reducir el riesgo por mal uso, pérdida, no disponibilidad, etc. de la información, Evitar virus informáticos, fraudes, espionaje, vandalismo, etc.
- Garantizar la continuidad del negocio.
- Reducir los costos y tiempo asociados a los incidentes.
- Mejorar la implicación y participación del personal en la gestión de la seguridad.
- Mejorar la confianza de clientes y partners
- Cumplir la legislación vigente referente a la seguridad de la información.
- Mejorar la imagen de la compañía a nivel internacional.

En general, es un elemento diferenciador frente a la competencia.

La ISO27001:2013 es la primera revisión de la versión ISO27001:2005. Antes La primera versión de la ISO27001, fue publicada en octubre de 2005, basándose en la ISO 17799. La versión 2005 fue revisada y mejorada en diciembre de 2013. En comparación con la versión anterior, la 2013 está “mejor enfocada” hacia la valoración del funcionamiento del SGSI por los resultados operativos relacionados con el cumplimiento de los objetivos de seguridad. [51]

- Los cambios más representativos al comparar la versión 2005 y la 2013 de la ISO27001 son:
- En esta nueva versión aparece la necesidad de homogeneizar la estructura y cohesión con otros estándares.
- Ofrece mayor libertad y flexibilidad de implementación y mayor facilidad para las empresas alcanzar adhesión a este estándar y puedan certificarse.
- Fueron eliminados temas duplicados y generalizados conceptos muy sesgados.
- Se reestructuran los capítulos y subapartados de acuerdo a la nueva estructura de alto nivel.
- Se enfoca en las necesidades de la organización y en las partes interesadas.
- Todas las definiciones que estaban en la versión 2005 han sido eliminadas y aquellas que aún son relevantes, han sido reubicadas en la ISO/IEC 27000.
- La nueva versión resalta que es necesario un sistema de Mejora Continua, pero no obliga a utilizar el modelo PHVA, sino cualquier modelo que permita lograr este fin.
- Continúan las acciones preventivas, pero ya no como un requerimiento puntual sino como parte del sistema de gestión de riesgos.
- Se exige que haya una participación de la alta administración.
- Se cambia el concepto de una Política de SGSI por el concepto de una Política de Seguridad de la Información.

- En la versión anterior, la norma era categórica en exigir ciertos documentos, mientras que la nueva versión pide que algunos procesos críticos estén documentados, pero en general es más flexible con la información documentada.
- Se referencia la ISO 31000 como base para hacer seguimiento de los riesgos.
- Los activos, vulnerabilidades y amenazas ya no son la base obligatoria para la evaluación de riesgos, sino que son un método más.
- Se emplea el concepto “consecuencias” en vez de “impacto”
- El concepto de “dueño” o “propietario” de un activo se ha reemplazado por el término “dueño del riesgo”, elevando el nivel de responsabilidad en la organización.
- Ya no hay medidas preventivas. Se fusionó en la evaluación y tratamiento del riesgo.
- La nueva norma ISO / IEC 27001:2013 es más fácil de integrar con otras normas de gestión como la ISO 9001, ISO 22301, ISO 20000, que también han sido actualizadas.
- Permite a las empresas ajustar el SGSI a sus necesidades reales y evitando sobrecargas innecesarias.
- Se piden requerimientos especiales en cuanto a la comunicación (hacer planificación y gestión de la comunicación).
- Las secciones aumentaron de 11 a 14.
- Los controles disminuyeron de 133 a 113.
- Los requisitos pasan de 102 a 130.

ISO / IEC 27002: 2013: Al igual que la 27001, la norma ISO 27002 fue publicada originalmente como un cambio de nombre de la norma ISO 17799, la cual se basaba en un documento publicado por el gobierno del Reino Unido, que se convirtió en estándar en 1995.

En 2005 se publicó la primera versión de la ISO 27002, y posteriormente se actualizó en 2013. [52]

ISO / IEC 27002: 2013 proporciona directrices para las normas de seguridad de la información de la organización y las prácticas de gestión de seguridad de la información, incluyendo la selección, implementación y gestión de los controles, teniendo en cuenta el medio ambiente riesgo seguridad de la información de la organización.

Con la actualización de esta norma, las organizaciones pueden encontrar una guía que sirva para la implementación de los controles de seguridad de la organización y de las prácticas más eficaces para gestionar la seguridad de la información. [52]

ISO 27002:2013 se estructura en 14 secciones o dominios, de donde emanan 35 objetivos de control y de estos emanan un total de 114 controles. Cada uno tiene asociada una guía de implantación. Una organización que se adecúe a este estándar tendrá en consideración cuáles de estos les aplican y cuáles no. [53]

La versión más reciente de esta norma, publicada en 2013 por ISO e IEC fue publicada por ICONTEC, en el segundo semestre 2015.

ISO / IEC 27003: 2010: La ISO 27003 provee una guía práctica para desarrollar el plan de implementación del SGSI dentro de las organizaciones. [54]

ISO / IEC 27003: 2010 se centra en los aspectos críticos necesarios para el éxito del diseño e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) según la norma ISO / IEC 27001. En él se describe el proceso de especificación y diseño de un SGSI desde su inicio hasta la producción de los planes de ejecución, define un proyecto de implantación de un SGSI y proporciona orientación sobre cómo planificar el proyecto SGSI, resultando en un plan final de ejecución del proyecto SGSI. [48]

ISO / IEC 27005: 2011: ISO / IEC 27005 proporciona directrices para la gestión de riesgos de seguridad de la información. Es compatible con los conceptos generales especificados en la norma ISO / IEC 27001 y está diseñado para ayudar a la ejecución satisfactoria de seguridad de la información basado en un enfoque de gestión de riesgos.

El conocimiento de los conceptos, modelos, procesos y terminologías que se describen en la norma ISO / IEC 27001 e ISO / IEC 27002 es importante para una comprensión completa de la norma ISO / IEC 27005.

ISO / IEC 27005 es aplicable a todo tipo de organizaciones (por ejemplo, las empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro), cuya intención es la de gestionar los riesgos que pueden comprometer la seguridad de la información de la organización. [55]

ISO / IEC 27035: 2011: ISO / IEC 27035 proporciona un enfoque estructurado y planificado para detectar, informar y evaluar los incidentes de seguridad de la información, responder y gestionar los incidentes de seguridad de la información, detectar, evaluar y gestionar las vulnerabilidades de seguridad de la información y mejorar continuamente la seguridad de la información y la gestión de incidencias, como resultado de la gestión de incidentes de seguridad de la información y las vulnerabilidades.[56]

ISO/IEC 31000: 2009: La ISO 31000: 2009 resulta de gran importancia para el presente trabajo de grado, ya que proporciona principios y directrices genéricas sobre gestión de riesgos.

De la misma forma puede ser utilizado por cualquier público, la empresa privada o de la comunidad, asociación, grupo o individuo. Por lo tanto, la norma ISO 31000: 2009 no es específica para cualquier industria o sector. [57]

Asimismo se puede aplicar a lo largo de la vida de una organización y para una amplia gama de actividades, incluidas las estrategias y decisiones, operaciones, procesos, funciones, proyectos, productos, servicios y activos. [59]

En general, la serie 27000 está enfocada en la seguridad, lo cual le hace que se complemente a los procesos manejados por COBIT o ITIL. Esta diferencia hace que la ISO 27000 tenga un alcance menor pero más profundo en el tema de seguridad de la información en comparación con ITIL o COBIT. Como el objetivo de este estándar se encuentra alineado con los objetivos propuestos en el presente trabajo de grado, se tomó

la decisión de utilizar la serie ISO / IEC 27000 como guía principal en el diseño de la propuesta de instalación de un SGSI aplicado a las instituciones educativas.

3.1.7.4. Otras normas y estándares.

De igual forma existen otras normas existentes en el contexto de este trabajo de grado las cuales serán presentadas en la *Tabla 1 Otras Normas y Estándares*, con su respectiva caracterización: [58]

Nombre	Caracterización
LEY SOX	La Ley Sarbanes-Oxley (SOX), de EE.UU., nombrada así en referencia de sus creadores, obliga a las empresas públicas nacionales de dicho país, o extranjeras inscritas en la Securities and Exchange Comission a llevar un control y almacenamiento informático estricto de su actividad. La ley nace producto de grandes escándalos financieros ocurridos en compañías norteamericanas como Enron y Worldcom, durante el año 2002, en los cuales se comprobó que información financiera fue falsificada. Esta ha tenido un alto impacto a nivel mundial en empresas que transan sus valores en la bolsa de EE.UU.
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 organizaciones. 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. En síntesis, 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. Esta normativa está dedicada a proporcionar orientación a la gestión ejecutiva y las entidades de gobierno sobre los aspectos fundamentales de organización de este, la ética empresarial, control interno, gestión del riesgo empresarial, el fraude, y la presentación de informes financieros.
VAL IT	VAL IT es un framework de gobernabilidad que se puede utilizar para crear valor de negocio de las inversiones en TI. Consiste en un conjunto de principios rectores y una serie de procesos y mejores prácticas que se los define como un conjunto de prácticas de gestión claves para apoyar y ayudar a la

	gerencia ejecutiva y juntas a nivel empresarial. La última versión del framework, publicado por el IT Governance Institute (ITGI, en inglés: IT Governance Institute), basado en la experiencia de los profesionales y académicos globales, prácticas y metodologías fue nombrado Valor de la Empresa: Gobierno de TI Inversiones, el Val IT Framework 2.0. Este cubre los procesos y prácticas de gestión claves para tres dominios específicos y va más allá de las nuevas inversiones para incluir los servicios de TI, activos, otros recursos y los principios y procesos para la gestión de la cartera de TI. Esta iniciativa, en la que se incluyen investigaciones, publicaciones y servicios de soporte, tiene como objetivo ayudar a la gerencia a abordar este reto, así como garantizar que las organizaciones logren un valor óptimo de las inversiones de negocio posibilitadas por TI, a un coste económico, y con un nivel conocido y aceptable de riesgo. Val IT constituye una extensión y complemento de COBIT, que proporciona un marco de control global para el gobierno de TI.
RISK IT	Es un marco de referencia normativo de ISACA, basado en un conjunto de principios rectores para una gestión efectiva de riesgos de TI. Es un marco de riesgos relacionados con la tecnología de la información (TI) que brinda una visión completa de los riesgos de los negocios asociados a iniciativas de tecnología de la información. Risk IT se apoya en el marco de COBIT mundialmente reconocido para la administración de TI de ISACA, para brindar un vínculo que faltaba entre la gestión de riesgos corporativos convencionales y la gestión y el control de riesgos de TI. Las empresas logran ganancias al arriesgar, pero algunas veces tratan de eliminar los verdaderos riesgos que generan ganancias. Risk IT se puede descargar gratis en www.isaca.org/riskit, y está diseñado para ayudar a las empresas a aumentar sus oportunidades de ingresos al administrar los riesgos de manera más efectiva, en lugar de tratar de eliminarlos completamente.
BMIS	Para brindar a los profesionales de la seguridad de información una guía completa que aborde los aspectos de personas, el proceso, la organización y la tecnología de la seguridad de información, ISACA emitió los resultados de dos años de investigación y de revisión experta: el Modelo de Negocio para la Seguridad de Información (Business Model for Information Security, BMIS), disponible como un descargado gratuito en www.isaca.org/bmis. El Business Modelo for Information Security es una aproximación holística y orientada al negocio para la administración de la seguridad informática, El BMIS puede utilizarse en empresas de todos tamaños y es compatible con otros marcos de seguridad de información ya existentes. Es independiente de cualquier tecnología en particular y puede aplicarse en todas las industrias, países y sistemas legales y regulatorios. Además, abarca la privacidad y seguridad tradicional de información y proporciona vínculos a riesgos, seguridad física y cumplimiento.

Tabla 1 Otras Normas y Estándares.

4. DESCRIPCIÓN DE LA SOLUCIÓN

4.1. Estructura de la solución.

Para el desarrollo de esta solución se proponen cuatro etapas que se definen a continuación:

Etapa 1: Encuesta de seguridad Informática en Colombia.

Inicialmente se realizará una revisión exhaustiva de estado de la seguridad informática en el país a partir de la encuesta Nacional de Seguridad de la Información del año 2014.

Etapa 2: Prototipo del SGSI.

En esta etapa se construirá un prototipo para la implementación de un SGSI en organizaciones del sector educación, con el fin de instalar dicho prototipo en diferentes instituciones.

Etapa 3: Marco legal.

Se ajustará el prototipo creado según la normatividad legal que es aplicable al trabajo de grado.

Etapa 4. Validación del prototipo.

Para la validación del prototipo utilizaremos como datos sintéticos de pruebas dos instituciones educativas, que para este caso serán el Centro Colombo Americano de Medellín y la Institución Universitaria Escolme.

En la *Figura 7 Estructura metodológica de solución planteada en el trabajo de grado*, se puede observar de forma más clara las etapas de la solución:

Figura 7 Estructura Metodológica de Solución Planteada en el Trabajo de Grado.

4.2. Etapa 1: Encuesta de seguridad Informática en Colombia

Para la ejecución de esta etapa se revisó la XIV Encuesta Nacional de Seguridad Informática, desarrollada en el marco de la XIV Jornada Internacional de Seguridad Informática, realizada los días 16 y 17 de junio del año 2014 en la ciudad de Bogotá.

Esta encuesta es desarrollada por la Asociación Colombiana de Ingenieros de Sistemas (ACIS) [59] y busca conocer los avances en el tema de la Seguridad de la Información.

Este estudio permite realizar un análisis de tendencias que sirven de base para diversos actores como Gobierno, Proveedores, Academia e Industria, en su toma de decisiones.

4.2.1. Estructura de XIV Encuesta Nacional de Seguridad Informática

Antes de conocer los resultados de la encuesta del año 2014, es necesario entender la estructura de la misma, la cual costa de 6 secciones:

Sección 1 Demografía: Esta sección permite trazar el perfil de los encuestados, identificando los sectores que participan, el tamaño de la organización, el personal dedicado de tiempo completo al área de seguridad, la dependencia organizacional de la seguridad y los cargos y ubicación geográfica de las personas que respondieron las preguntas.

Sección 2 Presupuestos: Esta sección muestra si las organizaciones consideran a la información como un activo y por ende, han presupuestado un rubro específico para su aseguramiento, permitiendo revisar el tipo de tecnología en el que invierten y estimar el monto de la inversión que realizan.

Sección 3 Fallas de Seguridad: Esta sección revisa los tipos de incidentes de seguridad más frecuentes, los mecanismos para su detección y a quién se notifica o bien, las causas por las cuales no se denuncian. Adicionalmente, se identifica si se reconoce la importancia de la evidencia digital en el proceso de gestión de incidentes.

Sección 4 Herramientas y prácticas de seguridad de la información: En este segmento de la encuesta, el objetivo es identificar las prácticas de las empresas sobre la seguridad de la información, los dispositivos o herramientas que con más frecuencia utilizan para el desarrollo de la infraestructura tecnológica y las estrategias que emplean para enterarse de las fallas de seguridad.

Sección 5 Políticas de seguridad: Esta sección indaga sobre la formalidad de las políticas de seguridad en la organización, los principales obstáculos para su formulación y los contactos nacionales y/o internacionales con los que cuenta para perseguir posibles intrusos.

Sección 6 Capital intelectual: Finalmente, esta sección analiza la situación del desarrollo profesional en materia de seguridad de la información: personal dedicado a esta tarea, personal certificado, importancia de las certificaciones y años de experiencia en el área.

Cada una de las secciones cuenta con un número de preguntas, las cuales son obligatorias para el encuestado, a continuación se establece la relación entre la sección y el número de preguntas en la *Tabla 2 Estructura de la Encuesta*:

Nombre de la sección	Número de Preguntas
Sección 1 Demografía	7
Sección 2 Presupuestos	5
Sección 3 Fallas de Seguridad	9
Sección 4 Herramientas y prácticas de seguridad de la información	3
Sección 5 Políticas de seguridad	6
Sección 6 Capital intelectual	7

Tabla 2 Estructura de la Encuesta.

De esta manera se tienen 37 preguntas requeridas. Al final de la encuesta se presentan 4 preguntas adicionales y opcionales para el usuario.

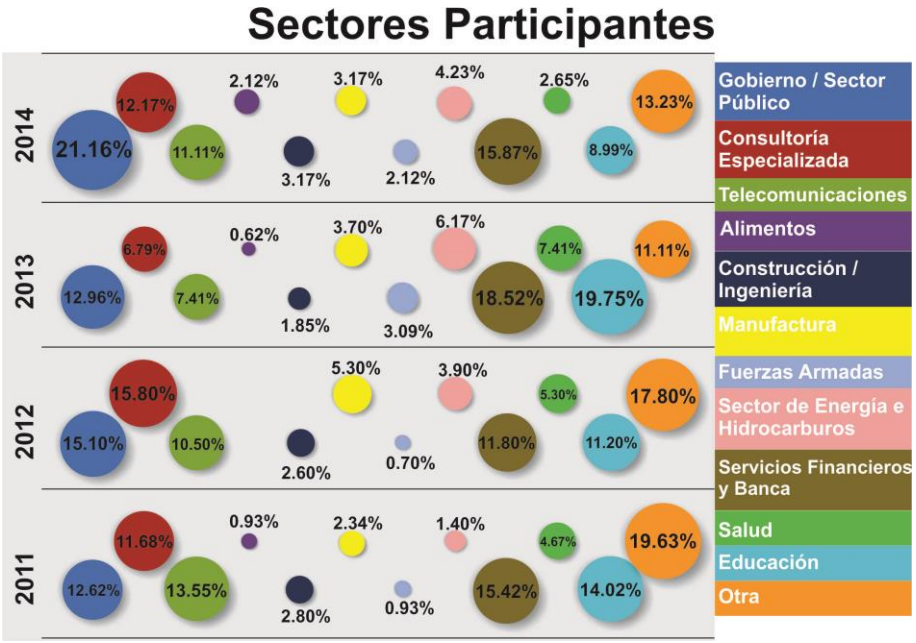
Para revisar la encuesta completa se puede revisar el Anexo 1 XIV Encuesta Nacional de Seguridad Informática.

4.2.2. Resultados de la XIV Encuesta Nacional de Seguridad Informática.

Como se mencionó anteriormente, los resultados de esta encuesta fueron presentados en el marco de la XIV Jornada Internacional de Seguridad Informática. La encuesta fue desarrollada por ACIS a través de Internet, y contó con la participación de 189 encuestados, quienes con sus respuestas permiten conocer la realidad del país. [60]

4.2.3. Sectores Participantes

En relación a este aspecto podemos observar en la *Figura 8 Sectores Participantes*, un comparativo donde se presentan los participantes de la encuesta desde el año 2011 hasta el año 2014:



Figuran 8 Sectores Participantes.

Como se puede observar, en el año 2014 la participación más alta se presentó desde el sector Gobierno /Sector público, con un 21.16% de participación, seguido por el sector Consultoría Especializada con un 12.17% y posteriormente con un 11% el sector de las Telecomunicaciones. Esta es una tendencia que se presenta de forma similar en los años anteriores.

4.2.4. Cargo de la Organización

En relación a este elemento, en la *Figura 9 Cargos en la Organización*, se muestran los cargos más relevantes que participaron en esta encuesta y se realizó un comparativo donde se evidencia cuáles subieron y cuáles bajaron en relación a los años 2013-2014:

Figura 9 Cargos en la Organización.

Se puede observar que el número más representativo para el año 2014 es en los Profesionales de Departamentos de Sistemas/Tecnología con un 23.28%, pero que comparado con el año 2013 descendió de forma leve. Se destaca el crecimiento en la participación de los Profesionales del Departamentos de Seguridad Informática que pasó de un 8.64% a un 13.23% y de igual forma se evidencia el mismo fenómeno en los Directores/Jefes de Sistemas/Tecnología que pasan de un 13.58% a 16.93%.

4.2.5. Presupuestos

En relación a los presupuestos el informe arroja datos interesantes, como que entre los años 2011-2012 se dio el mayor número de empresas que manejaron un rubro para la seguridad de la información, para mejor compresión se presenta la *Figura 10 Presupuestos 1:*

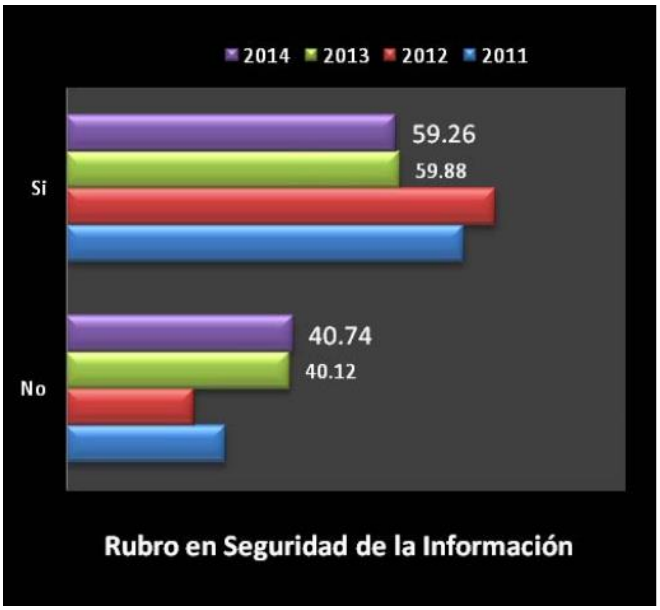


Figura 10 Presupuestos 1.

De igual forma se puede observar en la *Figura 10 Presupuestos 1,* que entre los años 2013-2014 se ha presentado una disminución en el número de empresas que manejan estos rubros, lo cual es lamentable teniendo en cuenta la importancia que la seguridad de la información tiene hoy día en las organizaciones.

De igual forma, se presenta la *Figura 11 Presupuestos 2*, donde se muestra la participación monetaria contemplada por las organizaciones:

Figura 11 Presupuestos 2.

Se puede observar un incremento en rubros de más de USD$130.000 asignados en el año 2014, este incremento equivale a un 8.34%. De igual manera incrementa en 11.71% de los encuestados que tienen presupuestos entre USD$20.000 y USD$50.000.

4.2.6. Cifras Importantes de la encuesta.

Esta sección describe las cifras que han presentado mayor y menor variación en la encuesta para 2014.

Los de mayor variación con respecto al año 2013

A continuación se describen las cifras más importantes de la encuesta para 2014:

- El 50.29% de los encuestados no realiza el análisis de riesgos de información y manifiesta que lo concibe como parte del proceso de gestión de riesgos empresariales.
- El 51.55% realiza en las organizaciones el ejercicio de evaluación de riesgos, una vez al año.
- El 47.62% no conoce el monto de las asignaciones de recursos financieros para el año 2013 en materia de seguridad de la información.
- El 50.59% reconoce las regulaciones nacionales como motivadores de los programas en materia de seguridad de la información.

- El 44.97% permanece informado sobre las fallas de los sistemas a través de sus proveedores, como el principal elemento para conocer las carencias de seguridad.
- El 23.28% de los encuestados posee la certificación CISM y es la más reconocida en el mercado nacional.
- El 34.39% afirma que fueron sus propios empleados quienes han notificado las fallas de seguridad dentro de la organización.
- El 42.78% manifiesta que tienen contactos con las autoridades nacionales e internacionales para atender casos de ciberataques.
- El 15.87% confirma en los SIEM las herramientas o mecanismos utilizados para la protección de sus redes informáticas.

Los de menor variación con respecto a 2013

Son aquellos criterios considerados por los encuestados en el año 2014, como los menos importantes. Su variación frente a años anteriores es negativa:

- El 44.97% permanece informado sobre las fallas de los sistemas a través de sus proveedores, como el principal elemento para conocer las carencias de seguridad.
- El 23.28% de los encuestados posee la certificación CISM, la cual es la más reconocida en el mercado nacional.
- El 34.39% afirma que fueron sus propios empleados quienes han notificado las fallas de seguridad dentro de la organización.
- El 42.78% manifiesta que tienen contactos con las autoridades nacionales e internacionales para atender casos de ciberataques.
- El 15.87% confirma en los SIEM las herramientas o mecanismos utilizados para la protección de sus redes informáticas.
- El 41.80% considera que la falta de colaboración entre las áreas/departamentos es un obstáculo para lograr una adecuada seguridad de la información en las organizaciones, en comparación con el 55% de años anteriores que la consideraba un obstáculo fundamental.

- El 19.58% contempla usar la buena práctica COBIT para modelar la seguridad de la información. En años anteriores este porcentaje fue de 31%.
- El 40.21% afirma que sus responsables de seguridad no poseen ningún tipo de certificación orientada a la seguridad de la información, en comparación con años anteriores, porcentaje que era del 51%.
- En años anteriores, más del 34% de los encuestados consideraba la pérdida de valor de los accionistas como motivo para no denunciar los incidentes de seguridad. Este año sólo el 23.28% consideró este punto importante para no denunciar los incidentes.
- El 36.51% de los encuestados considera que hay pocas -o nulas- alianzas con proveedores de tecnología de seguridad y/o agremiaciones relacionadas con el tema, frente a años anteriores, en que más del 47% de los encuestados consideraba este punto relevante.

4.2.7. Las nuevas preguntas

En esta etapa de la evaluación de la encuesta se analizaron los nuevos ítems que fueron incluidos en el año 2014, uno de ellos son los temas o claves relevantes que deben tener en cuenta los responsables de la seguridad de la información, los encuestados del 2014 señalan la fuga de la información como el elemento más importante a tener en cuenta, seguido de la seguridad en la nube, de igual forma las APTs o amenazas persistentes avanzadas son el tercer elemento a considerar.

Para ilustrar la situación se presenta la *Figura 12 Temas Claves*:

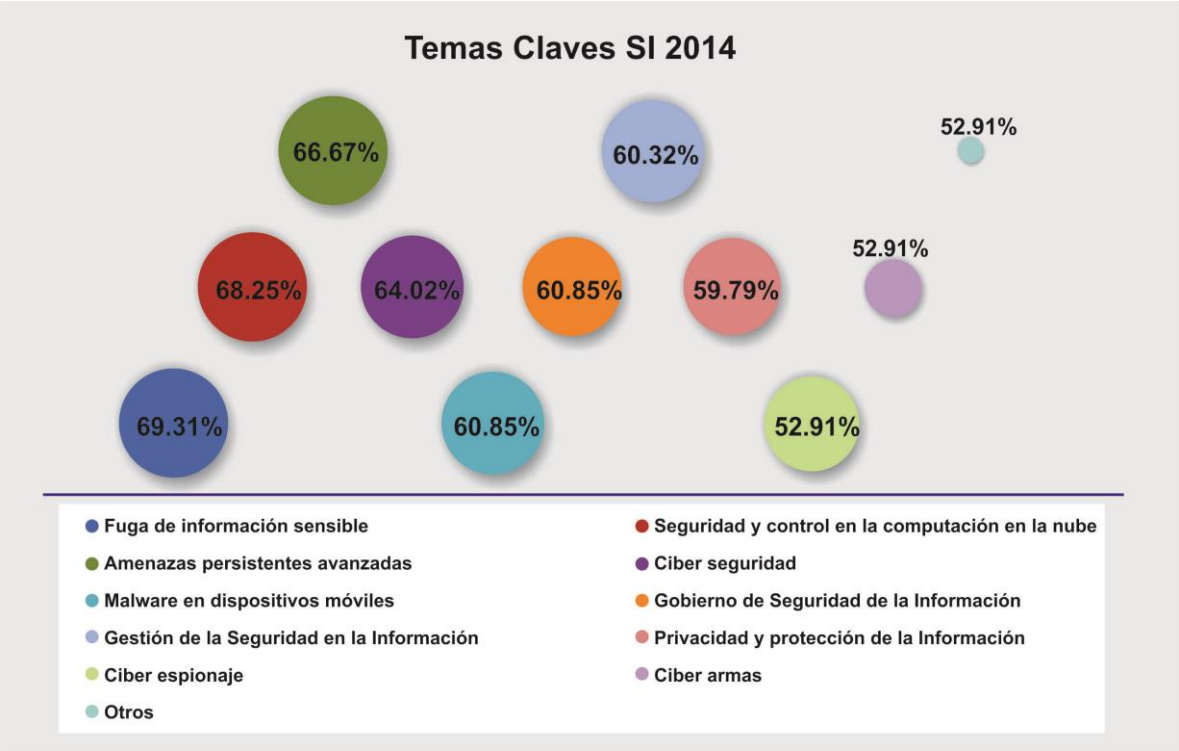


Figura 12 Temas Claves.

Dentro de este mismo grupo de preguntas nuevas, se preguntó sobre en qué actividades están más concentrados los responsables de la seguridad de la información, en la *Figura 13 Roles y Responsabilidades,* se puede apreciar las respuestas:

Figura 13 Roles y Responsabilidades.

Los resultados muestran que un 66.67% está dedicado a velar por la protección de la información empresarial; un 65.61% está encaminado a precisar los controles de TI; y en tercer lugar, un 59.79% sigue prácticas en materia de seguridad de la información.

Esto demuestra que estamos pasando de tener una visión solamente técnica a una visión más enfocada a la preocupación del negocio, de igual forma nos señala que el área de seguridad de la información es considerada como un factor determinante y necesario de establecer en las empresas para proteger la información y no solamente limitarnos a las plataformas de TI.

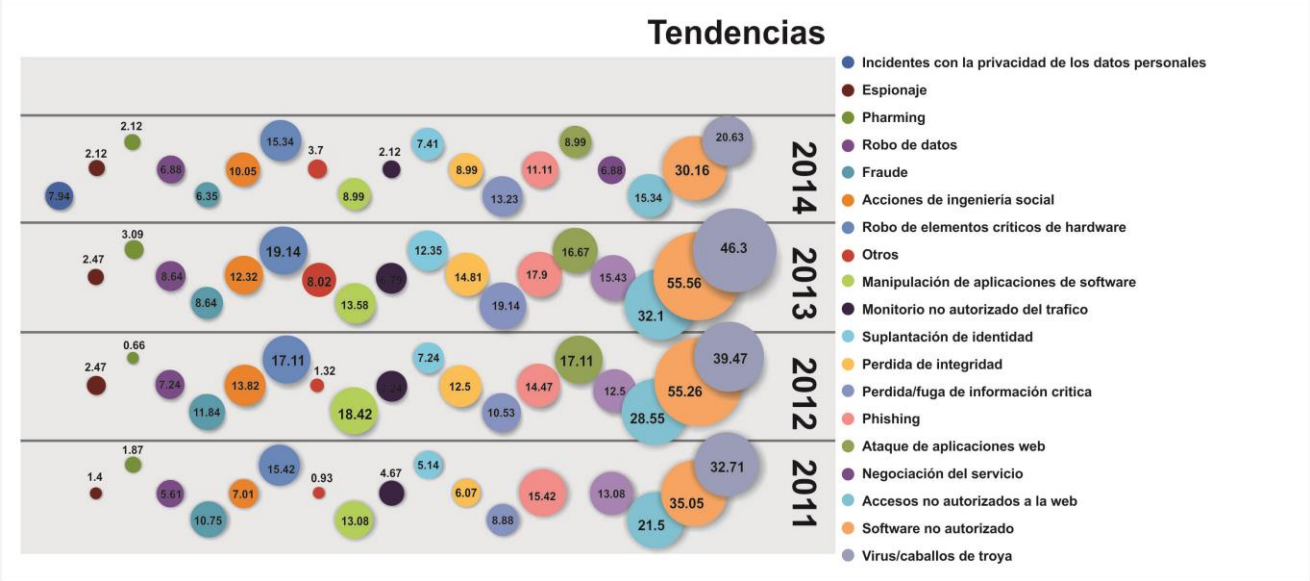
4.2.8. Tendencias

La encuesta de forma histórica ha tenido participación de diferentes actores que todos los años responden al llamado a responder la encuesta a continuación se presenta la *Tabla 3 Tendencias de Participación,* donde se resume la participación de estos diferentes actores y cómo es su participación con relación al año 2013:

Sector	Participación	Relación con años anteriores
Gobierno	18%	Incremento 8 puntos en relación al año 2013
Servicios Financieros	15.87%	Decrece en el 2013 estaba en un 18.52%
Consultoría especializada	14%	Con más de 5 puntos de incremento en su participación en relación a 2013
Telecomunicaciones	13%	Con más de 3 puntos de incremento en su participación en relación a 2013

Tabla 3 Tendencias de Participación.

De igual manera en lo referente a tendencias la encuesta nos presenta el comportamiento de las distintas anomalías electrónicas y cómo se viene comportando de forma similar en los periodos de 2011-2014. En la *Figura 14 Tendencias,* lo podemos apreciar en detalle:



Figuran 14 Tendencias.

Se puede notar que los virus/Caballos de Troya, y el software no autorizado permanecen como las anomalías más importantes presentadas en las organizaciones.

De forma similar se muestra que en relación a los virus se presentó una disminución de casi un 26% en relación a los años 2011-2013, esto denota la trasformación de este tipo de ataques a nuevas técnicas, como puede ser el secuestro de la información más conocidos como Ransomware.

La encuesta de seguridad también indagó por las herramientas tecnológicas utilizadas para diseñar infraestructuras de seguridad, entre las principales encontramos las tradicionales como firewall, antivirus, VPN, aunque se siguen utilizando presentaron un descenso en algunos casos; por ejemplo los firewalls tradicionales muestran una disminución del 22%, frente al año 2013. De igual forma en 2014 fueron incluidos los firewalls de nueva generación y las herramientas anti-DDOS que vienen tomando fuerza dentro de las organizaciones. En la *Figura 15 Herramientas de Seguridad,* se pueden apreciar en detalle los diferentes elementos mencionados:

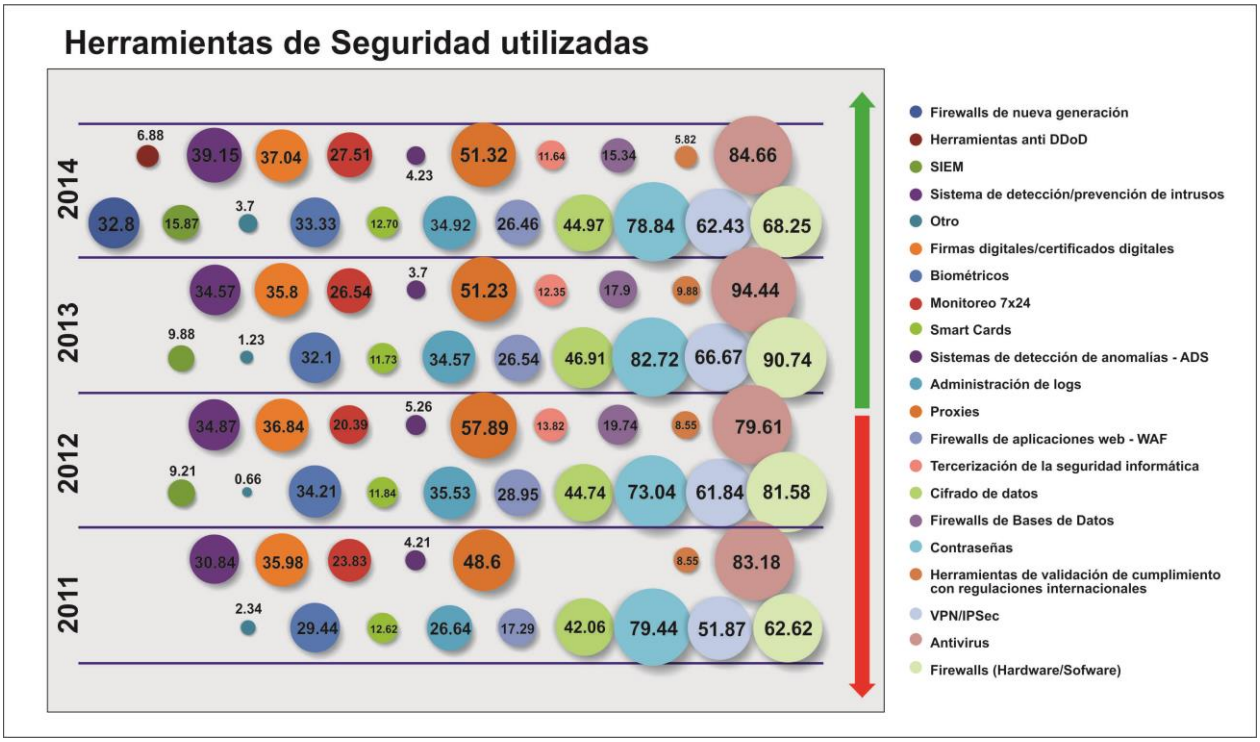


Figura 15 Herramientas de Seguridad.

Conclusiones generales encuesta de seguridad

1. Las regulaciones normativas nacionales e internacionales permiten fortalecer y apoyar los sistemas de gestión de seguridad de la información. En Colombia se tienen normas como por ejemplo las que regulan los sectores financieros o la ley Ley 1581 de 2012 proyección de datos personales.

2. En 2014 se presentaron cambios importantes frente al 2013, como son la concientización en materia de seguridad de la información, de una seguridad dedicada solo a comprar tecnología a comprender que la seguridad es un proceso más que deben tener las organizaciones.

3. Los códigos maliciosos como los virus informáticos están transformándose técnicamente y están llegando de nuevas maneras a las empresas.

4. La fuga de la información sigue siendo el elemento más importante para los encargados de la seguridad de la información así como de la seguridad en la nube, y las amenazas persistentes avanzadas.

5. Los Firewall de nueva generación, las herramientas anti-DDOS y SIEM (Security Incident and Event Management) son las herramientas de seguridad más utilizadas en Colombia.

6. Los presupuestos son uno de los mayores desafíos de los responsables de seguridad de la información; conseguir estos recursos para trazar programas enfocados a proteger la organización, es uno de los retos importantes.

7. Las certificaciones CISM, CRISC, CISA y CISSP son las más apreciadas por el mercado. El estudio mundial de las 15 certificaciones mejor pagadas de la empresa GlobalKnowledge [61], ratifica a CRISC como la certificación más popular con mayores beneficios financieros para las personas; ubica a CISM y CISSP en el segundo y tercer puestos, respectivamente; y a CISA en cuarto lugar.

8. Los estándares internacionales se vienen desarrollando en Colombia con las buenas prácticas en seguridad de la información, ISO27000, ITIL y COBIT se consolidan como marcos para edificar arquitecturas de seguridad de la información.

Después del análisis realizado se concluyó que la seguridad informática es un tema creciente pero inmaduro y en general no suficientemente valorado.

Bajo este criterio, se ratifica la necesidad de crear un sistema de gestión de la seguridad de la información como marco base, para el desarrollo de esta disciplina en el área educativa de la región.

4.3. Etapa 2: Prototipo del SGSI.

4.4.1. Introducción al prototipo propuesto.

4.4.1.1. Entendiendo del prototipo.

Lo primero que es necesario aclarar antes de presentar el prototipo, es la intensión que se tiene con el mismo; como ya se ha planteado en la “Descripción del Problema y Propuesta de Solución”, este trabajo de grado, desea lograr que las instituciones educativas tengan una herramienta para mejorar la seguridad informática al interior de sus empresas, busca además acercar a las instituciones a una posible implementación de un Sistema de Gestión de Seguridad de la Información basados en el estándar ISO27001:2013 y finalmente ayudarles a preparar el camino para una posible certificación en este estándar.

En principio se podría pensar que este prototipo lo que busca es explicar el funcionamiento del estándar ISO27001:2013, lo cual es errado y no es el propósito del mismo, para tales fines, solo es necesario comprar el estándar y revisar todos sus dominios y controles donde claramente está explicados.

Este prototipo lo que busca es ir mucho más allá, desea mostrar la estructura del estándar, profundizar en su entendimiento y brindar una serie de herramientas ligadas directamente a la estructura del estándar, donde podrán ser aplicadas de forma libre y adaptadas a sus respectivos contextos. Estas herramientas serán de gran utilidad para hacer realidad aumentar los niveles maduración en seguridad informática.

Es así como las herramientas anexas a este prototipo son un gran valor agregado que se tiene después de la investigación de años, clasificando información y entendiendo cómo se podrían establecer mecanismos sencillos que acompañen a las instituciones educativas a emprender el camino de aumentar los niveles de seguridad informática. Más adelante de forma detallada se presentarán cada una de las herramientas anexas a este trabajo de grado.

Una segunda aclaración que es necesario identificar, es el hecho que si bien este prototipo está pensando para instituciones educativas, podría ser adaptado a otros tipos de empresas que de igual modo deseen mejorar sus niveles de seguridad informática, por

medio del entendimiento del estándar, acompañados de las herramientas, antes mencionadas.

Finalmente es necesario aclarar que para el desarrollo de este prototipo se utilizará la metodología PHVA, la cual fue explicada anteriormente de este trabajo de grado.

4.4.1.2. Estructura del prototipo

El prototipo propuesto está organizado en Fases, Etapas y Procesos, en las **Fases** se especificarán las cuatro fases de la metodología PHVA y dentro de ellas se manejarán las **Etapas** principales que permitirán desarrollar cada una de estas fases. Al interior de las Etapas se encontrarán una cantidad determinada de **Procesos** que se deben realizar.

Todas estas Fases, Etapas y Procesos están basados como ya se ha mencionada en repetidas ocasiones en el estándar ISO27001:2013.

En la *Figura 16 Fases Prototipo*, se puede apreciar de forma más clara las fases del prototipo para mayor comprensión:

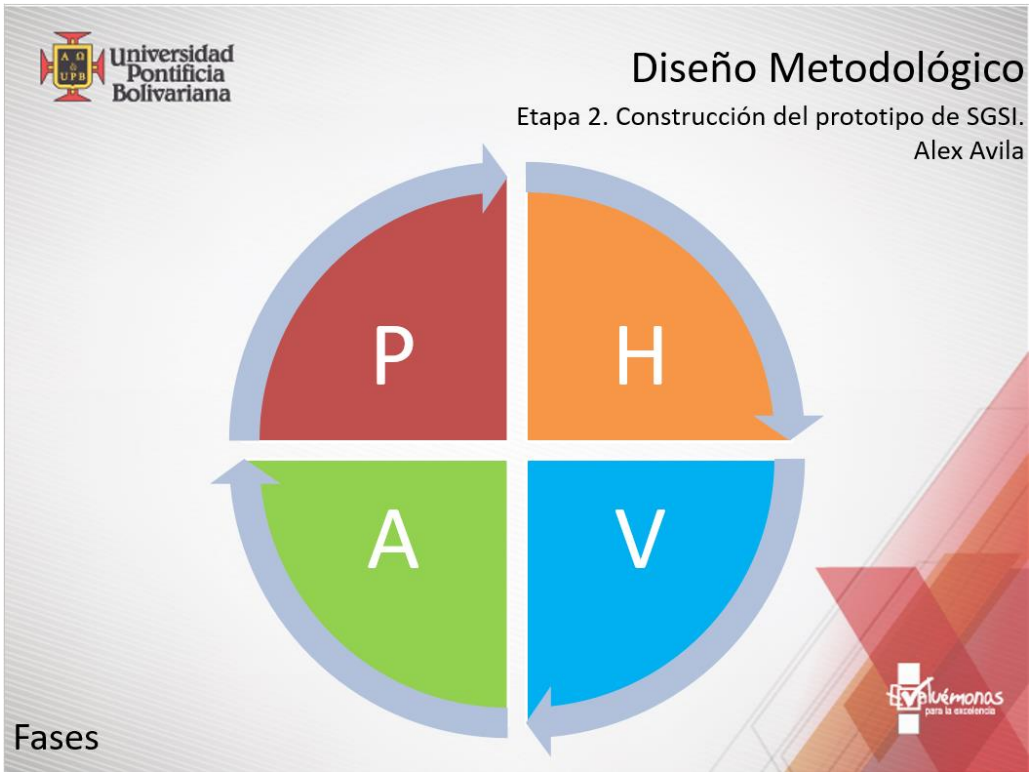


Figura 16 Fases Prototipo.

Al interior de las Fases, existe una serie de Etapas que pueden variar según la Fase donde se desarrollen, es así como por ejemplo en la Fase de Planear se tienen cuatro etapas; Contexto de la organización, Liderazgo, Planificación y Soporte, pero en la Fase de Hacer solo se cuenta con la etapa de Operación.

Para mejor compresión, a continuación se presenta la *Figura 17 Fases y Etapas Prototipo:*

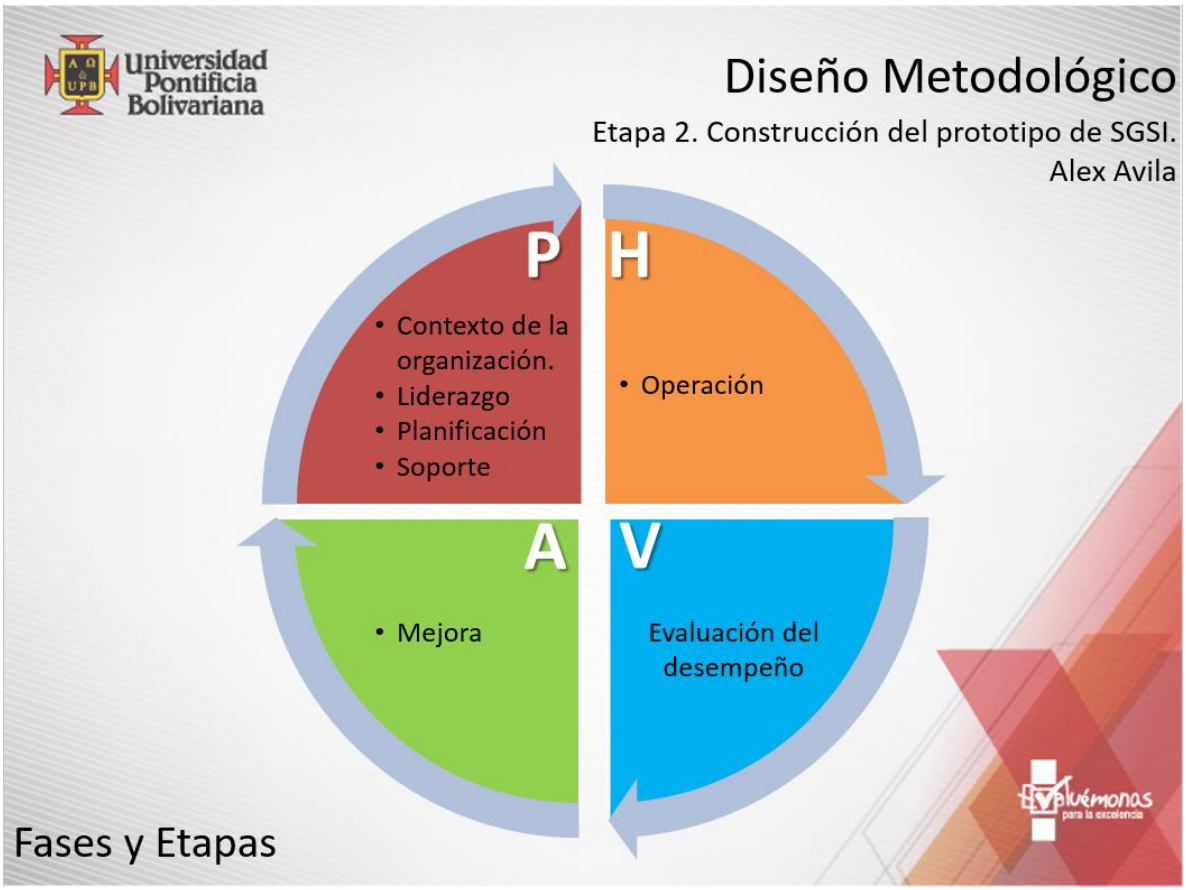


Figura 17 Fases y Etapas Prototipo.

Posteriormente al interior de las Etapas se desarrollarán una serie de Procesos que propone el estándar, estos también varían dependiendo de la Etapa en desarrollo.

A continuación se presentarán una seria de figuras que serán la hoja de ruta para aproximar a las organizaciones a la implementación del prototipo propuesto; en la *Figura 18 Fase de Planear, con Etapas y Procesos*, se puede apreciar el camino a desarrollar en toda la Fase de Planear:

Figura 18 Fase de Planear, con Etapas y Procesos.

En la *Figura 19 Fase de Hacer, con Etapas y Procesos*, se puede apreciar el camino a desarrollar en toda la Fase de Hacer:

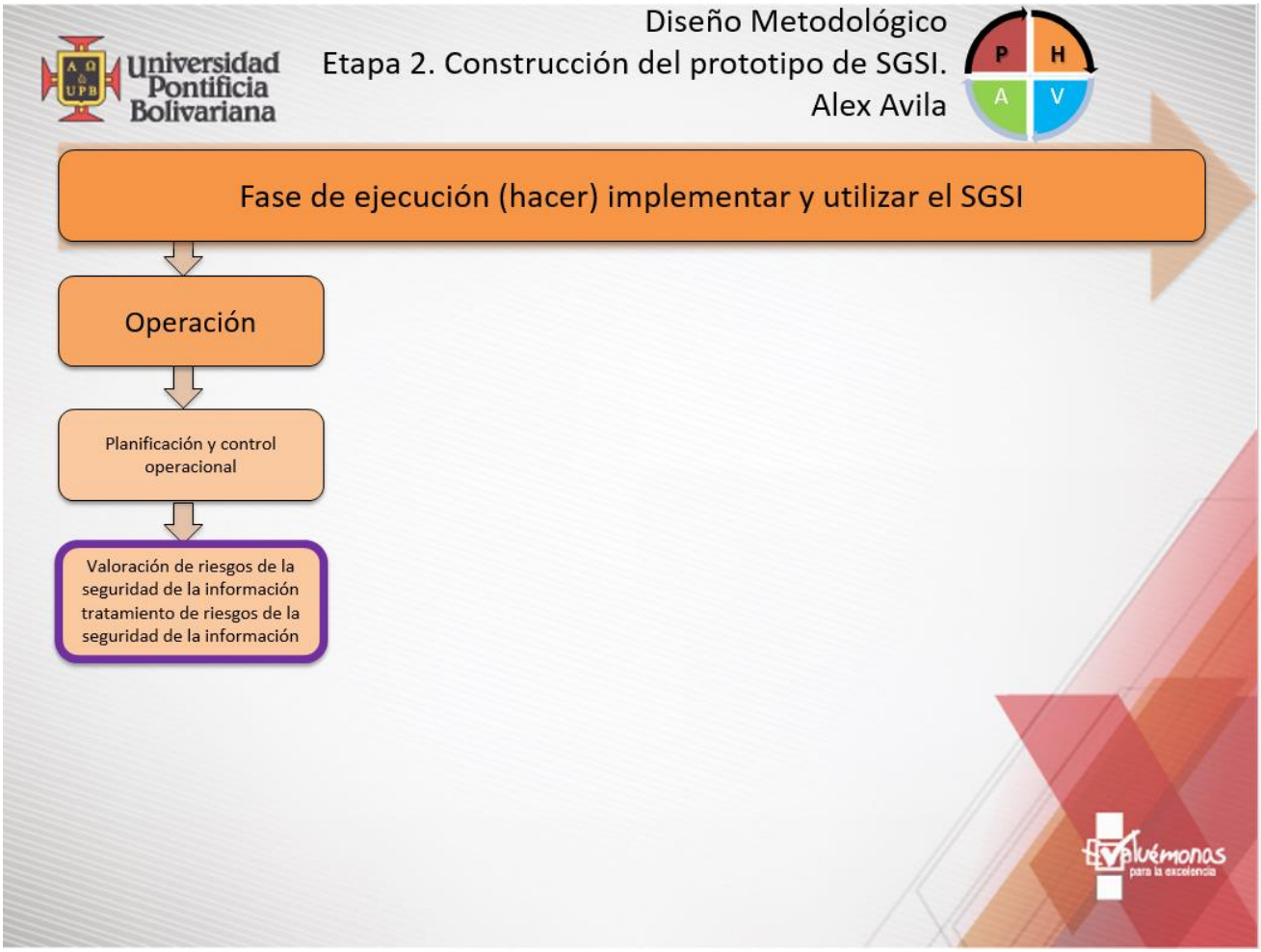


Figura 19 Fase de Hacer, con Etapas y Procesos.

En *la Figura 20 Fase de Verificar, con Etapas y Procesos*, se puede apreciar el camino a desarrollar en toda la Fase de Verificar:

Figura 20 Fase de Verificar, con Etapas y Procesos.

Finalmente en la *Figura 21 Fase de Actuar, con Etapas y Procesos,* se puede apreciar el camino a desarrollar en toda la Fase de Actuar:

Figura 21 Fase de Actuar, con Etapas y Procesos.

Como se pudo observar, hay algunos de los Procesos que aparecen resaltados y otros no, estos que aparecen resaltados, son para los cuales en este prototipo agregó una herramienta para su implementación, cabe decir que se seccionaron los Procesos más significativos del estándar (desde el punto de vista del autor del trabajo de grado) o los que podrían ser más complejos en su implementación, como son por ejemplo la Valoración y Tratamiento del Riesgo o el Conocimiento de la Organización y su Contexto.

Lo anterior no quiere decir que los demás procesos nos son importantes en el estándar, solo que tienen una fácil interpretación y son más sencillos de comprender y desarrollar.

Para mejor compresión, en la *Figura 22 Ejemplo de Procesos Herramientas Prototipo*, se presenta un ejemplo:

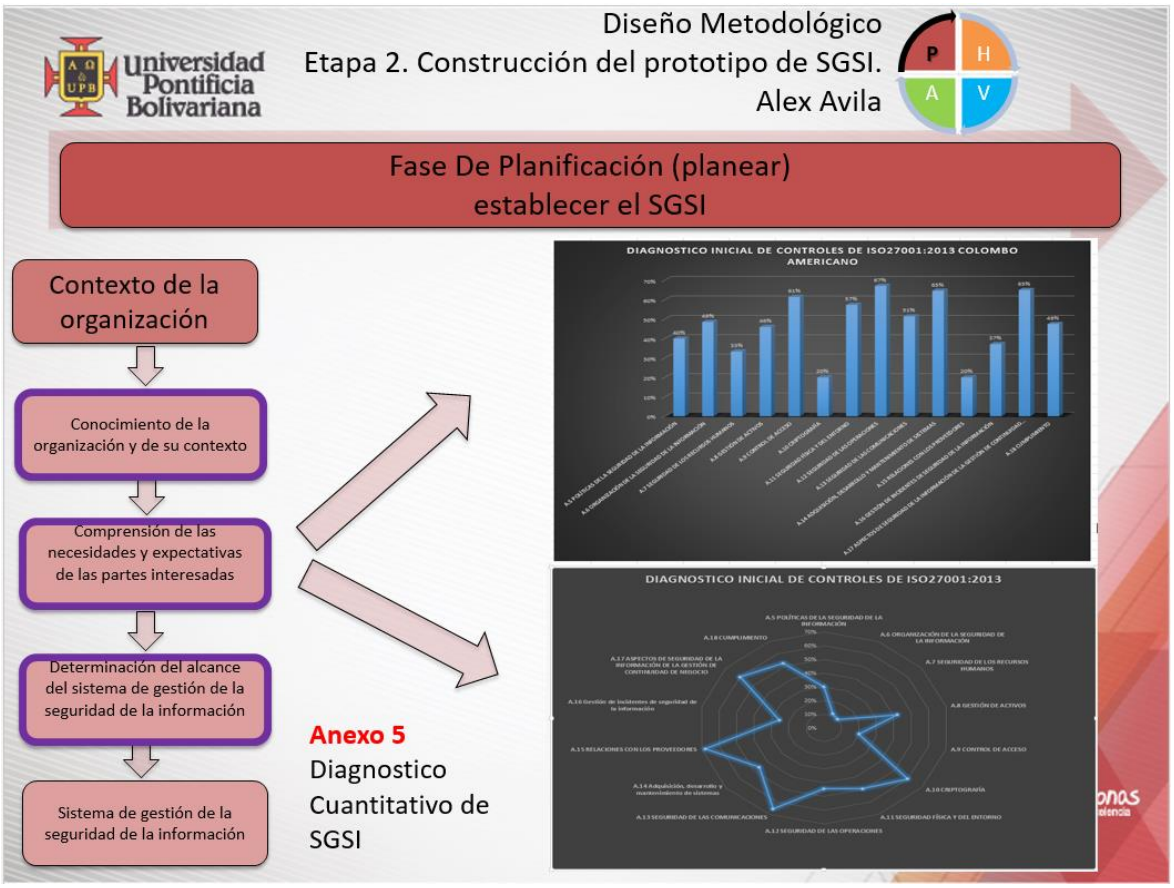


Figura 22 Ejemplo de Procesos Herramientas Prototipo.

En la *Figura 22 Ejemplo de Procesos Herramientas Prototipo* se muestra el esquema de la Fase de Planear con sus Etapas y Procesos, se puede ver como el Proceso de "Comprensión de las necesidades y expectativas de las partes interesadas" esta resaltado y se tiene el Anexo 5 llamado "Diagnostico Cuantitativo SGSI" el cual permite que las personas que utilicen el prototipo pueden hacer un diagnóstico inicial de estado de seguridad de la información al interior de las empresas basados en el estándar propuesto para el trabajo de grado.

4.4.1.3. Detalle de las Fases, Etapas y Procesos.

Para mejor compresión, a continuación se presenta la *Tabla 4 Detalle de las Fases, Etapas y Procesos*, con sus respectivas categorías, donde se podrán revisar cada una las Fases, Etapas y Procesos en detalle:

Fases	Etapas	Procesos
Fase de planificación (Planear): establecer el SGSI	Contexto de la organización	• Conocimiento de la organización y de su contexto. • Comprensión de las necesidades y expectativas de las partes interesadas. • Determinación del alcance del sistema de gestión de la seguridad de la información. • Sistema de gestión de la seguridad de la información.
	Liderazgo	• Liderazgo y compromiso. • Política. • Roles, responsabilidades y autoridades en la organización.
	Planificación	• Acciones para tratar riesgos y oportunidades. • Objetivos de la seguridad de la información y planes para lograrlos.
	Soporte	• Recurso. • Competencia. • Toma de conciencia. • Comunicación. • Información documentada.
Fase de ejecución (Hacer): implementar y utilizar el SGSI	Operación	• Planificación y control operacional. • Valoración de riesgos de la seguridad de la información, tratamiento de riesgos de la seguridad de la información.
Fase de seguimiento (Verificar): monitorear y revisar el SGSI	Evaluación del desempeño	• Seguimiento, medición, análisis y evaluación • Auditoría interna • Revisión por la dirección
Fase de Mejora (Actuar): monitorear y revisar el SGSI	Mejora	• No conformidades y acciones correctivas • Mejora continua

Tabla 4 Detalle de las Fases, Etapas y Procesos.

4.4.1.4. Herramientas Anexas al Prototipo.

A continuación se presentará la *Tabla 5 Detalle de las Fases, Etapas y Procesos*, donde se relacionan todos los recursos que se anexarán a este trabajo de grado, con el fin de contribuir a la visión general de los SGSI en las diferentes instituciones educativas y empresas en general, cada uno de estos formatos debe ser acondicionado según las necesidades propias y los contextos donde sean utilizados:

Núm.	Fase	Etapa	Proceso	Herramienta
1	**Planear**	Contexto de la organización.	Comprensión de las necesidades y expectativas de las partes interesadas.	**Anexo 2 Plan_del_proyecto.docx.**
2	**Planear**	Contexto de la organización.	Determinación del alcance del sistema de gestión de la seguridad de la información.	**Anexo 3 Documento_sobre_el_alcance_del_SGSI.docx.**
3	**Planear**	Contexto de la organización.	Sistema de gestión de la seguridad de la información	**Anexo 4 Diagnóstico Inicial.docx.**
4	**Planear**	Contexto de la organización.	Sistema de gestión de la seguridad de la información	**Anexo 5 Diagnostico Cuantitativo de SGSI.xlsx.**
5	**Planear**	Liderazgo	Política	**Anexo 6 Política_de_seguridad_de_la_información.docx.**
6	**Planear**	Liderazgo	Política	**Anexo 7 Ejemplo de Políticas de Seguridad de la Información.docx.**
7	**Planear**	Liderazgo	Roles, responsabilidades y autoridades en la organización.	**Anexo 8 Roles y Responsabilidades.docx.**
8	**Planear**	Planificación	Acciones para tratar riesgos y oportunidades.	**Anexo 9 Gestión de Riegos de SGSI.xlsx.** **Anexo 17 Software Tratamiento Riesgos (Desarrollo propio para gestionar los riesgos)**
9	**Planear**	Soporte	Toma de conciencia Comunicación	**Anexo 10 Toma De Conciencia y Comunicación.docx.**
10	**Planear**	Soporte	Información documentada	**Anexo 11 Documentación.docx**
11	**Hacer**	Operación	Valoración de riesgos de la seguridad de la información tratamiento de riesgos de la seguridad de la información.	**Anexo 9 Gestión de Riegos de SGSI.xlsx.** **Anexo 17 Software Tratamiento Riesgos (Desarrollo propio para gestionar los riesgos)**
12	**Verificar**	Evaluación del desempeño	Auditoría interna	**Anexo 13 Auditoria.docx.**
13	**Verificar**	Evaluación del desempeño	Revisión por la dirección	**Anexo 14 Revisión Por La Dirección.docx.**

Tabla 5 Relación de Herramientas en el Prototipo.

4.4.1.5. ***Esquema completo del Prototipo.***

Finalmente a continuación se presentará el esquema completo del prototipo en la *Figura 23 Esquema Global del Prototipo*, para permitir tener una visión global del esquema de implementación.

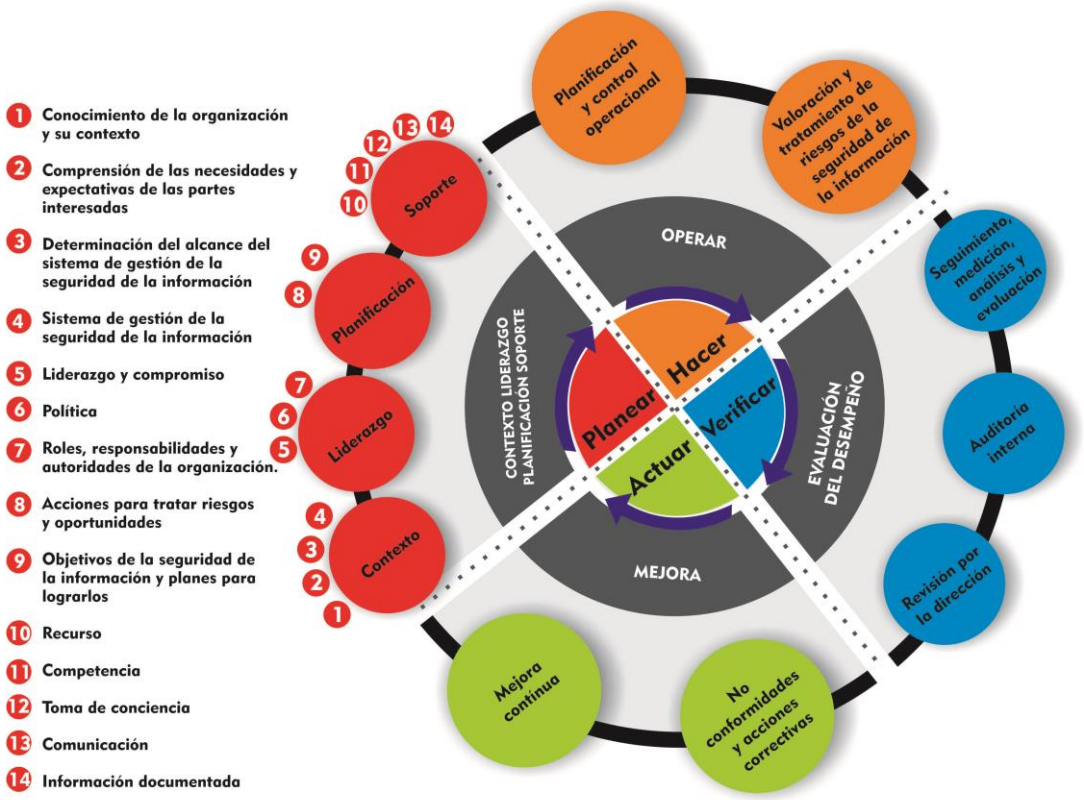


Figura 23 Esquema Global del Prototipo

Las organizaciones deberán definir cuáles de las actividades descritas en este prototipo son aplicables a ellas y cuáles se pueden simplificar o ampliar según los criterios propios de cada organización.

4.4.2. Desarrollo de la propuesta

4.4.2.1. Fase de planificación (Planear) establecer el SGSI

4.4.2.1.1. Contexto de la Organización

Esta etapa tiene como objetivo principal definir los requerimientos para comprender cuestiones externas e internas, también define las partes interesadas, sus requisitos y el alcance del SGSI.

4.4.2.1.1.1. Conocimiento de la organización y de su contexto

Para el desarrollo de este proceso, se debe tener en cuenta la cláusula 4.1 de la Norma Técnica NTC-ISO-IEC COLOMBIANA 27001, la cual dice:
"La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan su capacidad para lograr los resultados previstos de su sistema de gestión de la seguridad de la información."[63]

Nota: "La determinación de estas cuestiones hace referencia al establecimiento del contexto externo e interno de la organización, considerado en el numeral 5.3 de la NTC-ISO 31000:2011."[64]

Se debe tener en cuenta en este proceso:

- Identificar y comprender el contexto de la organización antes de establecer el sistema de gestión de seguridad de la información (SGSI).
- Identificar los problemas internos relevantes para el propósito de la organización y considerar la posible influencia de estos sobre la capacidad de lograr los resultados que el SGSI tiene la intención de lograr.
- Identificar los problemas externos relevantes para el propósito de la organización y considerar la posible influencia de estos sobre la capacidad para lograr los resultados que el SGSI tiene la intención de lograr.
- Determinar la influencia que los interesados externos podrían tener.

4.4.2.1.1.2. Comprensión de las necesidades y expectativas de las partes interesadas

Para el desarrollo de este proceso se debe tener en cuenta la cláusula 4.2 de la Norma Técnica NTC-ISO-IEC COLOMBIANA 27001, la cual dice:

"La organización debe determinar:
a) las partes interesadas que son pertinentes al sistema de gestión de la seguridad de la información; y
b) los requisitos de estas partes interesadas pertinentes a seguridad de la información.
NOTA: Los requisitos de las partes interesadas pueden incluir los requisitos legales y reglamentarios y las obligaciones contractuales." [65]

Se debe tener en cuenta en este proceso:

- Identificar todas las partes que tienen interés en SGSI de la organización.
- Identificar los requisitos, incluyendo las necesidades y expectativas.

Recurso Planeación del proyecto

Como ayuda en este proceso se recomienda tener en cuenta el esquema propuesto por 27001Academy 2, llamado "**Plan_del_proyecto.docx"** [66] el cual está identificado como "**Anexo 2 Plan_del_proyecto.docx" en este proyecto**.

4.4.2.1.1.3. Determinación del alcance del sistema de gestión de la seguridad de la información

Para el desarrollo de este proceso, se debe tener en cuenta la cláusula 4.3 de la Norma Técnica NTC-ISO-IEC COLOMBIANA 27001, la cual dice:

"La organización debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance.

Cuando se determina este alcance, la organización debe considerar:

a) las cuestiones externas e internas referidas en el numeral 4.1, y

b) los requisitos referidos en el numeral 4.2; y
c) las interfaces y dependencias entre las actividades realizadas por la organización y las que realizan otras organizaciones.

El alcance debe estar disponible como información documentada.” [67]

Se podría decir que la planeación para la implementación de un SGSI, es una etapa ineludible, por tanto, definir el alcance para la implementación del sistema en una organización es uno de los primeros aspectos a considerar.

Teniendo en cuenta la existencia de organizaciones que difieren en tamaño por el número de empleados, volumen de información manejada, número de clientes, volúmenes de activos físicos y lógicos, número de sedes u oficinas, entre otros elementos, se hace necesario determinar en qué áreas o dependencias de la organización se desea implantar el SGSI como primera medida y cuáles posteriormente. Las primeras áreas a considerar son aquellas que por sus funciones y responsabilidades ayudan en primera instancia con el cumplimiento de la misión institucional. [68]

Se debe tener en cuenta en este proceso:

- Averiguar cuáles son los límites que se deben considerar en la definición del alcance.
- Usar los límites e información recolectada para dar claridad a la organización sobre el alcance del SGSI.
- Documentar el alcance del SGSI de la organización.
- Controlar el documento del alcance del SGSI de la organización.

Si se desea tener mayor información sobre los elementos para definir el Alcance del SGSI, se puede profundizar en Guía Técnica Colombiana GTC ISO/IEC 27003:2010, [68] de igual forma se recomienda leer las reflexiones que sobre el tema propone Dejan Kosutic en el artículo “Problemas para definir el alcance de la norma ISO27001.” [69]

Recurso Alcance

Como ayuda en este proceso, se recomienda tener en cuenta el esquema propuesto por 27001Academy 2 llamado “**Documento_sobre_el_alcance_del_SGSI**” [66] el cual está

identificado como “**Anexo 3 Documento_sobre_el_alcance_del_SGSI**” en este trabajo de grado.

4.4.2.1.1.4. Sistema de gestión de la seguridad de la información

Para el desarrollo de este proceso se debe tener en cuenta la cláusula 4.4 de la Norma Técnica NTC-ISO-IEC COLOMBIANA 27001, la cual dice:

“La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información, de acuerdo con los requisitos de esta Norma.” [70]

Se debe tener en cuenta en este proceso:

- Establecer un SGSI según la Norma Técnica NTC-ISO-IEC COLOMBIANA 27001.

Recurso SGSI

Como soporte al proceso anterior, se recomienda utilizar el “**Anexo 4 Diagnóstico Inicial.docx**” donde por medio de una herramienta para el Gap Analysis, puede ver el nivel de implementación de la ISO27001:2013 en la organización, revisando si se encuentra en un estado inicial o si por el contrario falta poco para alcanzar el nivel de madurez adecuado. [71]

De igual forma, se recomienda utilizar el “**Anexo 5 Diagnóstico Cuantitativo de SGSI.xlsx**” esta es otra herramienta [72] para el Gap Analysis construida en Microsoft Excel que permitirá a las instituciones educativas y las empresas en general, saber de forma cuantitativa cuál es su nivel, en relación a la adopción de un SGSI. Al final del proceso las empresas podrán saber de forma gráfica cómo están en relación a la utilización de los SGSI. Como ejemplos se presenta la *Figura 24 Resultados Herramienta de Diagnostico 1* y la *Figura 25 Resultados Herramienta de Diagnostico 2:*

Resultado diagnóstico inicial Escolme

DOMINIOS	PORCENTAJE DESARROLLADO
A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN	20%
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	37%
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	20%
A.8 GESTIÓN DE ACTIVOS	34%
A.9 CONTROL DE ACCESO	33%
A.10 CRIPTOGRAFÍA	0%
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO	57%
A.12 SEGURIDAD DE LAS OPERACIONES	70%
A.13 SEGURIDAD DE LAS COMUNICACIONES	37%
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	55%
A.15 RELACIONES CON LOS PROVEEDORES	60%
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	46%
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	50%
A.18 CUMPLIMIENTO	63%
PROMEDIO	42%

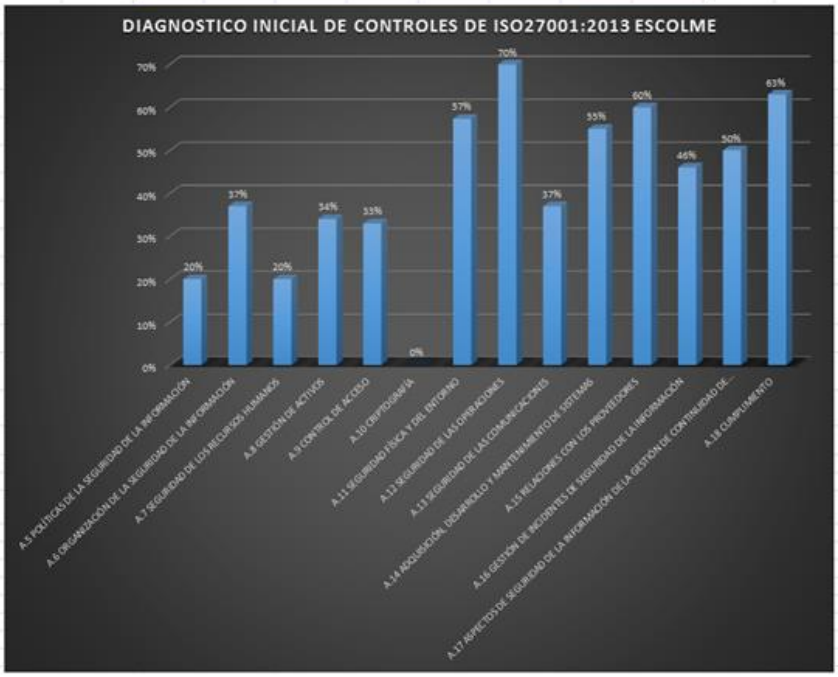


Figura 24 Resultados Herramienta de Diagnostico 1.

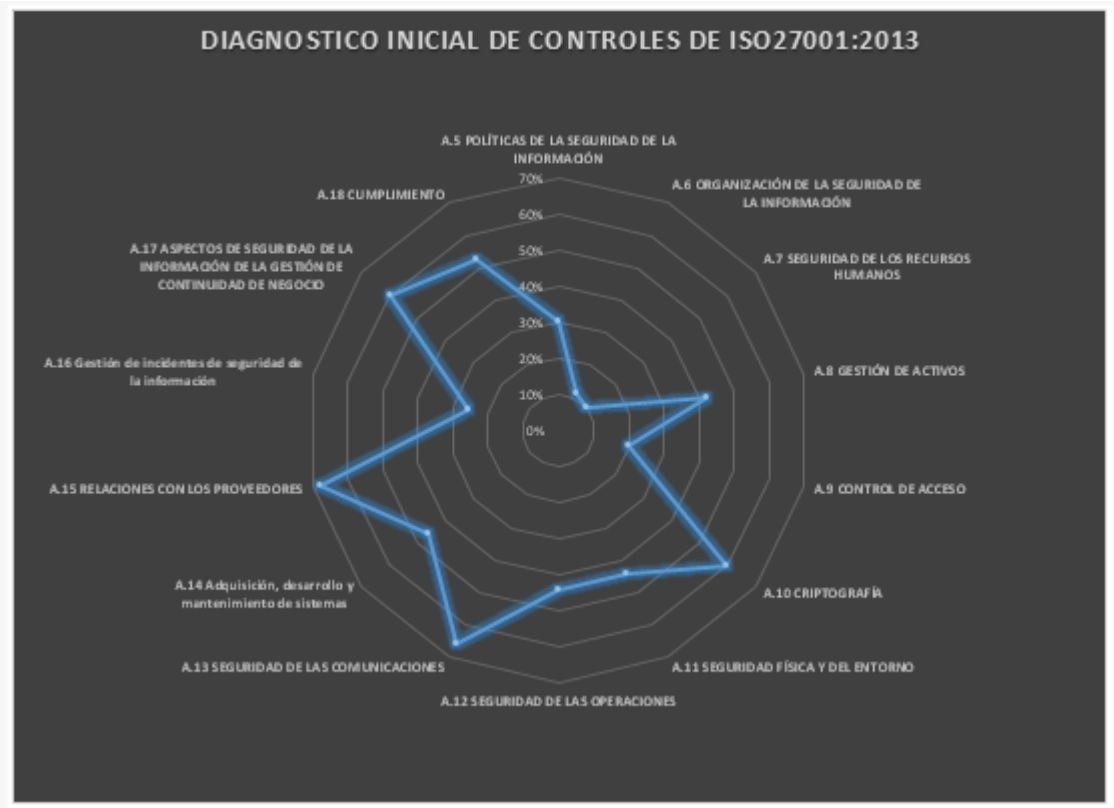


Figura 25 Resultados Herramienta de Diagnostico 2.

4.4.2.1.2. Liderazgo

En esta etapa se definen las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.

4.4.2.1.2.1. Liderazgo y Compromiso

Para el desarrollo de este proceso, se debe tener en cuenta la cláusula 5.1 de la Norma Técnica NTC-ISO-IEC COLOMBIANA 27001, la cual entre otros elementos dice:

“La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información:

“a) asegurando que se establezcan la política de la seguridad de la información y los objetivos de la seguridad de la información y que estos sean compatibles con la dirección estratégica de la organización;
b) asegurando la integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos de la organización;
c) asegurando que los recursos necesarios para el sistema de gestión de la seguridad de la información estén disponibles;
d) comunicando la importancia de una gestión de la seguridad de la información eficaz y de la conformidad con los requisitos del sistema de gestión de la seguridad de la información.
Entre otros” [73]

Se debe tener en cuenta en este proceso:

- Demostrar el compromiso con el SGSI.
- Asegurarse de que se establecen las políticas del SGSI.
- Asegurarse de que se establecen los objetivos del SGSI.
- Asegurarse de que SGSI logra los resultados previstos.
- Asegurarse de que los requisitos del SGSI se convierten en parte integral de los procesos de la organización.
- Asegurarse que los recursos necesarios SGSI están disponibles cuando se necesitan.
- Comunicar el compromiso de su SGSI.
- Realizar compañas de concientización
- Animar a los gerentes a demostrar el liderazgo y compromiso con la seguridad de la información dentro de sus propias áreas.

4.4.2.1.2.2. Política

Este es uno de los elementos más importantes del SGSI. En él se deben establecer las políticas de seguridad y tiene como objetivo principal recoger las directrices que debe seguir la seguridad de la información de acuerdo a las necesidades de la organización y la legislación vigente. Además debe establecer las pautas de actuación en el caso de incidentes y definir las responsabilidades. Debe explicar qué es lo que está permitido y qué no; determinar los límites del comportamiento aceptable y cuál es la respuesta si estos se sobrepasan; e identificar los riesgos a los que está sometida la organización.

Para el desarrollo de este proceso se debe tener en cuenta la cláusula 5.2 de la Norma Técnica NTC-ISO-IEC COLOMBIANA 27001, la cual entre otros elementos dice:

"La alta dirección debe establecer una política de la seguridad de la información que:
a) sea adecuada al propósito de la organización;
b) incluya objetivos de seguridad de la información (véase el numeral 6.2) o proporcione el marco de referencia para el establecimiento de los objetivos de la seguridad de la información;
c) incluya el compromiso de cumplir los requisitos aplicables relacionados con la seguridad de la información; finalmente que
d) incluya el compromiso de mejora continua del sistema de gestión de la seguridad de la información.
La política de la seguridad de la información debe:
e) estar disponible como información documentada;
f) comunicarse dentro de la organización; y
g) estar disponible para las partes interesadas, según sea apropiado."

La Alta Dirección debe establecer una política que:

- Sea adecuada al propósito de la empresa.
- Incluya objetivos de Seguridad de la Información o proporcione el marco para el establecimiento de los mismos.

- Incluya un compromiso de cumplir los requisitos aplicables relacionados con la Seguridad.
- Incluya compromiso de Mejora Continua

Es recomendable leer el documento llamado “Implantación de un SGSI en la empresa” desarrollado por Inteco [74] el cual propone entre otros aspectos para definir políticas de seguridad, los siguientes:

- El documento debe delimitar qué se tiene que proteger, de quién y por qué.
- Debe ser de dominio público dentro de la organización por lo que debe estar disponible para su consulta siempre que sea necesario.
- Debe ser la referencia para la resolución de conflictos y otras cuestiones relativas a la seguridad de la organización.
- Debe definir responsabilidades teniendo en cuenta que estas van asociadas a la autoridad dentro de la compañía.
- En función de las responsabilidades se decidirá quién está autorizado a acceder a qué tipo de información.

De la misma forma el documento recomienda que las políticas deben contener por lo menos los siguientes cinco apartados:

- Definición de la seguridad de la información y sus objetivos globales, el alcance de la seguridad y su importancia como mecanismo de control que permite compartir la información
- Declaración por parte de la Dirección apoyando los objetivos y los principios de la seguridad de la información.
- Breve explicación de las políticas.
- Definición de responsabilidades generales y específicas, en las que se incluirán los roles pero nunca a las personas concretas dentro de la organización.

- Referencias a documentación que pueda sustentar la política.

La política de la seguridad debe ser un documento totalmente actualizado por lo que debe ser revisado y modificado anualmente. Además existen otros tres casos en los que es imprescindible su revisión y actualización:

- Después de grandes incidentes de seguridad.
- Después de una auditoria sin éxito.
- Frente a cambios que afectan la estructura de la organización

Finalmente, en relación a este proceso es recomendable revisar el libro “An Introduccion to ISO/IEC 27001:2013” [75] de David Brewer en el Anexo A del libro mencionado.

Un buen ejemplo de la manera de establecer políticas de seguridad, lo podemos encontrar en el Formato e implementación de políticas de seguridad y privacidad de la información propuesto por el Ministerio de las TIC con el Modelo de Seguridad para las entidades del Estado [76]

Recurso Políticas

Como ayuda en este proceso se recomienda tener en cuenta el esquema propuesto por 27001Academy llamado “**Política_de_seguridad_de_la_información**” [66] el cual está identificado como “**Anexo 6 Política_de_seguridad_de_la_información.docx**” en este trabajo de grado.

En este mismo contexto se recomienda revisar los ejemplos de políticas generales seguridad de la información, desarrollado por SOPHOS [77] llamado “**Ejemplo de Políticas de Seguridad de la Información**” el cual está identificado como “**Anexo 7 Ejemplo de Políticas de Seguridad de la Información.docx**” en este trabajo de grado.

4.4.2.1.2.3. Roles, responsabilidades y autoridades en la organización

Para el desarrollo de este proceso se debe tener en cuenta la cláusula 5.3 de la Norma Técnica NTC-ISO-IEC COLOMBIANA 27001, la cual entre otros elementos dice:

“La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen.

La alta dirección debe asignar la responsabilidad y autoridad para:

a) asegurarse de que el sistema de gestión de la seguridad de la información sea conforme con los requisitos de esta Norma;

b) informar a la alta dirección sobre el desempeño del sistema de gestión de la seguridad de la información.” [78]

Se debe tener en cuenta en este proceso:

- Asignar la responsabilidad y la autoridad para asignar la definición de roles de seguridad en las personas apropiadas dentro de su organización.
- Comunicar toda seguridad de la información relevante, funciones de gestión, responsabilidades y autoridades.

Recurso roles, responsabilidades

Como ayuda en este proceso se recomienda tener en cuenta el archivo llamado “**Anexo 8 Roles y Responsabilidades**” [79] el cual está identificado como “**Anexo 8 Roles y Responsabilidades.docx**” en este trabajo de grado.

4.4.2.1.3. Planificación

En esta etapa se definen los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.

4.4.2.1.3.1. Acciones para tratar riesgos y oportunidades

Para el desarrollo de este proceso se debe tener en cuenta la cláusula 6.1 de la Norma Técnica NTC-ISO-IEC COLOMBIANA 27001, la cual entre otros elementos indica la importancia de determinar los riesgos y oportunidades, con el fin de:

- Lograr que el sistema de gestión de la seguridad de la información pueda alcanzar los resultados previstos.

- Establecer y mantener los criterios de riesgo de la seguridad de la información.
- Incluir los criterios de aceptación de riesgos; y los criterios para realizar valoraciones de riesgos de la seguridad de la información.
- Aplicar el proceso de valoración de riesgos de la seguridad de la información para identificar los riesgos asociados con la pérdida de confidencialidad, de integridad y de disponibilidad de información dentro del alcance del sistema de gestión de la seguridad de la información. [80]

Se debe tener en cuenta:

- Identificar los riesgos y oportunidades que podrían influir en la efectividad del SGSI de la organización o interrumpir su funcionamiento.
- Considerar cómo los asuntos internos y externos podrían afectar la efectividad del SGSI en lograr los resultados previstos.
- Considerar cómo los requerimientos legales y regulatorios podrían afectar la efectividad del SGSI.
- Definir cómo se van a llevar a cabo las evaluaciones de riesgos.
- Definir cómo se van a identificar los propietarios de riesgo.
- Definir cómo se va a garantizar que las evaluaciones de los riesgos producirán resultados consistentes y válidos.
- Dar prioridad a los riesgos de seguridad de información de la organización.
- Documentar el proceso de evaluación de riesgos de seguridad de la información.
- Revisar cada uno de los controles determinados en 6.1.3 b) de la Norma Técnica NTC-ISO-IEC COLOMBIANA 27001 con los del Anexo A, y verificar que no se han omitido controles necesarios para las necesidades de la empresa [81].

Recurso Tratamiento de los Riesgos

Si bien todos los elementos de SGSI son importantes, la evaluación y tratamiento de los riesgos requiere esencial manejo, como ya se mencionó en los capítulos anteriores de este trabajo de grado, la evaluación y el tratamiento de los riesgos son actividades de gran responsabilidad para las personas que administran la seguridad en las empresas, estos procesos requiere conocer en detalle todos los activos de la empresa y entender cuáles de estos son vitales y requiere un tratamiento especial. Este conjunto de evaluaciones y propuestas para tratar los riesgos se pueden desarrollar con las herramientas propuestas en este trabajo de grado.

En este escenario, para este proceso se presentan dos herramientas que pueden ser de gran utilidad para la evaluación y tratamiento de los riesgos. La primera de ellas es una herramienta desarrollada en Microsoft Excel, la cual permite realizar todo el proceso de evaluación y tratamiento de los riesgos. Puede ser consultada en el archivo llamado "**Anexo 9 Gestión de Riegos de SGSI**" el cual está identificado **como Anexo 9 Gestión de Riegos de SGSI.xlsx"** en este trabajo de grado.

La segunda es un programa desarrollado en Java (Spring Framework 4), HTML5 y jQuery 1.8, que tiene la misma finalidad. Puede ser consultado en el carpeta llamada "**Anexo 17 Software Tratamiento Riesgos**" en este trabajo de grado.

Ambas herramientas serán explicadas en detalle más adelante en la Fase de ejecución, en los procesos de Valoración de riesgos de la seguridad de la información y Tratamiento de riesgos de la seguridad de la información.

4.4.2.1.3.2. Objetivos de seguridad de la información y planes para lograrlos

Se deben establecer objetivos en funciones y niveles pertinentes, los objetivos deben según cláusula 6.2 de la Norma Técnica NTC-ISO-IEC COLOMBIANA 27001:

“a) ser coherentes con la política de seguridad de la información;
b) ser medibles (si es posible);
c) tener en cuenta los requisitos de la seguridad de la información aplicables y los resultados de la valoración y del tratamiento de los riesgos;
d) ser comunicados; y
e) ser actualizados, según sea apropiado.
La organización debe conservar información documentada sobre los objetivos de la seguridad de la información.
Cuando se hace la planificación para lograr los objetivos de la seguridad de la información, la organización debe determinar:
f) lo que se va a hacer;
g) qué recursos serán requeridos;
h) quién será responsable;
i) cuándo se finalizará; y
j) cómo se evaluarán los resultados.” [82]

Es importante:

- Establecer objetivos de seguridad de información de su organización.
- Establecer planes para lograr los objetivos de seguridad de la información.
- Especificar qué se debe hacer para alcanzar sus objetivos.
- Especificar quién será responsable de la consecución de objetivos.

4.4.2.1.4. Soporte

Esta sección es parte de la fase de Planificación del ciclo PHVA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.

4.4.2.1.4.1. Recursos

Se debe determinar y proporcionar los recursos para establecer, implementar, mantener y mejorar el SGSI.

4.4.2.1.4.2. Competencia

Se deben especificar las competencias de las personas que están relacionadas con la implementación del SGSI. Entre otros elementos, se debe tener en cuenta según el 7.2 de la Norma Técnica NTC-ISO-IEC COLOMBIANA 27001:

"a) determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo el cual afecta su desempeño en cuanto a la seguridad de la información y
b) asegurarse de que estas personas sean competentes, basándose en la educación, formación o experiencia adecuadas;
c) cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas y
d) conservar la información documentada apropiada, como evidencia de la competencia."[83]

En esta etapa es necesario:

- Adquirir las competencias requeridas cada vez que el personal actual no cumpla con los requisitos de competencia de seguridad de información de su organización.
- Evaluar la eficacia de las medidas adoptadas para adquirir las competencias de seguridad de la información que la organización necesita tener.

4.4.2.1.4.3. Toma de Conciencia

Según el numeral 7.3 de la Norma Técnica NTC-ISO-IEC COLOMBIANA 27001, las personas deben tomar conciencia de:

"a) la política de la seguridad de la información;
b) su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluyendo los beneficios de una mejora del desempeño de la seguridad de la información; y

c) las implicaciones de la no conformidad con los requisitos del sistema de gestión de la seguridad de la información.” [84]

Para el desarrollo adecuado de esta etapa es necesario:

- Asegurarse de que las personas quienes trabajan para la organización entienden conscientemente las políticas de seguridad de la información.
- Asegurarse de que las personas quienes trabajan para la organización entienden cómo pueden apoyar y ayudar a mejorar la eficacia del SGSI.

4.4.2.1.4.4. Comunicación

Se debe determinar la necesidad de comunicaciones externas e internas que incluyan según la cláusula 7.4 de la Norma Técnica NTC-ISO-IEC COLOMBIANA 27001, entre otros elementos:
“a) el contenido de la comunicación;
b) cuándo comunicar;
c) a quién comunicar;
d) quién debe comunicar; y
e) los procesos para llevar a cabo la comunicación.” [85]

Recurso Toma De Conciencia y Comunicación

Para la toma de conciencia y la comunicación del SGSI, se propone un plan completo de comunicaciones, con toda la estrategia para concientizar al público interno de la empresa sobre la importancia de la seguridad de la información. Como apoyo en este proceso, se recomienda tener en cuenta el documento llamado **“Toma De Conciencia y Comunicación”**, el cual está identificado como “**Anexo 10 Toma De Conciencia y Comunicación.docx**” en este trabajo de grado.

Entre las actividades que propone la estrategia se encuentran:

- Capacitaciones a los empleados
- Estrategia comunicacional por intranet o redes internas

- Estrategia comunicacional impresa
- Estrategia comunicacional didáctica

Algunos de los elementos gráficos creados para esta estrategia se pueden evidenciar en la *Figura 26 Logotipo del SGSI*, *Figura 27 Mensaje Creativo SGSI y Figura 28 Afirmación y Apoyo al SGSI*, los cuales son presentados a continuación:

Figura 26 Logotipo del SGSI.

Figura 27 Mensaje Creativo SGSI.

Figura 28 Afirmación y Apoyo al SGSI.

De igual forma, por medio de imágenes que pueden ser difundidas por diferentes medios como correos electrónicos, piezas impresas y el Inside de la empresa, se propone concientizar a las personas de la trascendencia de la implementación del SGSI en la empresa y la participación de todos en este proceso de gran importancia. A continuación

se presentan algunas de estas piezas en la *Figura 29 Pieza Publicitaria SGSI 1, Figura 30 Pieza Publicitaria SGSI 2 y Figura 31 Pieza Publicitaria SGSI 3.*

Figura 29 Pieza Publicitaria SGSI 1.

Figura 30 Pieza Publicitaria SGSI 2.

Figura 31 Pieza Publicitaria SGSI 3

4.4.2.1.4.5. Información documentada

Se debe agregar la información documentada requerida por la norma y la información documentada que la organización ha determinado, es necesaria para la eficiencia del SGSI.

Es preciso definir en esta etapa la creación y las actualizaciones y de igual forma el control de la información documentada.

Para la creación y las actualizaciones es importante:

- Averiguar qué tan extensa debe ser la documentación SGSI.
- Identificar todos los documentos y registros que necesita el SGSI.

Del mismo modo al momento de establecer el control de la información documentada es necesario:

- Asegurarse que los documentos y registros del SGSI, estén correctamente identificados y descritos.

- Asegurarse de que los documentos y registros del SGSI, estén correctamente formateados y presentados.
- Asegurarse de que los documentos y registros del SGSI estén debidamente revisados y aprobados.

De manera específica, ISO27001:2013 indica que un SGSI debe estar formado por los siguientes documentos:

- Alcance del SGSI
- Objetivos y política de seguridad de la información
- Metodología de evaluación y tratamiento de riesgos
- Declaración de aplicabilidad
- Plan de tratamiento de riesgos
- Informe de evaluación de riesgos
- Definición de roles y responsabilidades de seguridad
- Inventario de activos
- Uso aceptable de los activos
- Política de control de acceso
- Procedimientos operativos para gestión de TI
- Principios de ingeniería para sistema seguro
- Política de seguridad para proveedores
- Procedimiento para la gestión de incidentes
- Procedimientos para continuidad del negocio
- Requisitos legales, normativos y contractuales

Recurso Documentación

Como ayuda en este proceso se recomienda tener en cuenta el documento llamado "Documentación" el cual está identificado como "**Anexo 11 Documentación**" en este trabajo de grado y se puede encontrar con el nombre del archivo "**Anexo 11 Documentacion.docx**", en su contenido se plantean recomendaciones para la documentación del SGSI.

4.4.2.2. Fase de ejecución (Hacer) implementar y utilizar el SGSI

4.4.2.2.1. Operación

Esta sección es parte de la fase de Planificación del ciclo PHVA y precisa la implementación de la valoración y el tratamiento de riesgos, de igual forma los controles y otros procesos necesarios para cumplir los objetivos de seguridad de la información.

4.4.2.2.1.1. Planificación y control operacional

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información y para implementar las acciones determinadas en el numeral 6.1. Se deben implementar planes para lograr los objetivos del SGSI.
Se debe mantener información documentada cuando sea necesaria, para tener confianza en que los procesos se han llevado a cabo según lo planificado
Se deben controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, mitigando los efectos adversos, cuando se requiera. [86]

Para lograrlo es necesario tener en cuenta que:

- Se debe planificar el desarrollo de los procesos en los SGSI.
- Se deben desarrollar los procesos del SGSI de la organización.
- Se deben establecer los controles internos y externos en los procesos del SGSI.
- Se deben mantener los procesos del SGSI de la organización.

4.4.2.2.1.2. Valoración de riesgos de la seguridad de la información

Se deben llevar a cabo evaluaciones de riesgos a intervalos planificados o cuando se propongan u ocurran cambios significativos, según los criterios establecidos en 6.1.2.a.

Se debe conservar información documentada de los resultados de las evaluaciones del riesgo.
Esto significa que para lograr una valoración adecuada de los riesgos se debe:

- Realizar evaluaciones periódicas de riesgos de seguridad de la información.

- Dar prioridad a los riesgos cada vez que se realizan dichas evaluaciones.
- Mantener un registro de los resultados de evaluación de riesgos.

4.4.2.2.1.3. Tratamiento de riesgos de la seguridad de la información

Se debe implementar el plan de tratamiento de los riesgos y conservar información documentada de los resultados obtenidos en dicho proceso.

Recurso Valoración de riesgos y Tratamiento de riesgos

Herramienta Gestión de Riegos de SGSI

Como ya se mencionó en la Fase anterior de planificación, este recurso es una serie de procesos desarrollados en Excel (**Anexo 9 Gestión de Riegos de SGSI.xlsx**.) que le permitirán hacer la evaluación y definición del tratamiento de los riesgos. A continuación en la *Figura 32 Esquema para la Gestión de Riesgos*, se hará una descripción de los pasos para el manejo de la metodología planteada:

Figura 32 Esquema para la Gestión de Riesgos.

Hoja Definir los Activos: se trata de establecer cuáles son los activos que se quieren evaluar. Es necesario recordar que un activo es todo aquello con valor para una

organización y que necesita protección, en el ámbito informático pueden ser datos, infraestructura, hardware, software, etc.

Dentro del esquema planteado se presentan siete categorías de activos principales; Humanas, Hardware, Infraestructura, Software, Datos, Servicios, Aplicativos. En el proceso de adaptación, las instituciones educativas o las empresas deben definir sus propias categorías. A continuación en la *Figura 33 Definición de Activos*, se presentará los activos propuestos en esta herramienta:

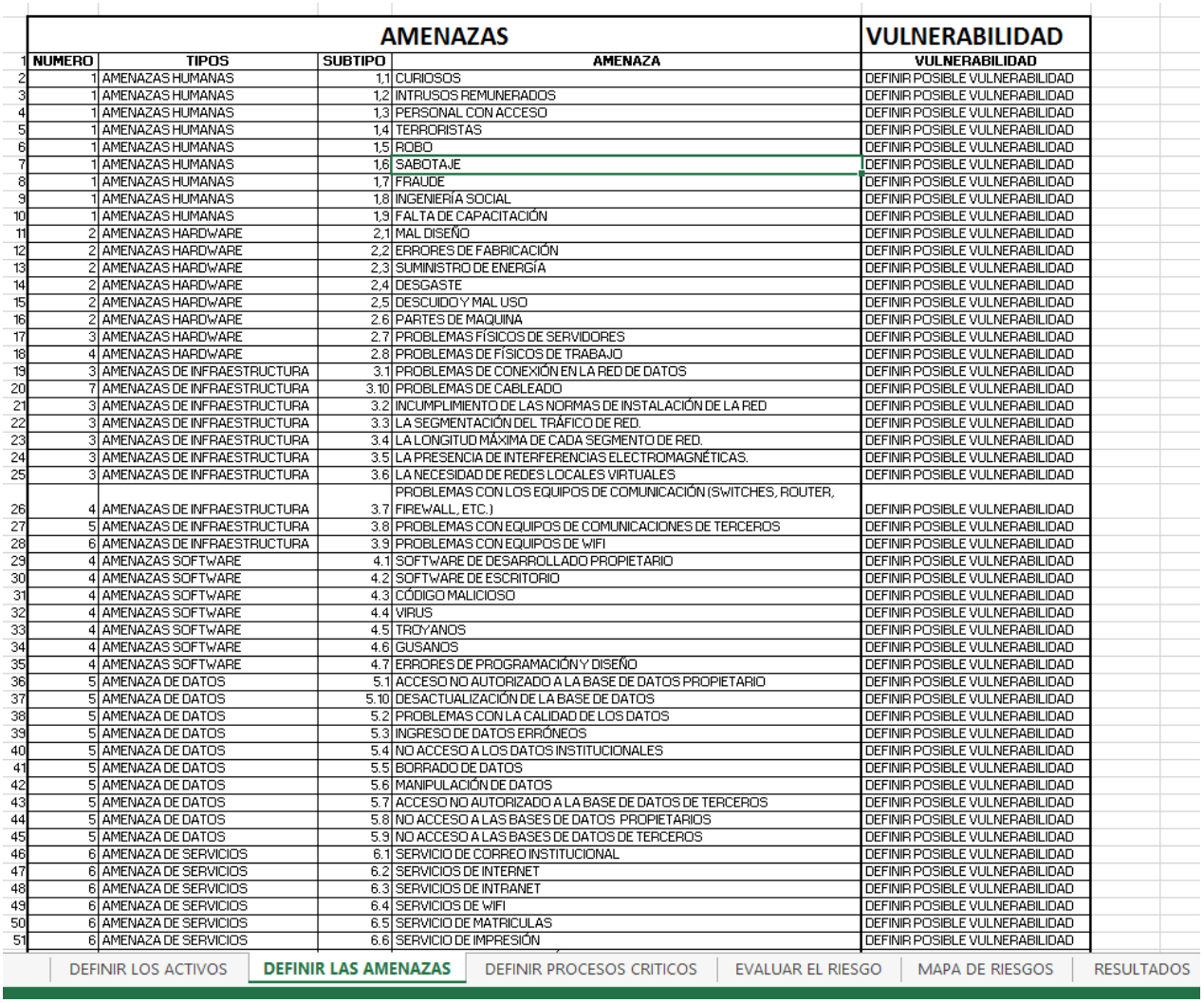
TIPOS DE ACTIVOS	
DEFINICIÓN	Es todo aquello con valor para una organización y que necesita protección, en el ámbito informático pueden ser datos, infraestructura, hardware, software, personal, información, servicios, etc.
NUMERO	*TIPOS*
1	HUMANAS
2	HARDWARE
3	INFRAESTRUCTURA
4	SOFTWARE
5	DATOS
6	SERVICIOS
7	APLICATIVOS

DEFINIR LOS ACTIVOS | DEFINIR LAS AMENAZAS | DEFINIR PROCESOS CRITICOS

Figura 33 Definición de Activos.

Hoja Definir Las Amenazas

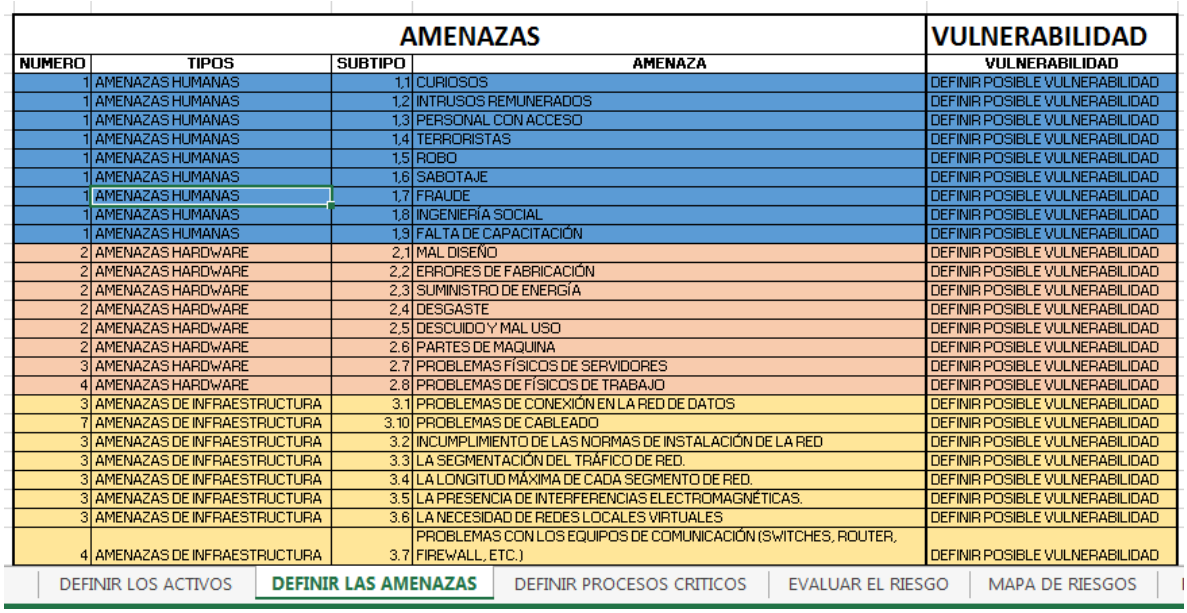
En esta hoja se presentan una serie de amenazas para cada uno de los activos planeados en la hoja anterior, de igual forma el usuario podrá ingresar las vulnerabilidades asociadas a cada una de las posibles amenazas de su contexto. A continuación en la *Figura 34 Activos Propuestos con Posibles Amenazas*, se presentan los activos propuestos y algunas de las amenazas más comunes que se podrían presentar en las empresas de diferentes sectores:



	AMENAZAS				VULNERABILIDAD
1	NUMERO	TIPOS	SUBTIPO	AMENAZA	VULNERABILIDAD
2	1	AMENAZAS HUMANAS	1,1	CURIOSOS	DEFINIR POSIBLE VULNERABILIDAD
3	1	AMENAZAS HUMANAS	1,2	INTRUSOS REMUNERADOS	DEFINIR POSIBLE VULNERABILIDAD
4	1	AMENAZAS HUMANAS	1,3	PERSONAL CON ACCESO	DEFINIR POSIBLE VULNERABILIDAD
5	1	AMENAZAS HUMANAS	1,4	TERRORISTAS	DEFINIR POSIBLE VULNERABILIDAD
6	1	AMENAZAS HUMANAS	1,5	ROBO	DEFINIR POSIBLE VULNERABILIDAD
7	1	AMENAZAS HUMANAS	1,6	SABOTAJE	DEFINIR POSIBLE VULNERABILIDAD
8	1	AMENAZAS HUMANAS	1,7	FRAUDE	DEFINIR POSIBLE VULNERABILIDAD
9	1	AMENAZAS HUMANAS	1,8	INGENIERÍA SOCIAL	DEFINIR POSIBLE VULNERABILIDAD
10	1	AMENAZAS HUMANAS	1,9	FALTA DE CAPACITACIÓN	DEFINIR POSIBLE VULNERABILIDAD
11	2	AMENAZAS HARDWARE	2,1	MAL DISEÑO	DEFINIR POSIBLE VULNERABILIDAD
12	2	AMENAZAS HARDWARE	2,2	ERRORES DE FABRICACIÓN	DEFINIR POSIBLE VULNERABILIDAD
13	2	AMENAZAS HARDWARE	2,3	SUMINISTRO DE ENERGÍA	DEFINIR POSIBLE VULNERABILIDAD
14	2	AMENAZAS HARDWARE	2,4	DESGASTE	DEFINIR POSIBLE VULNERABILIDAD
15	2	AMENAZAS HARDWARE	2,5	DESCUIDO Y MAL USO	DEFINIR POSIBLE VULNERABILIDAD
16	2	AMENAZAS HARDWARE	2.6	PARTES DE MAQUINA	DEFINIR POSIBLE VULNERABILIDAD
17	3	AMENAZAS HARDWARE	2.7	PROBLEMAS FÍSICOS DE SERVIDORES	DEFINIR POSIBLE VULNERABILIDAD
18	4	AMENAZAS HARDWARE	2.8	PROBLEMAS DE FÍSICOS DE TRABAJO	DEFINIR POSIBLE VULNERABILIDAD
19	3	AMENAZAS DE INFRAESTRUCTURA	3.1	PROBLEMAS DE CONEXIÓN EN LA RED DE DATOS	DEFINIR POSIBLE VULNERABILIDAD
20	7	AMENAZAS DE INFRAESTRUCTURA	3.10	PROBLEMAS DE CABLEADO	DEFINIR POSIBLE VULNERABILIDAD
21	3	AMENAZAS DE INFRAESTRUCTURA	3.2	INCUMPLIMIENTO DE LAS NORMAS DE INSTALACIÓN DE LA RED	DEFINIR POSIBLE VULNERABILIDAD
22	3	AMENAZAS DE INFRAESTRUCTURA	3.3	LA SEGMENTACIÓN DEL TRÁFICO DE RED.	DEFINIR POSIBLE VULNERABILIDAD
23	3	AMENAZAS DE INFRAESTRUCTURA	3.4	LA LONGITUD MÁXIMA DE CADA SEGMENTO DE RED.	DEFINIR POSIBLE VULNERABILIDAD
24	3	AMENAZAS DE INFRAESTRUCTURA	3.5	LA PRESENCIA DE INTERFERENCIAS ELECTROMAGNÉTICAS.	DEFINIR POSIBLE VULNERABILIDAD
25	3	AMENAZAS DE INFRAESTRUCTURA	3.6	LA NECESIDAD DE REDES LOCALES VIRTUALES	DEFINIR POSIBLE VULNERABILIDAD
26	4	AMENAZAS DE INFRAESTRUCTURA	3.7	PROBLEMAS CON LOS EQUIPOS DE COMUNICACIÓN (SWITCHES, ROUTER, FIREWALL, ETC.)	DEFINIR POSIBLE VULNERABILIDAD
27	5	AMENAZAS DE INFRAESTRUCTURA	3.8	PROBLEMAS CON EQUIPOS DE COMUNICACIONES DE TERCEROS	DEFINIR POSIBLE VULNERABILIDAD
28	6	AMENAZAS DE INFRAESTRUCTURA	3.9	PROBLEMAS CON EQUIPOS DE WIFI	DEFINIR POSIBLE VULNERABILIDAD
29	4	AMENAZAS SOFTWARE	4.1	SOFTWARE DE DESARROLLADO PROPIETARIO	DEFINIR POSIBLE VULNERABILIDAD
30	4	AMENAZAS SOFTWARE	4.2	SOFTWARE DE ESCRITORIO	DEFINIR POSIBLE VULNERABILIDAD
31	4	AMENAZAS SOFTWARE	4.3	CÓDIGO MALICIOSO	DEFINIR POSIBLE VULNERABILIDAD
32	4	AMENAZAS SOFTWARE	4.4	VIRUS	DEFINIR POSIBLE VULNERABILIDAD
33	4	AMENAZAS SOFTWARE	4.5	TROYANOS	DEFINIR POSIBLE VULNERABILIDAD
34	4	AMENAZAS SOFTWARE	4.6	GUSANOS	DEFINIR POSIBLE VULNERABILIDAD
35	4	AMENAZAS SOFTWARE	4.7	ERRORES DE PROGRAMACIÓN Y DISEÑO	DEFINIR POSIBLE VULNERABILIDAD
36	5	AMENAZA DE DATOS	5.1	ACCESO NO AUTORIZADO A LA BASE DE DATOS PROPIETARIO	DEFINIR POSIBLE VULNERABILIDAD
37	5	AMENAZA DE DATOS	5.10	DESACTUALIZACIÓN DE LA BASE DE DATOS	DEFINIR POSIBLE VULNERABILIDAD
38	5	AMENAZA DE DATOS	5.2	PROBLEMAS CON LA CALIDAD DE LOS DATOS	DEFINIR POSIBLE VULNERABILIDAD
39	5	AMENAZA DE DATOS	5.3	INGRESO DE DATOS ERRÓNEOS	DEFINIR POSIBLE VULNERABILIDAD
40	5	AMENAZA DE DATOS	5.4	NO ACCESO A LOS DATOS INSTITUCIONALES	DEFINIR POSIBLE VULNERABILIDAD
41	5	AMENAZA DE DATOS	5.5	BORRADO DE DATOS	DEFINIR POSIBLE VULNERABILIDAD
42	5	AMENAZA DE DATOS	5.6	MANIPULACIÓN DE DATOS	DEFINIR POSIBLE VULNERABILIDAD
43	5	AMENAZA DE DATOS	5.7	ACCESO NO AUTORIZADO A LA BASE DE DATOS DE TERCEROS	DEFINIR POSIBLE VULNERABILIDAD
44	5	AMENAZA DE DATOS	5.8	NO ACCESO A LAS BASES DE DATOS PROPIETARIOS	DEFINIR POSIBLE VULNERABILIDAD
45	5	AMENAZA DE DATOS	5.9	NO ACCESO A LAS BASES DE DATOS DE TERCEROS	DEFINIR POSIBLE VULNERABILIDAD
46	6	AMENAZA DE SERVICIOS	6.1	SERVICIO DE CORREO INSTITUCIONAL	DEFINIR POSIBLE VULNERABILIDAD
47	6	AMENAZA DE SERVICIOS	6.2	SERVICIOS DE INTERNET	DEFINIR POSIBLE VULNERABILIDAD
48	6	AMENAZA DE SERVICIOS	6.3	SERVICIOS DE INTRANET	DEFINIR POSIBLE VULNERABILIDAD
49	6	AMENAZA DE SERVICIOS	6.4	SERVICIOS DE WIFI	DEFINIR POSIBLE VULNERABILIDAD
50	6	AMENAZA DE SERVICIOS	6.5	SERVICIO DE MATRICULAS	DEFINIR POSIBLE VULNERABILIDAD
51	6	AMENAZA DE SERVICIOS	6.6	SERVICIO DE IMPRESIÓN	DEFINIR POSIBLE VULNERABILIDAD

Figura 34 Activos Propuestos con Posibles Amenazas.

A continuación en la *Figura 35 Definición de Amenazas*, se muestra su presentación en la herramienta propuesta:



AMENAZAS				VULNERABILIDAD
NUMERO	TIPOS	SUBTIPO	AMENAZA	VULNERABILIDAD
1	AMENAZAS HUMANAS	1,1	CURIOSOS	DEFINIR POSIBLE VULNERABILIDAD
1	AMENAZAS HUMANAS	1,2	INTRUSOS REMUNERADOS	DEFINIR POSIBLE VULNERABILIDAD
1	AMENAZAS HUMANAS	1,3	PERSONAL CON ACCESO	DEFINIR POSIBLE VULNERABILIDAD
1	AMENAZAS HUMANAS	1,4	TERRORISTAS	DEFINIR POSIBLE VULNERABILIDAD
1	AMENAZAS HUMANAS	1,5	ROBO	DEFINIR POSIBLE VULNERABILIDAD
1	AMENAZAS HUMANAS	1,6	SABOTAJE	DEFINIR POSIBLE VULNERABILIDAD
1	AMENAZAS HUMANAS	1,7	FRAUDE	DEFINIR POSIBLE VULNERABILIDAD
1	AMENAZAS HUMANAS	1,8	INGENIERÍA SOCIAL	DEFINIR POSIBLE VULNERABILIDAD
1	AMENAZAS HUMANAS	1,9	FALTA DE CAPACITACIÓN	DEFINIR POSIBLE VULNERABILIDAD
2	AMENAZAS HARDWARE	2,1	MAL DISEÑO	DEFINIR POSIBLE VULNERABILIDAD
2	AMENAZAS HARDWARE	2,2	ERRORES DE FABRICACIÓN	DEFINIR POSIBLE VULNERABILIDAD
2	AMENAZAS HARDWARE	2,3	SUMINISTRO DE ENERGÍA	DEFINIR POSIBLE VULNERABILIDAD
2	AMENAZAS HARDWARE	2,4	DESGASTE	DEFINIR POSIBLE VULNERABILIDAD
2	AMENAZAS HARDWARE	2,5	DESCUIDO Y MAL USO	DEFINIR POSIBLE VULNERABILIDAD
2	AMENAZAS HARDWARE	2.6	PARTES DE MAQUINA	DEFINIR POSIBLE VULNERABILIDAD
3	AMENAZAS HARDWARE	2.7	PROBLEMAS FÍSICOS DE SERVIDORES	DEFINIR POSIBLE VULNERABILIDAD
4	AMENAZAS HARDWARE	2.8	PROBLEMAS DE FÍSICOS DE TRABAJO	DEFINIR POSIBLE VULNERABILIDAD
3	AMENAZAS DE INFRAESTRUCTURA	3.1	PROBLEMAS DE CONEXIÓN EN LA RED DE DATOS	DEFINIR POSIBLE VULNERABILIDAD
7	AMENAZAS DE INFRAESTRUCTURA	3.10	PROBLEMAS DE CABLEADO	DEFINIR POSIBLE VULNERABILIDAD
3	AMENAZAS DE INFRAESTRUCTURA	3.2	INCUMPLIMIENTO DE LAS NORMAS DE INSTALACIÓN DE LA RED	DEFINIR POSIBLE VULNERABILIDAD
3	AMENAZAS DE INFRAESTRUCTURA	3.3	LA SEGMENTACIÓN DEL TRÁFICO DE RED.	DEFINIR POSIBLE VULNERABILIDAD
3	AMENAZAS DE INFRAESTRUCTURA	3.4	LA LONGITUD MÁXIMA DE CADA SEGMENTO DE RED.	DEFINIR POSIBLE VULNERABILIDAD
3	AMENAZAS DE INFRAESTRUCTURA	3.5	LA PRESENCIA DE INTERFERENCIAS ELECTROMAGNÉTICAS.	DEFINIR POSIBLE VULNERABILIDAD
3	AMENAZAS DE INFRAESTRUCTURA	3.6	LA NECESIDAD DE REDES LOCALES VIRTUALES	DEFINIR POSIBLE VULNERABILIDAD
4	AMENAZAS DE INFRAESTRUCTURA	3.7	PROBLEMAS CON LOS EQUIPOS DE COMUNICACIÓN (SWITCHES, ROUTER, FIREWALL, ETC.)	DEFINIR POSIBLE VULNERABILIDAD

DEFINIR LOS ACTIVOS | DEFINIR LAS AMENAZAS | DEFINIR PROCESOS CRITICOS | EVALUAR EL RIESGO | MAPA DE RIESGOS

Figura 35 Definición de Amenazas.

Hoja definir procesos Críticos

En esta hoja se deben seleccionar los activos y las amenazas que sean considerados críticos para la empresa, estos son los que serán evaluados. Es importante anotar que cuando se selecciona un activo solo aparecerán las amenazas relacionas con este activo, tanto los activos como las amenazas, fueron definidos en las hojas anteriores.

De igual forma, se aclara que esta herramienta está diseñada para trabajar con 15 posibles amenazas, aunque puede ser personalizada según los contextos donde sea utilizada.

A continuación en la *Figura 36 Definición de los Procesos Críticos*, se muestra su presentación en la herramienta propuesta:

Figura 36 Definición de los Procesos Críticos.

Hoja Evaluar El Riesgo

Después de seleccionar los 15 o menos procesos críticos que se desean evaluar, la hoja Evaluar El Riesgo carga esos datos y presenta dos columnas de evaluación, una donde se evaluará el impacto que puede tener la amenaza y otra donde se evaluará la probabilidad de presentarse la misma.

Posterior a la evaluación, se calculará de forma automática cada una de las amenazas y se dará una evaluación de Alto, Medio o Bajo según el resultado obtenido. Los cálculos se realizarán según la siguiente matriz de evaluación. En la *Tabla 6 Matriz De Evaluación* de *Amenazas*, se puede revisar los posibles resultados de la matriz.

ESCALA DE RESULTADOS			
MATRIZ DE RESULTADOS			
PROBABILIDAD	**IMPACTO**	**COLOR RESULTADO**	**NIVIEL DE CRITICIDAD**
1	1	VERDE	BAJO
1	2	VERDE	BAJO
1	3	VERDE	BAJO
1	4	AMARILLO	MEDIO
1	5	AMARILLO	MEDIO
2	1	VERDE	BAJO
2	2	VERDE	BAJO
2	3	AMARILLO	MEDIO
2	4	AMARILLO	MEDIO
2	5	ROJO	ALTO
3	1	VERDE	BAJO
3	2	AMARILLO	MEDIO
3	3	AMARILLO	MEDIO
3	4	AMARILLO	MEDIO
3	5	ROJO	ALTO
4	1	VERDE	BAJO
4	2	AMARILLO	MEDIO
4	3	AMARILLO	MEDIO
4	4	ROJO	ALTO
4	5	ROJO	ALTO
5	1	AMARILLO	MEDIO
5	2	AMARILLO	MEDIO
5	3	ROJO	ALTO
5	4	ROJO	ALTO
5	5	ROJO	ALTO

Tabla 6 Matriz De Evaluación de Amenazas.

A continuación en la *Figura 37 Evaluación de Riesgos*, se muestra su presentación en la herramienta propuesta:

#	ACTIVOS	ACTIVOS	POSIBLE VULNERABILIDAD(DEFINIR POSIBLES VULNERABILIDADES	CALIFICACION		RESULTADO	EVALUACION RIESGO
				PROBABILIDAD	IMPACTO		
1	INFRAESTRUCTURA	PROBLEMAS DE CONEXIÓN EN LA RED DE DATOS	DEFINIR POSIBLE VULNERABILIDAD	2,0	2,0	2,0	BAJO
2	DATOS	BORRADO DE DATOS	DEFINIR POSIBLE VULNERABILIDAD	2,0	3,0	2,5	MEDIO
3	HARDWARE	DESCUIDO Y MAL USO	DEFINIR POSIBLE VULNERABILIDAD	3,0	3,0	3,0	MEDIO
4	APLICATIVOS	APLICATIVOS DE CORREO	DEFINIR POSIBLE VULNERABILIDAD	4,0	5,0	4,5	ALTO
5	SERVICIOS	SERVICIO DE AUTENTICACIÓN	DEFINIR POSIBLE VULNERABILIDAD	3,0	5,0	4,0	ALTO
6	INFRAESTRUCTURA	PROBLEMAS CON LOS EQUIPOS DE COMUNICACIÓN (SWITCHES, ROUTER, FIREWALL, ETC.)	DEFINIR POSIBLE VULNERABILIDAD	2,0	4,0	3,0	MEDIO
7	HUMANAS	ROBO	DEFINIR POSIBLE VULNERABILIDAD	3,0	5,0	4,0	ALTO
8	HARDWARE	DESGASTE	DEFINIR POSIBLE VULNERABILIDAD	1,0	2,0	1,5	BAJO
9	INFRAESTRUCTURA	PROBLEMAS CON LOS EQUIPOS DE COMUNICACIÓN (SWITCHES, ROUTER, FIREWALL, ETC.)	DEFINIR POSIBLE VULNERABILIDAD	1,0	4,0	2,5	MEDIO
10	SOFTWARE	SOFTWARE DE ESCRITORIO	DEFINIR POSIBLE VULNERABILIDAD	1,0	5,0	3,0	MEDIO
11	DATOS	NO ACCESO A LOS DATOS INSTITUCIONALES	DEFINIR POSIBLE VULNERABILIDAD	2,0	3,0	2,5	MEDIO
12	SERVICIOS	SERVICIO DE MATRICULAS	DEFINIR POSIBLE VULNERABILIDAD	1,0	3,0	2,0	BAJO
13	HUMANAS	FALTA DE CAPACITACIÓN	DEFINIR POSIBLE VULNERABILIDAD	2,0	5,0	3,5	ALTO
14	HARDWARE	SUMINISTRO DE ENERGÍA	DEFINIR POSIBLE VULNERABILIDAD	5,0	1,0	3,0	MEDIO
15	HUMANAS	SABOTAJE	DEFINIR POSIBLE VULNERABILIDAD	1,0	1,0	1,0	BAJO

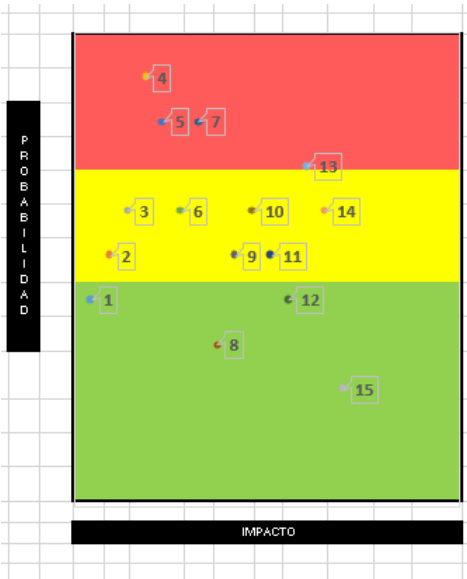
DEFINIR LOS ACTIVOS | DEFINIR LAS AMENAZAS | DEFINIR PROCESOS CRITICOS | EVALUAR EL RIESGO | MAPA DE RIESGOS | RESULTAD ...

Figura 37 Evaluación de Riesgos.

Hoja Mapa De Riesgos

Esta hoja es informativa, en ella se presenta el resultado de la evaluación de los riesgos y una matriz de calor donde se muestra la ubicación de cada una de las amenazas evaluadas.

A continuación en la *Figura 38 Mapa de Riesgos,* se muestra su presentación en la herramienta propuesta:



ESTA INFORMACION LA TRAE EL SISTEMA NO EDITAR				
	#	Riesgo Mapeado	Vulnerabilidad	Criticidad
1	INFRAESTRUCTURA	PROBLEMAS DE CONEXIÓN EN LA RED DE DATOS	DEFINIR POSIBLE VULNERABILIDAD	BAJO
2	DATOS	BORRADO DE DATOS	DEFINIR POSIBLE VULNERABILIDAD	MEDIO
3	HARDWARE	DESCUIDO Y MAL USO	DEFINIR POSIBLE VULNERABILIDAD	MEDIO
4	APLICATIVOS	APLICATIVOS DE CORREO	DEFINIR POSIBLE VULNERABILIDAD	ALTO
5	SERVICIOS	SERVICIO DE AUTENTICACIÓN	DEFINIR POSIBLE VULNERABILIDAD	ALTO
6	INFRAESTRUCTURA	PROBLEMAS CON LOS EQUIPOS DE COMUNICACIÓN (SWITCHES, ROUTER, FIREWALL, ETC.)	DEFINIR POSIBLE VULNERABILIDAD	MEDIO
7	HUMANAS	ROBO	DEFINIR POSIBLE VULNERABILIDAD	ALTO
8	HARDWARE	DESGASTE	DEFINIR POSIBLE VULNERABILIDAD	BAJO
9	INFRAESTRUCTURA	PROBLEMAS CON LOS EQUIPOS DE COMUNICACIÓN (SWITCHES, ROUTER, FIREWALL, ETC.)	DEFINIR POSIBLE VULNERABILIDAD	MEDIO
10	SOFTWARE	SOFTWARE DE ESCRITORIO	DEFINIR POSIBLE VULNERABILIDAD	MEDIO
11	DATOS	NO ACCESO A LOS DATOS INSTITUCIONALES	DEFINIR POSIBLE VULNERABILIDAD	MEDIO
12	SERVICIOS	SERVICIO DE MATRICULAS	DEFINIR POSIBLE VULNERABILIDAD	BAJO
13	HUMANAS	FALTA DE CAPACITACIÓN	DEFINIR POSIBLE VULNERABILIDAD	ALTO
14	HARDWARE	SUMINISTRO DE ENERGÍA	DEFINIR POSIBLE VULNERABILIDAD	MEDIO
15	HUMANAS	SABOTAJE	DEFINIR POSIBLE VULNERABILIDAD	BAJO

Figura 38 Mapa de Riesgos.

Hoja Resultados

En esta hoja se presentan todos los procesos críticos que fueron evaluados y su nivel de criticidad como resultado de la evaluación, de igual forma presenta una serie de campos que deben ser diligenciados al interior de cada organización según sus propios contextos.

Estos campos son:

Control

Este campo se refiere a las normas, los procedimientos, los conocimientos y las estructuras organizacionales concebidas para ofrecer una garantía moderada de que los objetivos de negocio se lograrán y los sucesos no programados se impedirán o detectarán y corregirán.

Por ejemplo, si el tipo de activo fuese una Amenaza de Tipo Humano y la amenaza fuese un Intruso Remunerado, los posibles controles podrían ser:

- Aumentar la seguridad de los sistemas durante su funcionamiento, por ejemplo se podría utilizar un firewall, un IDS o un IPS para evitar los intrusos.
- Utilizar herramientas que permitan la detección de violaciones de seguridad en los sistemas.
- Tener redundancias y políticas de continuidad del negocio.
- Utilizar datos cifrados en los datos confidenciales de la empresa.
- Utilizar políticas de acceso a todos los archivos y aplicativos de la empresa.
- Revisar las políticas sobre el uso de las contraseñas.

Entre muchos otros.

Plan de implantación

Se refiere a la forma como se realizarán los cambios para logra controlar la amenaza evaluada.

Impacto operativo

Se refiere a todos los cambios a nivel de hardware que se deben realizar para controlar la amenaza evaluada.

Impacto funcional

Se refiere a todos los cambios a nivel del personal que se deben realizar para controlar la amenaza evaluada, esto puede incluir capacitaciones, personal con competencias determinas, nuevas contrataciones de personal o inclusive cambios de roles al interior de las empresas.

Dominios y Controles De ISO27001:20013 que le aplican y aspectos legales

Hace referencia a todos los Dominios y Controles de la norma ISO27001:2013 que pueden ser aplicados a la amenaza evaluada y todos los aspectos legales que podrían estar ligados a ella.

Enlaces y recursos relacionados

Hace referencia a todos los enlaces y recursos que pueden servir de ayuda para mitigar la amenaza evaluada.

A continuación en la *Figura 39 Resultados*, se muestra su presentación en la herramienta propuesta:

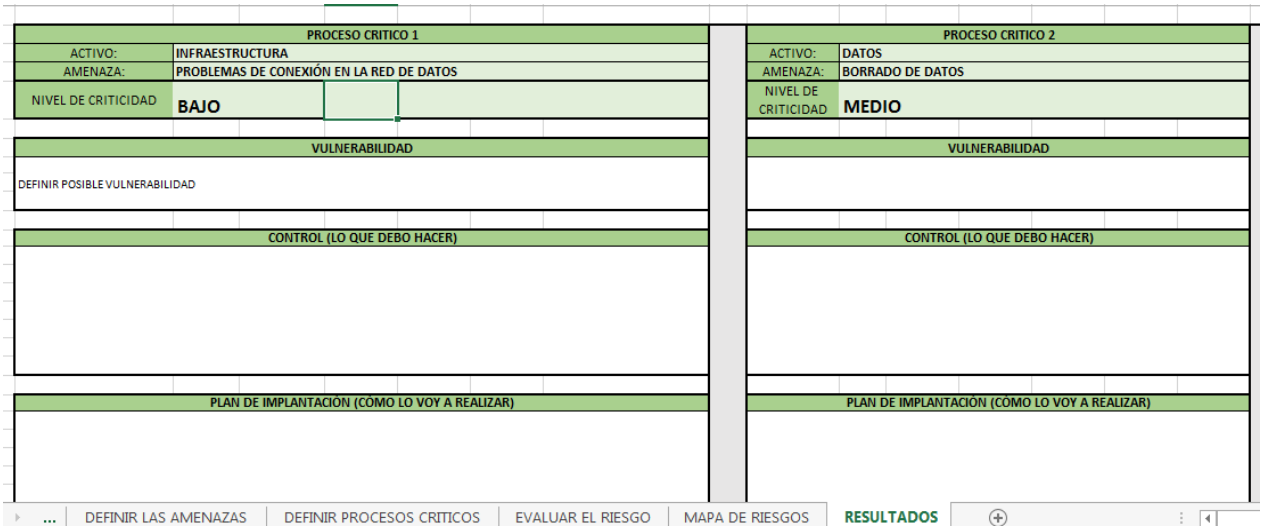


Figura 39 Resultados.

Software Gestión de Riegos de SGSI

El segundo recurso que se propone en este trabajo de grado para el tratamiento de los riesgos en la implementación de un SGSI, es un programa (**Anexo 17 Software Tratamiento Riesgos (Desarrollo propio para gestionar los riesgos)** desarrollado para tal fin, este programa se propone con la intención de que las instituciones educativas y las empresas en general puedan utilizarlo para hacer un diagnóstico de sus riesgos y la posible solución a los mismos.

El programa planteado sigue la misma metodología del recurso anterior, su diferencia radica en que este programa, de forma automática generará los resultados y descargará un informe con las sugerencias a las amenazas seleccionadas, es decir, el usuario no ingresa los campos de Control, Plan de implantación, Impacto operativo, Impacto funcional, Dominios y Controles De ISO27001:2013 que le aplican, tampoco los aspectos legales, Enlaces y recursos relacionados.

A continuación se explica de forma general la manera cómo funciona el programa

Aspectos Técnicos del programa: a continuación se describen los aspectos técnicos relacionados con el programa desarrollado:

Lenguaje de programación: Java (Spring Framework 4), HTML5, jQuery 1.8

JDK Java: JRE 1.7

Patrón de diseño: MVC

Servidor de aplicaciones: Apache Tomcat 7

Motor de Base de Datos: MYSQL 5

Descripción del programa

En la primera ventana del aplicativo, se presentan los activos y las amenazas relacionadas con este activo, es decir, si seleccionamos el activo Hardware solo aparecen las amenazas relacionadas al Hardware, como por ejemplo; Errores de Fabricación o Problemas Físicos de los servidores.

A continuación en la *Figura 40 Seleccionar Activo Software Propuesto,* y la *Figura 41 Seleccionar Activo Software Propuesto,* se puede apreciar cómo se vería en el software propuesto:

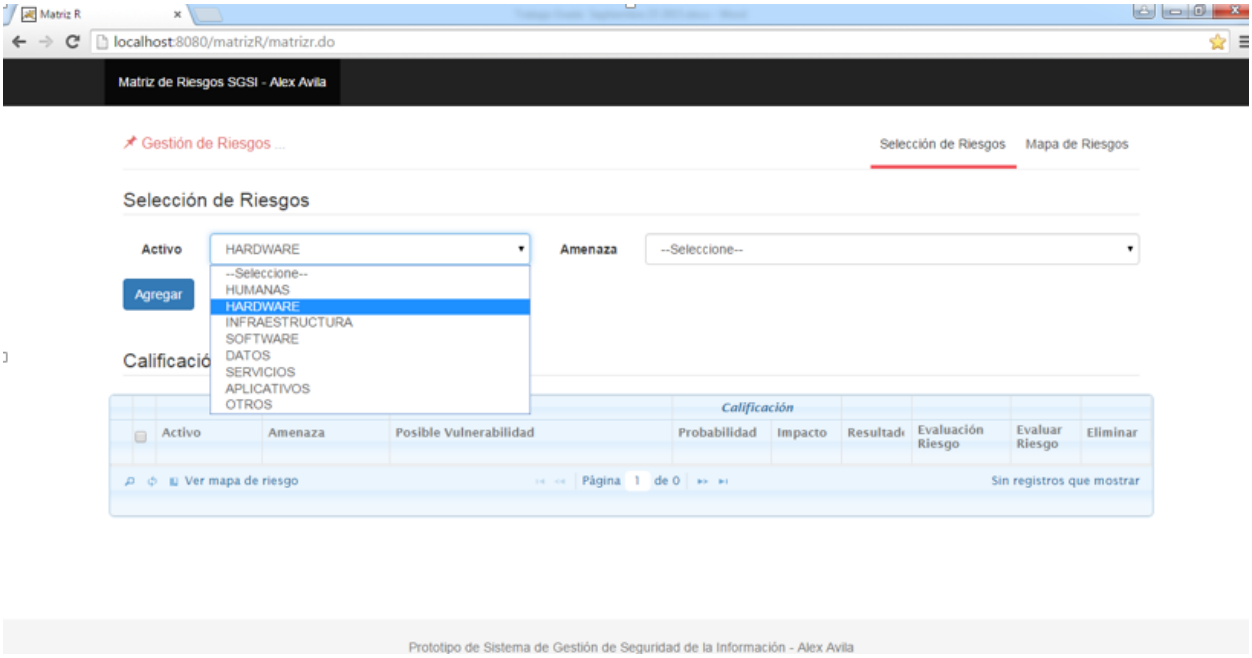


Figura 40 Seleccionar Activo en Software Propuesto.

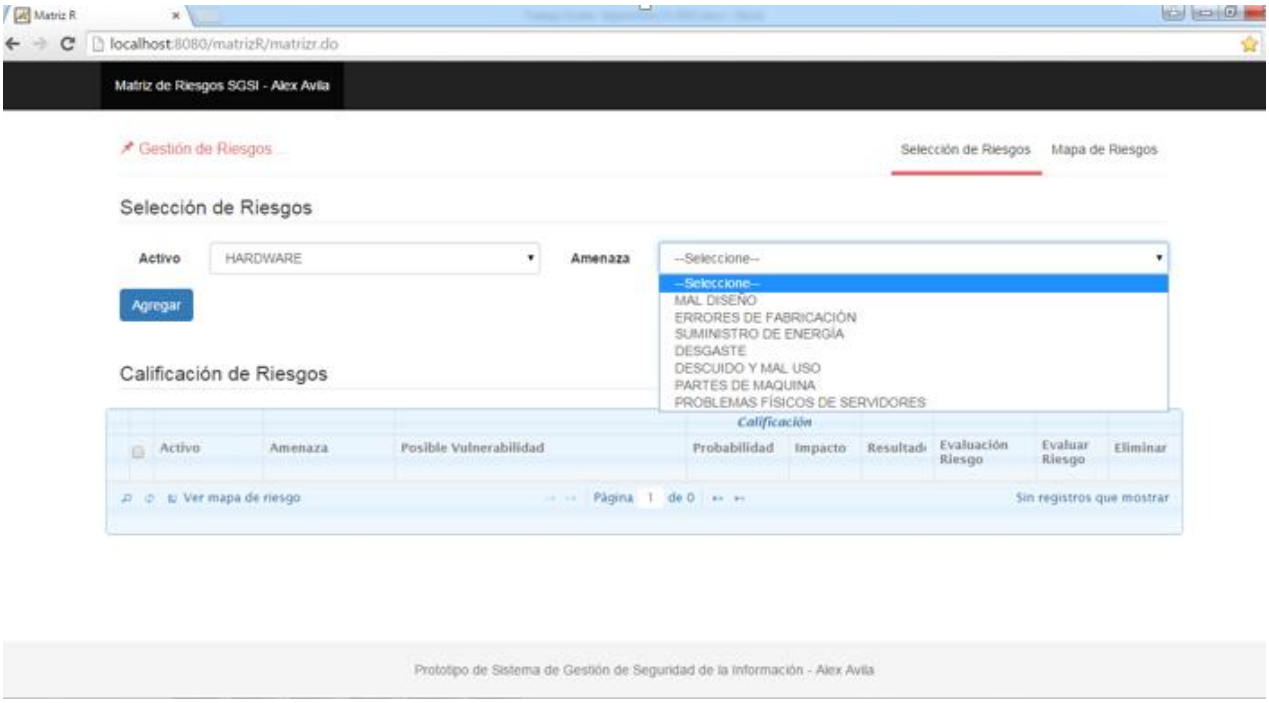


Figura 41 Seleccionar la Amenaza Software Propuesto.

Después de seleccionados los activos y las amenazas, se debe presionar el botón “Agregar” para poder elegir otras que se deseen evaluar, esta herramienta no tiene límites de amenazas a evaluar como ocurre en el recurso anterior, el cual está diseñado inicialmente para la evaluación de 15 amenazas. En consecuencia, el usuario puede seleccionar todos los activos y amenazas que considere necesarios en su contexto.

A continuación en la *Figura 42 Presentación Varias Amenazas Software Propuesto,* se muestra cómo se presenta el software después de seleccionar varios activos y amenazas:

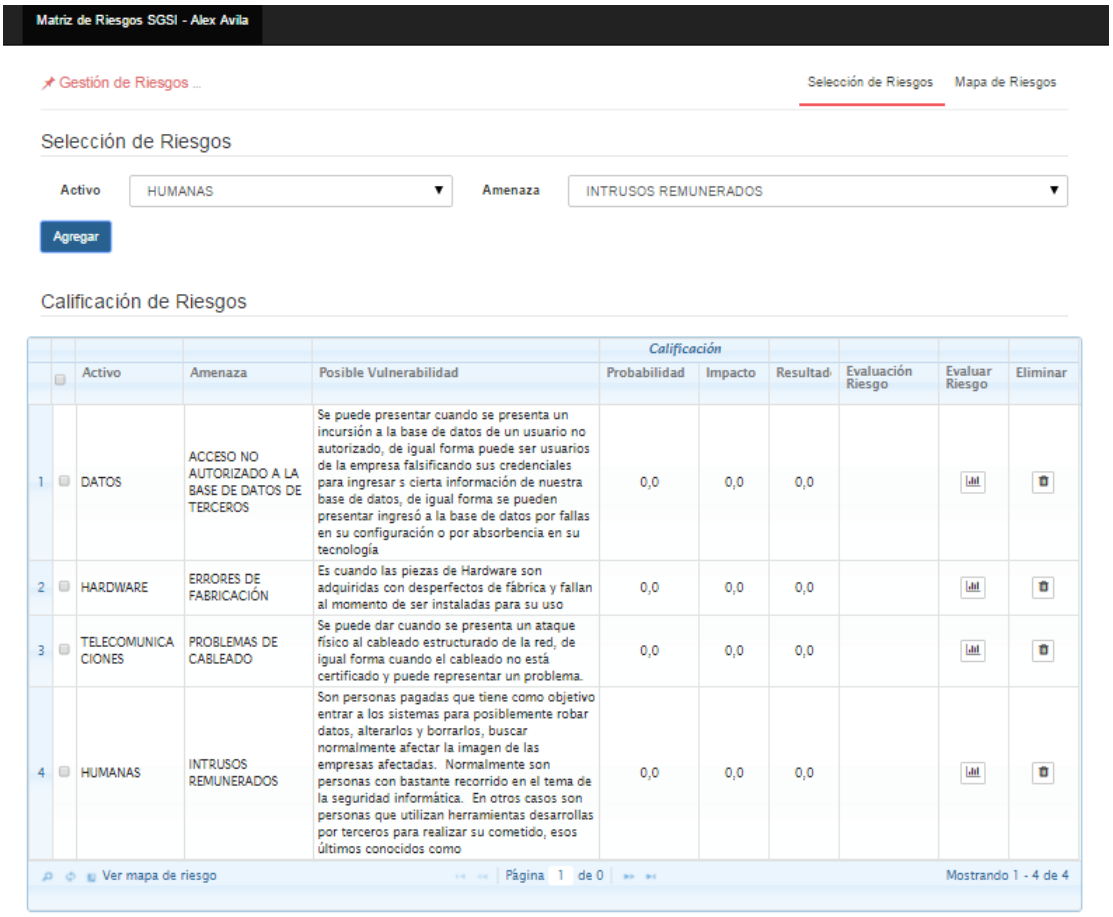


Figura 42 Presentación Varias Amenazas Software Propuesto.

A continuación, se procede a evaluar los riesgos de cada amenaza utilizando el botón Evaluar Riesgo, esto lo podemos evidenciar en la *Figura 43 Evaluación de Amenazas Software Propuesto:*

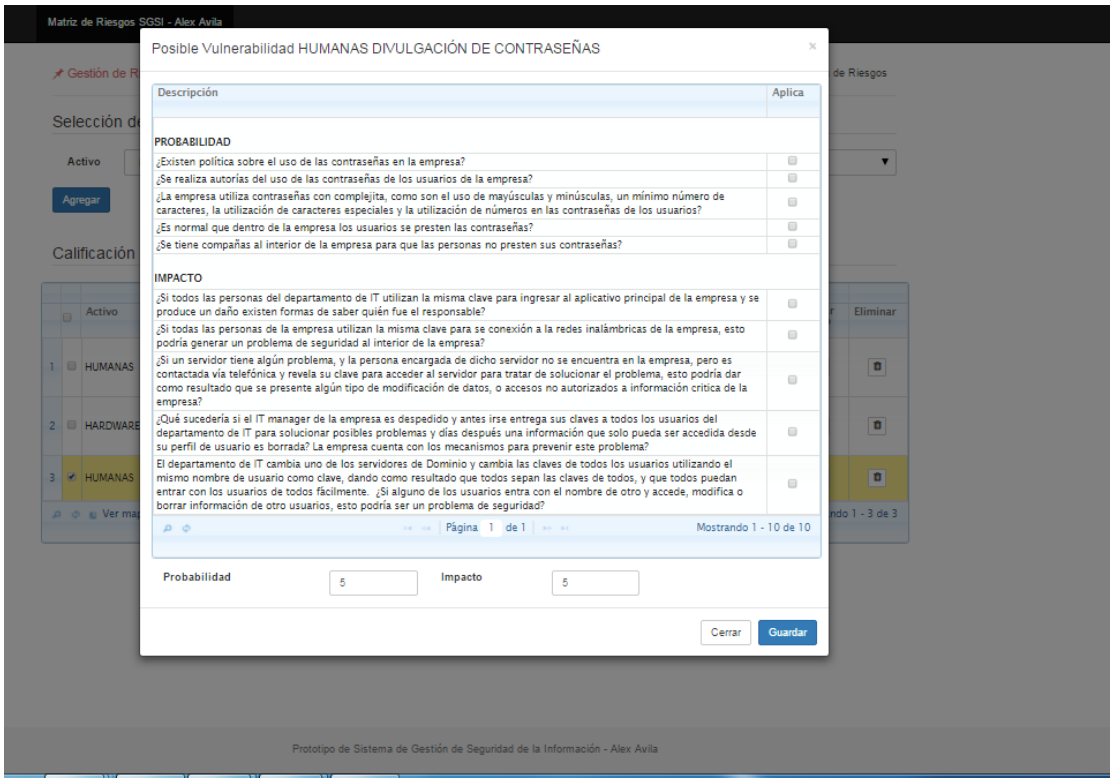
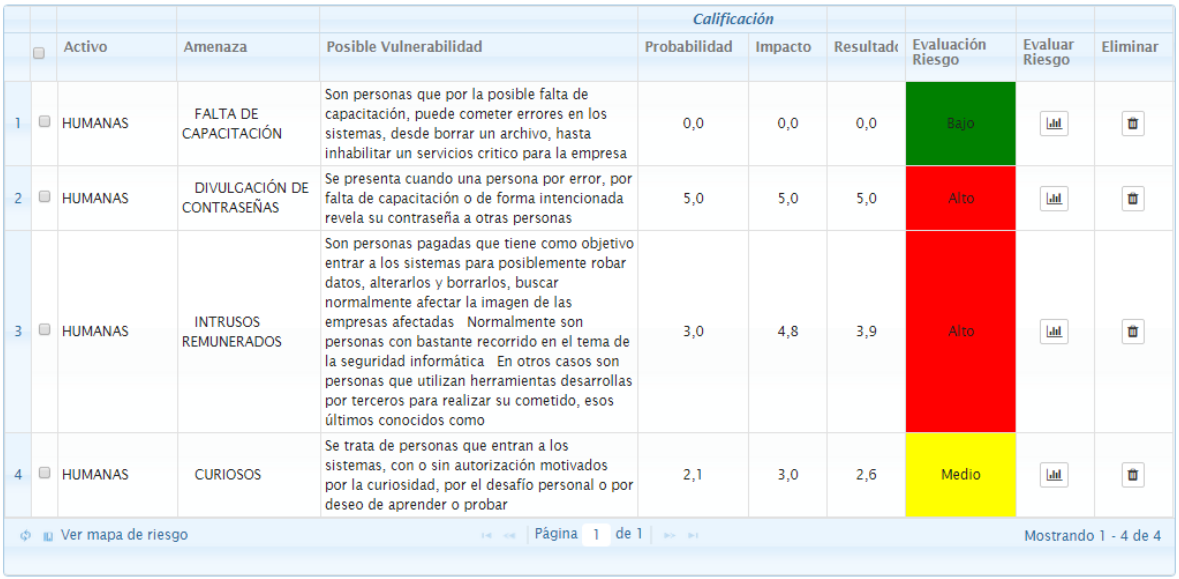


Figura 43 Evaluación de Amenazas Software Propuesto.

En la *Figura 43 Evaluación de Amenazas Software Propuesto*, pudimos ver como aparecen una serie de preguntas las cuales ayudarán a la persona que está utilizando el programa a que su respuesta sea más acertada; inicialmente se le realizan 5 preguntas relacionadas con el impacto que podría tener la amenaza evaluada, posteriormente, se repite el proceso preguntando por la probabilidad que tiene esta amenaza en el contexto evaluado. Con las respuestas a las preguntas se calcula de forma automática el 90% de la respuesta el otro 10% es ingresado por teclado por parte del evaluador.

Esta forma de evaluación busca que las respuestas sean mucho más claras para el evaluador y mucho más acertadas para el sistema.

Después de evaluar los riesgos, el sistema nos presenta los resultados como se puede apreciar en la *Figura 44 Resumen de Evaluación de las Amenazas Software Propuesto:*



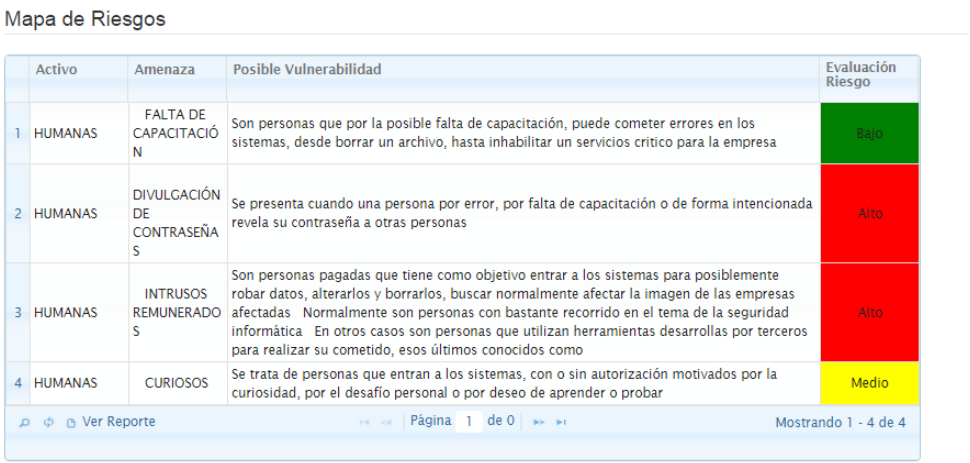
		Activo	Amenaza	Posible Vulnerabilidad	Calificación: Probabilidad	Impacto	Resultad	Evaluación Riesgo	Evaluar Riesgo	Eliminar
1		HUMANAS	FALTA DE CAPACITACIÓN	Son personas que por la posible falta de capacitación, puede cometer errores en los sistemas, desde borrar un archivo, hasta inhabilitar un servicios critico para la empresa	0,0	0,0	0,0	Bajo		
2		HUMANAS	DIVULGACIÓN DE CONTRASEÑAS	Se presenta cuando una persona por error, por falta de capacitación o de forma intencionada revela su contraseña a otras personas	5,0	5,0	5,0	Alto		
3		HUMANAS	INTRUSOS REMUNERADOS	Son personas pagadas que tiene como objetivo entrar a los sistemas para posiblemente robar datos, alterarlos y borrarlos, buscar normalmente afectar la imagen de las empresas afectadas Normalmente son personas con bastante recorrido en el tema de la seguridad informática En otros casos son personas que utilizan herramientas desarrollas por terceros para realizar su cometido, esos últimos conocidos como	3,0	4,8	3,9	Alto		
4		HUMANAS	CURIOSOS	Se trata de personas que entran a los sistemas, con o sin autorización motivados por la curiosidad, por el desafío personal o por deseo de aprender o probar	2,1	3,0	2,6	Medio		

Ver mapa de riesgo | Página 1 de 1 | Mostrando 1 - 4 de 4

Figura 44 Resumen de Evaluación de las Amenazas Software Propuesto.

Para terminar el proceso se procede a seleccionar la opción de Ver Mapa de Riesgo y se mostrarán los riesgos seleccionados y su nivel de criticidad, finalmente el usuario evaluador puede seleccionar la opción de Ver Reporte para descargar el informe con las recomendaciones para intervenir los riesgos seleccionados.

En la *Figura 45 Resultado de las Amenazas,* se pueden apreciar algunos riesgos seleccionados después de su evaluación:



Mapa de Riesgos

	Activo	Amenaza	Posible Vulnerabilidad	Evaluación Riesgo
1	HUMANAS	FALTA DE CAPACITACIÓN	Son personas que por la posible falta de capacitación, puede cometer errores en los sistemas, desde borrar un archivo, hasta inhabilitar un servicios critico para la empresa	Bajo
2	HUMANAS	DIVULGACIÓN DE CONTRASEÑAS	Se presenta cuando una persona por error, por falta de capacitación o de forma intencionada revela su contraseña a otras personas	Alto
3	HUMANAS	INTRUSOS REMUNERADOS	Son personas pagadas que tiene como objetivo entrar a los sistemas para posiblemente robar datos, alterarlos y borrarlos, buscar normalmente afectar la imagen de las empresas afectadas Normalmente son personas con bastante recorrido en el tema de la seguridad informática En otros casos son personas que utilizan herramientas desarrollas por terceros para realizar su cometido, esos últimos conocidos como	Alto
4	HUMANAS	CURIOSOS	Se trata de personas que entran a los sistemas, con o sin autorización motivados por la curiosidad, por el desafío personal o por deseo de aprender o probar	Medio

Ver Reporte | Página 1 de 0 | Mostrando 1 - 4 de 4

Figura 45 Resultado de las Amenazas.

4.4.2.3. Fase de seguimiento (Verificar) monitorear y revisar el SGSI

4.4.2.3.1. Evaluación del desempeño

Esta sección forma parte de la fase de Revisión del ciclo PHVA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección. [87]

4.4.2.3.1.1. Seguimiento, medición, análisis y evaluación

Se debe evaluar el desempeño del SGSI y la eficiencia del mismo. Según la cláusula 9.1 de la Norma Técnica NTC-ISO-IEC COLOMBIANA 27001, la organización debe determinar:

“a) a qué es necesario hacer seguimiento y qué es necesario medir, incluidos los procesos y controles de la seguridad de la información;
b) los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos; comparables y reproducibles.
c) cuándo se deben llevar a cabo el seguimiento y la medición;
d) quién debe llevar a cabo el seguimiento y la medición;
e) cuándo se deben analizar y evaluar los resultados del seguimiento y de la medición; y
f) quién debe analizar y evaluar estos resultados.

La organización debe conservar información documentada apropiada como evidencia de los resultados del monitoreo y de la medición. “[87]

4.4.2.3.1.2. Auditoría Interna

Se deben programar auditorías internas, con intervalos planificados para verificar el estado del SGSI

De debe verificar que:

“a) es conforme con:
1) los propios requisitos de la organización para su sistema de gestión de la seguridad de la información; y

2) los requisitos de esta Norma;
b) está implementado y mantenido eficazmente.

La organización debe:
c) planificar, establecer, implementar y mantener uno o varios programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación, y la elaboración de informes. Los programas de auditoría deben tener en cuenta la importancia de los procesos involucrados y los resultados de las auditorías previas;
d) para cada auditoría, definir los criterios y el alcance de ésta;
e) seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría;
f) asegurarse de que los resultados de las auditorías se informan a la dirección pertinente;
y g) conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de ésta. [88]

Recurso Auditorias

Como apoyo en este proceso se recomienda tener en cuenta el documento llamado "**Anexo 13 Auditoria**" el cual está identificado como "**Anexo 13 Auditoria.docx**" en este trabajo de grado. En él se presenta un formato modelo que tiene como intención realizar auditorías a la implementación del SGSI.

4.4.2.3.1.3. Revisión por la dirección.

La alta dirección debe verificar el SGSI en tiempos determinados para asegurarse de la conveniencia y eficacia continúa. Esta verificación debe incluir entre otros:
Establecer un proceso de revisión por la dirección.
Planear un proceso de revisión SGSI de la organización.
Revisar el rendimiento de sus SGSI.
Generar salidas de revisión de gestión.
Mantener un registro de los resultados de la revisión realizada.

Recurso Revisión por la dirección

Como ayuda en este proceso se recomienda tener en cuenta el documento llamado "**Anexo 14 Revisión Por La Dirección**" el cual está identificado como "**Anexo 14 Revisión Por La Dirección.docx**" en este trabajo de grado, en él se presenta un formato modelo que tiene como intención realizar la revisión por parte de la alta gerencia al SGSI.

4.4.2.4. Fase de mejora (Actuar) mantener y mejorar el SGSI

4.4.2.4.1. Mejora

Eesta sección forma parte de la fase de Mejora del ciclo PHVA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua

4.4.2.4.1.1. No conformidades y acciones correctivas

Cuando se presenta una no conformidad la organización debe:

- Identificar claramente cuáles son las no conformidades.
- Reaccionar a las no conformidades de la organización.
- Implementar acciones correctivas para hacer frente a las causas.
- Revisar la eficacia de sus acciones correctivas.
- Cambiar el SGSI de la organización siempre que sea necesario.

4.4.2.4.1.2. Mejora continua

Las organizaciones deben mejorar continuamente la conveniencia, las adecuaciones y la eficacia del SGSI.

4.4. Etapa 3: Marco legal

En esta etapa se revisarán algunos aspectos jurídicos que se deben tener en cuenta cuando se quiere implementar un SGSI y algunas normas que están directamente relacionadas con el proceso de implementación.

4.5.1. Reflexión desde lo jurídico

Según el doctor Arean Hernando Velasco Melo sobre ISO27001: "*Lo primero a lo que se debe dar claridad es que la ISO27001 es un estándar de gestión estratégica que conduce a conseguir mejorar la protección de la información, su relación con los aspectos jurídicos son un tema que no puede olvidar el departamento jurídico de las organizaciones que desean emprender el camino de la implementación de un SGSI".* [89]

Al respecto, el doctor Velasco Melo –el cual tuve la fortuna de tener como docente en esta maestría- plantea en su trabajo titulado "El derecho informático y la gestión de la seguridad de la información una perspectiva con base en la norma ISO27001" [83] que se pueden identificar seis grandes temas desde la perspectiva jurídica: La protección de datos personales, la contratación de bienes informáticos y telemáticos; el derecho laboral y prestación de servicios, respecto de la regulación de aspectos tecnológicos; los servicios de comercio electrónico; la propiedad intelectual y el tratamiento de los incidentes informáticos.

En su trabajo el doctor Velasco Melo establece relaciones entre cada uno de estos seis grandes temas y los controles presentados por la norma ISO27001, podríamos establecer algunos ejemplos; en lo referente a la protección de los datos, se puede revisar el dominio 18.1.4 Protección de datos y privacidad de la información personal, en lo relacionado con la contratación de bienes informáticos y telemáticos, se podría revisar el dominio 15 Relaciones Con Suministradores o en lo referente a los servicios de comercio electrónico, podríamos citar el dominio 13.2.3 Mensajería electrónica, para ser revisado.

La anterior reflexión es solo uno de los múltiples elementos que se deben tener en cuenta al momento de establecer alguno de los controles planteados por el ISO2700.

4.5.2. Normatividad

A continuación se presentan algunas de las normas que protegen y regulan diferentes aspectos relacionados con la gestión de la información.

4.5.2.1. Propiedad intelectual

Según La Superintendencia de Industria y Comercio: [90] "*La Propiedad Intelectual hace referencia a toda creación del intelecto humano. Las obras literarias, artísticas y científicas; las interpretaciones de los artistas intérpretes y las ejecuciones de los artistas ejecutantes, los fonogramas y las emisiones de radiodifusión; las invenciones en todos los campos de la actividad humana; los descubrimientos científicos; los dibujos y modelos industriales; las marcas de fábrica, de comercio y de servicio, así como los nombres y denominaciones de origen; y todos los demás derechos relativos a la actividad intelectual en los terrenos industrial, científico, literario y artístico.*

Los derechos de Propiedad Intelectual se dividen en dos ramas que protegen los intereses de los creadores al ofrecerles ventajas en relación con sus creaciones: La propiedad Industrial y La Protección a Derechos de Autor." [90] La normatividad colombiana que vela por el correcto manejo de la propiedad intelectual es:

4.5.2.2. Decreto 1162 de 2010

Este decreto establece el Sistema Administrativo Nacional de Derecho de Autor y la Comisión Intersectorial de PI (CIPI). CIPI es el órgano de coordinación para el Sistema Administrativo Nacional de la Propiedad Intelectual, que es el conjunto de políticas, directrices, normas, actividades, recursos, programas e instituciones públicas y privadas relacionadas con la propiedad intelectual. [91]

4.5.2.3. Decreto 4540 de 2006

Este Decreto faculta a la autoridad aduanera para intervenir en relación con mercancías supuestamente piratas o de marca falsificada; vinculadas a una importación, exportación o tránsito.

4.5.2.4. Derechos de autor

Según el centro Colombiano de Derecho de Autor, el derecho de autor [91] es "*el conjunto de reglas que salvaguardan al autor como creador de una obra, entendida ésta, como toda expresión humana producto del ingenio y del talento que se ve materializada de cualquier forma perceptible por los sentidos y de manera original, particularmente en el campo literario y artístico. En consecuencia se protegen las obras literarias en cualquier forma, los dibujos, pinturas, esculturas, obras fotográficas, audiovisuales. Los programas de computador, las adaptaciones, traducciones y en general, toda obra en el campo literario o artístico que pueda definirse o reproducirse por cualquier medio conocido o por conocer."* [91] Los elementos de la legislación colombiana que protegen los derechos de autor son:

4.5.2.5. Decisión 351 de la C.A.N.

Tiene como objetivo "reconocer una adecuada y efectiva protección a los autores y demás titulares de derechos, sobre las obras del ingenio, en el campo literario, artístico o científico, cualquiera que sea el género o forma de expresión y sin importar el método literario o artístico ni su destino. Así mismo se protegen los derechos conexos."[92]

4.5.2.6. Ley 23 de 1982.

Esta ley garantiza la protección a los autores de obras literarias, científicas y artísticas, al igual que a los intérpretes o ejecutantes, a los productores de programas y a los organismos de radiodifusión, en sus derechos conexos a los del autor. [93]

4.5.2.7. Decreto 1360 de 1989

Este Decreto regula a "Derecho de Autor & Expresiones Culturales Tradicionales, Ley (N º 23), 1982" en relación con el registro de software, como creación en el campo literario, en el Registro Nacional de Derecho de Autor.

4.5.2.8. Ley 44 de 1993

Esta ley modifica y adiciona la Ley 23 de 1982 y modifica la Ley 29 de 1944. Contempla disposiciones relacionadas con el Registro Nacional del Derecho de Autor y las Sociedades de Gestión Colectiva de Gestión Colectiva de Derechos de Autor y Derechos Conexos. [94]

4.5.2.9. Decreto 460 de 1995

Este decreto se refiere a la protección que se le brinda a las obras literarias y artísticas, así como a las interpretaciones y demás producciones salvaguardadas por el derecho conexo. [95]

4.5.2.10. Ley 545 de 1999

Se refiere a la protección de los derechos de los artistas intérpretes o ejecutantes y los productores de fonogramas. [96]

4.5.2.11. Ley 603 de 2000

La Ley 603 de 2000, en el Artículo segundo faculta a las autoridades tributarias colombianas para “verificar el estado de cumplimiento de las normas sobre derechos de autor, para impedir que a través de su violación, se evadan tributos”. [97]

4.5.2.12. Propiedad industrial

La Propiedad Industrial es el derecho exclusivo que posee una persona física o jurídica sobre una invención (patentes y modelos de utilidad), un signo distintivo (marcas y nombres comerciales) o un diseño industrial. [99] La normatividad destinada a su protección es:

Ley 1648 de 2013

Esta ley establece medidas de observancia a los Derechos de Propiedad Industrial en Colombia, en el marco del Tratado de Libre Comercio con Estados Unidos. [100]

4.5.2.13. Decisión 486 de la C.A.N.

Se refiere a la protección que tiene cada país con respecto a la propiedad industrial. [101]

La Decisión 486 aborda aspectos precisos en materia de patentes de invención, diseños industriales, marcas, denominación de origen y competencia desleal vinculada a la propiedad industrial, entre otros aspectos.

4.5.2.14. Comercio electrónico y firmas digitales

El E-commerce o Comercio Electrónico consiste en la distribución, venta, compra, marketing y suministro de información de productos o servicios a través de Internet. Conscientes de estar a la vanguardia, las Pymes no se han quedado atrás en este nuevo mercado, por lo que han hecho de los servicios de la red un lugar que permite acceder a sus productos y servicios durante las 24 horas del día. [102]

La firma digital es un mecanismo equivalente a la firma manuscrita que garantiza la identidad y responsabilidad del autor de un documento o transacción electrónica, así como permite comprobar la integridad del mismo, es decir que la información no ha sido alterada. [103]

La legislación colombiana delimita el manejo del comercio electrónico y las firmas digitales mediante:

4.5.2.15. Ley 527 de 1999

Se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales en Colombia [104].

Esta regulación tiene como objetivo brindar un adecuado tratamiento al contenido de las comunicaciones, denominado intercambio electrónico de informaciones o con sus siglas en inglés “EDI”, aunque no deja de lado otros medios conexos de comunicación de datos. Además recalca la integridad de la información, como atributo jurídico necesario para el desarrollo del comercio electrónico, pues la base para desarrollar confiablemente las nuevas tecnologías está dada por la veracidad del mensaje de datos.

4.5.2.16. Decreto 1747 de 2000.

Este decreto define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, establece las entidades de certificación y dicta otras disposiciones. Valida el uso de la Firma Digital emitida por entidades de certificación digital como mecanismo para garantizar la seguridad jurídica en las comunicaciones electrónicas, a través de los atributos de autenticidad, integridad y no repudio. [105]

4.5.2.17. Resolución 26930 de 2000

Aunque esta resolución se enfoca en los requisitos que deben cumplir las entidades de certificación abiertas o cerradas para solicitar su autorización y funcionamiento, también define los estándares, planes y procedimientos de seguridad para el intercambio de datos a través de medios electrónicos. [106]

4.5.2.18. Protección de datos personales

Los datos personales se refieren a toda aquella información asociada a una persona que nos permite su identificación, como puede ser su cedula, su libreta militar, su historial académico, su historial crediticio, los datos de sus familiares, los datos de sus tarjetas de créditos, los datos de los restaurantes que frecuenta. Siendo algunos datos más sensibles que otros como pueden ser los datos relacionados con la salud.

La Protección de Datos Personales reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de

naturaleza pública o privada.[107] La normatividad vigente para garantizar la protección de los datos es:

4.5.2.19. Ley 1581 de 2012

La ley estatutaria 1581 tiene como objetivo dar a conocer los derechos que tienen todas las personas de conocer, actualizar y rectificar todo tipo de información que posean las organizaciones acerca de ellas en bases de datos o archivos.

Esta ley aplica algunos principios fundamentales para el tratamiento de los datos, los cuales sirven de apoyo para implementar un sistema de gestión de seguridad de la información. [108] Estos principios se encuentran consagrados en el Título II, Articulo 4° y son:

- Principio de legalidad en materia de Tratamiento de datos
- Principio de finalidad
- Principio de libertad
- Principio de veracidad o calidad
- Principio de transparencia
- Principio de acceso y circulación restringida
- Principio de seguridad
- Principio de confidencialidad

4.5.2.20. Ley 1266 de 2008

La Ley 1266 o Ley de Habeas Data se refiere al derecho que tiene toda persona de conocer, actualizar y rectificar la información que se haya recogido sobre ella en archivos y bancos de datos de naturaleza pública o privada [109].

En el artículo 4 de dicha ley, se dan a conocer los principios para la administración de los datos, los cuales son [110]:

- Principio de veracidad o calidad de los registros o datos
- Principio de finalidad
- Principio de circulación restringida
- Principio de temporalidad de la información
- Principio de interpretación integral de derechos constitucionales
- Principio de seguridad

- Principio de confidencialidad

4.5.2.21. Ley 1273 de 2009

Se refiere a los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos [111].

Mediante esta ley, la legislación colombiana se equipara con la de otros países en cuanto a la normatividad sobre el cibercrimen, que ha venido vulnerando distintos campos de las relaciones y comunicaciones personales, empresariales e institucionales.

Dicha ley tipifica como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales o de diferencias térmicas o hidrométricas excesivas.

Para tener un panorama más amplio de las normas que están ligadas a ISO27001:2013 se presentan dos anexos donde se puede apreciar los controles de la ISO27001:2013 y las normas que podrían ser utilices cuando se desee implementar algunos de estos controles.

El documento propuesto es un archivo llamado “**Anexo 15 Controles** ISO27001:2013**”** el cual está identificado como “**Anexo 15 Controles ISO27001:2013.docx**” en este trabajo de grado.

También se propone el archivo llamado “**Anexo 16 Normatividad SGSI**” el cual está identificado como “**Anexo 16 Normatividad SGSI.docx**” en este trabajo de grado.

4.5. Etapa 4. Validación del prototipo

4.5.3. Introducción a la validación

En esta etapa del trabajo de grado se verificará el funcionamiento del mismo, utilizando como base dos instituciones educativas que desean a mediano plazo la implementación

de un SGSI, la primera institución es el Centro Colombo Americano y la segunda es la Institución Universitaria Escolme.

En ambos casos se establecieron aproximaciones con los encargados de sus departamentos de TI, quienes con gusto accedieron a participar de la validación de este prototipo.

4.5.4. Alcance de la validación

En ambas instituciones educativas se acordó hacer el diagnóstico de cómo se encuentran con relación a lo planteado por un SGSI, igualmente se realizará la valoración y el tratamiento de los riesgos, finalmente se harán las recomendaciones para tratar estos riesgos.

Por efectos de tiempo en la realización de este trabajo de grado y teniendo en cuenta que el proceso completo de implementación del SGSI podría tardar varios meses más, se acordó enfocar las pruebas a estos procesos del SGSI.

4.5.5. Entendiendo el Contexto de las instituciones educativas

Como parte de la aplicación del prototipo y como lo sugiere ISO27001:2013, se sostuvieron varias reuniones con los directores de TI de ambas instituciones con el fin de entender sus características y comprender mejor sus necesidades.

Como resultado de este primer acercamiento se pudo recolectar información importante que será presentada a continuación:

4.5.5.1. Colombo Americano de Medellín

El Centro Colombo Americano de Medellín (CCAM) es una institución dedicada a la enseñanza de inglés, la cual posee seis sedes: Sede Centro, Sede San Fernando Plaza, Sede Molinos, Sede Niquía – Bello, Sede Rionegro y Sede Apartadó.

La institución cuenta con múltiples plataformas en las que diariamente aproximadamente el 60% del personal tanto interno como externo (estudiantes, docentes y personal administrativo) hacen uso de ellas.

La Sede Centro cuenta con dos canales de Internet, uno dedicado con ETB con un ancho de banda de 40 megas destinado al área corporativa (personal staff de la institución) y otro con UNE con un ancho de banda de 100 megas (banda ancha) utilizado por dos salas de computo únicas en la sede. A esta misma red, pero en segmentos diferentes están conectados todos los Access Point con los cuales se brindan los servicios de internet WiFi a los estudiantes, empleados y público en general.

En las demás sedes por el tamaño de las mismas se tienen conexiones a internet de 10 megas, con un canal de banda ancha de 10 megas en cada sede.

Actualmente la institución tiene aproximadamente 6 servidores locales, algunos bajo la modalidad de hosting y otros más en la nube.

En cuanto a las estaciones de trabajo se tienen aproximadamente 250 equipos de cómputo en PC y portátiles.

Para finalizar se evidencia que la empresa tiene aproximadamente 230 empleados.

4.5.5.2. Institución Universitaria Escolme

La Institución Universitaria Escolme es reconocida en el sector de la educación superior de Medellín como la primera institución en Colombia con un programa que forma profesionales en el área de Mercadeo.

Actualmente la institución cuenta con 19 programas universitarios y 1 posgrado, todos ubicados en una sede central que cuenta con aproximadamente 120 empleados.

En relación con las conexiones a internet, la empresa cuenta con dos canales de internet dedicado de 100 megas cada uno. Uno de estos es utilizado para la parte administrativa y el otro para la conexión inalámbrica de los estudiantes y público en general.

Escolme cuenta con varios servidores con múltiples plataformas, algunos de ellos están de forma local y otros en una nube privada, del mismo modo cuenta con servidores en la modalidad de servicios.

En cuanto a las estaciones de trabajo, tiene aproximadamente 150 equipos de cómputo entre PC y portátiles.

4.5.5.3. Diagnóstico inicial

Con el ánimo de saber el nivel de adopción del SGSI en estas instituciones se procedió a realizar un diagnóstico inicial utilizando el **Anexo 5 Diagnóstico Cuantitativo de SGSI**, desarrollado para esta propuesta.

4.5.5.3.1. Resultado diagnóstico inicial Colombo Americano

A continuación en la *Figura 46 Resultados 1 Colombo Americano*, y *Figura 47 Resultados 2 Colombo Americano*, se presentan los resultados del Colombo Americano:

DOMINIOS	PORCENTAJE DESARROLLADO
A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN	40%
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	49%
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	33%
A.8 GESTIÓN DE ACTIVOS	46%
A.9 CONTROL DE ACCESO	61%
A.10 CRIPTOGRAFÍA	20%
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO	57%
A.12 SEGURIDAD DE LAS OPERACIONES	67%
A.13 SEGURIDAD DE LAS COMUNICACIONES	51%
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	65%
A.15 RELACIONES CON LOS PROVEEDORES	20%
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	37%
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	65%
A.18 CUMPLIMIENTO	48%
PROMEDIO	47%

Figura 46 Resultados 1 Colombo Americano

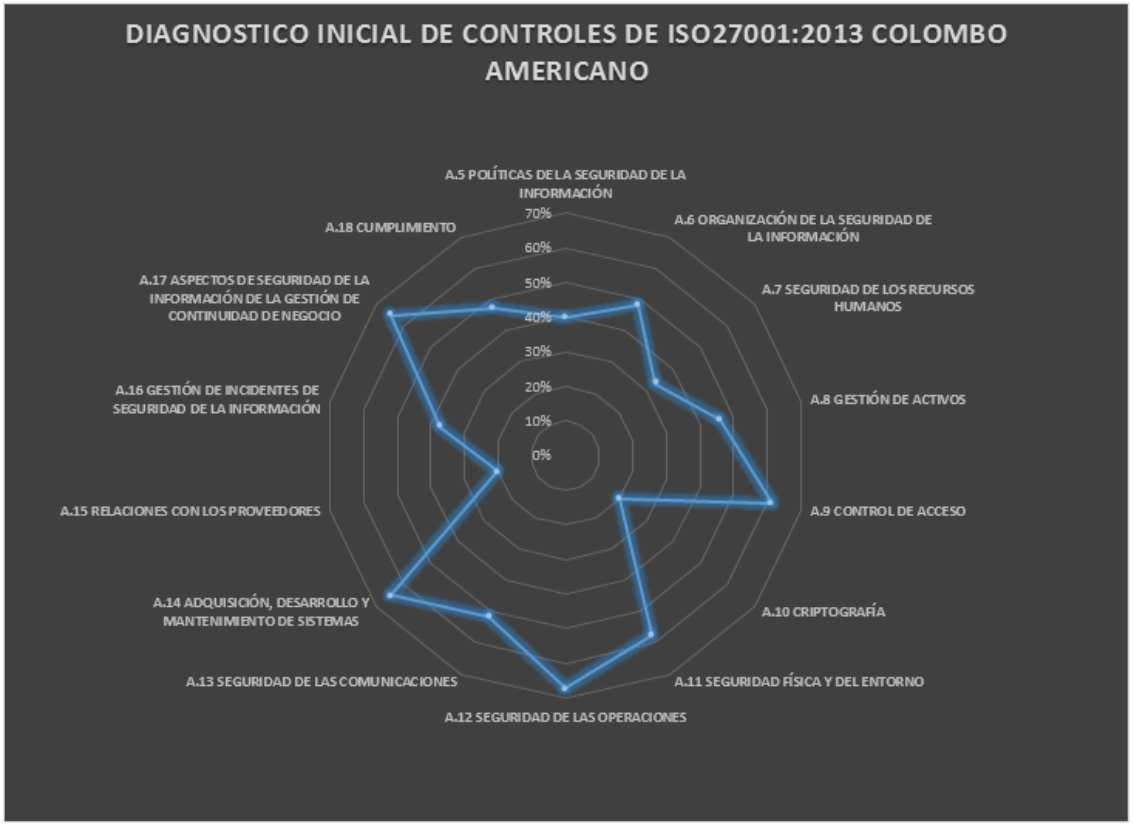


Figura 47 Resultados 2 Colombo Americano.

Podemos observar que el promedio general después de diagnosticar todos los controles es de un 47%, llamando la atención los bajos índices en los dominios de criptografía y relaciones con los proveedores. De igual forma se observan bajos índices en lo relacionado a Seguridad en los Recursos Humanos con un 33% y las Políticas de Seguridad de la Información con un 40%.

Finalmente se puede notar que en lo relacionado a Seguridad de las operaciones con un 67%, Adquisición Desarrollo y Mantenimiento de los Sistemas con un 65% y Aspectos de Seguridad de la Información de la Gestión de Continuidad del Negocio con un 65% nuevamente, son los elementos que mejor evaluación presentaron.

4.5.5.3.2. Resultado diagnóstico inicial Escolme

A continuación en la *Figura 48 Resultados 1 Escolme*, y *Figura 49 Resultados 2 Escolme*, se presentan los resultados la Institución Universitaria Escolme.

DOMINIOS	PORCENTAJE DESARROLLADO
A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN	20%
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	37%
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	20%
A.8 GESTIÓN DE ACTIVOS	34%
A.9 CONTROL DE ACCESO	33%
A.10 CRIPTOGRAFÍA	0%
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO	57%
A.12 SEGURIDAD DE LAS OPERACIONES	70%
A.13 SEGURIDAD DE LAS COMUNICACIONES	37%
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	55%
A.15 RELACIONES CON LOS PROVEEDORES	60%
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	46%
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	50%
A.18 CUMPLIMIENTO	63%
PROMEDIO	42%

Figura 48 Resultados 1 Escolme.

Figura 49 Resultados 2 Escolme.

Podemos observar que el promedio general después de diagnosticar todos los controles es de un 42%, llamando la atención los bajos índices en los dominios de criptografía con un 0%, Políticas de Seguridad de la Información con un 20% y Seguridad en los Recursos Humanos de igual modo con un 20%. De igual forma se observan bajos índices en el relacionado a Controles de acceso con un 33% y Gestión de Activos con un 34%.

Finalmente se puede notar que en lo relacionado a Seguridad de las Operaciones con un 70% y Cumplimiento con un 63%, son los elementos que mejor evaluación presentaron.

4.5.5.4. Evaluación y tratamiento de los riesgos en las instituciones.

Para el proceso de evaluación de los riesgos se solicitó a ambas instituciones educativas detallar cuáles eran los procesos más críticos en sus empresas con la intención de clasificarlos según la lista de activos y amenazas que se diseñaron en este trabajo de grado.

A continuación se presentan los procesos que dentro de las instituciones evaluadas son considerados críticos:

4.5.5.4.1. Procesos considerados críticos por el Colombo Americano.

- SAI: Sistema académico de la institución.
- Matriculas en línea: proceso de matrículas en internet realizado por los estudiantes.
- Servidor de dominio: servidor que controla todos los usuarios y objetos de la red.
- Servidor de contabilidad: Servidor institucional para el manejo de nómina, contabilidad y los activos de la empresa.
- Correo electrónico: Servicios de correo electrónico ubicados en un hosting fuera de la empresa.
- Internet: Conexión a Internet.
- Telefonía IP: Todos los teléfonos están conectados a una plataforma de telefonía IP llamada Centrex.
- Dispositivos de comunicaciones locales: Todos los equipos de comunicaciones de la empresa, como enrutadores, Swiches, Access Point y demás elementos necesarios para el funcionamiento de la red de datos.
- Energía: Luz eléctrica disponible 24x7.
- Base de datos Académica: existe una en Oracle donde se almacenan todos los procesos académicos de la institución.
- Servidor de aplicativo cine: Es un servidor donde se almacenan las películas que se proyectan en las salas de cine, es administrado algunas veces de forma remota por los distribuidores de las películas.
- WiFi: Es el servicio de conexión a internet inalámbrico que tiene la institución, para atender la demanda de todos sus públicos.
- Página web institucional: Es el sitio web corporativo.

4.5.5.4.2. Procesos considerados críticos por Escolme.

- WiFi: Es el servicio de conexión a internet inalámbrico que tiene la institución para todos sus públicos.
- Academusoft: Sistema académico de la institución.
- Servidor contable y de activos: Servidor institucional para la contabilidad y los activos de la empresa.
- Correo electrónico: Servicios de correo electrónico ubicado de toda la institución.
- Página web institucional: Es el sitio web corporativo.
- Bases de datos de académica: registro académico de los estudiantes.
- Servidores dominio: servidor que controla todos los usuarios y objetos de la red.
- Internet: Conexión a Internet.
- Equipos de comunicaciones locales: Todos los equipos de comunicaciones de la empresa, como enrutadores, Swiches, Access Point y demás elementos necesarios para el funcionamiento de la red de datos.

Después de realizar el análisis, llama la atención como varios de los procesos considerados críticos se repiten en ambas las instituciones.

Después de tener los procesos críticos de las instituciones se procedió a realizar la evaluación de los riesgos, inicialmente utilizando el **Anexo 9 Gestión de Riegos de SGSI** propuesto en este trabajo de grado. A continuación se presentan los aspectos más relevantes de esta evaluación.

4.5.5.4.3. Tratamiento de los riesgos Colombo Americano

Después de realizar el tratamiento de los riesgos para el Colombo Americano, se obtuvieron los resultados que se presentan en la *Figura 50 Resultado Tratamiento de los Riesgos Colombo Americano*:

ESTA INFORMACION LA TRAE EL SISTEMA NO SE DEBE EDITAR				INGRESE LOS VALORES		FORMA AUTOMATICA NO EDITAR	
#	ACTIVOS	ACTIVOS	POSIBLE VULNERABILIDAD(DEFINIR POSIBLES VULNERABILIDADES	CALIFICACION		RESULTADO	EVALUACION RIESGO
				PROBABILIDAD	IMPACTO		
1	SOFTWARE	SOFTWARE ACADEMICO SAI	Acceso no autorizado al programa académico, borrado de datos	3,0	5,0	4,0	ALTO
2	SOFTWARE	MATRICULAS EN LINEA	Disponibilidad del servicios o fraude al momento del pago	3,0	4,0	3,5	MEDIO
3	HARDWARE	SERVIDOR DE CINE	Disponibilidad del servidor y cambios no autorizados cuando se conectan de forma remota	3,0	3,0	3,0	MEDIO
4	HARDWARE	SERVIDOR DE DOMINIO	Suplantación de usuarios, borrado de datos, divulgaciones de contraseñas, entre otros	4,0	3,0	3,5	MEDIO
5	HARDWARE	SERVIDOR DE CONTABLE	Acceso no autorizado al servidor, disponibilidad del servidor	2,0	5,0	3,5	ALTO
6	SERVICIOS	SERVICIO DE CORREO INSTITUCIONAL	Disponibilidad del servicio de correo electrónico	3,0	3,0	3,0	MEDIO
7	SERVICIOS	SERVICIOS DE INTERNET	Disponibilidad del Servicios de internet, ingreso a páginas no autorizadas, descarga de programas no autorizados	4,0	4,0	4,0	ALTO
8	SERVICIOS	SERVICIOS DE WIFI	Disponibilidad del Servicios de internet WIFI, ingreso a páginas no autorizadas, descarga de programas no autorizados	4,0	4,0	4,0	ALTO
9	SERVICIOS	TELEFONIA	Disponibilidad de la telefonía, interceptación de las llamadas realizadas	3,0	2,0	2,5	MEDIO
10	INFRAESTRUCTURA	PROBLEMAS CON LOS EQUIPOS DE COMUNICACIÓN (SWITCHES, ROUTER, FIREWALL, ETC.)	Disponibilidad de los equipos de comunicaciones, ataques internos y externos	4,0	5,0	4,5	ALTO
11	HARDWARE	SUMINISTRO DE ENERGÍA	Sabotaje al suministro de energía, problemas de energía causados por agentes externos o internos	3,0	5,0	4,0	ALTO
12	APLICATIVOS	PAGINA WE INSTITUCIONAL	Disponibilidad de todos los púbicos a la página institucional, todo tipo de ataques informáticos en contra del servidor para impedir el funcionamiento adecuado de la pagina web	3,0	4,0	3,5	MEDIO
13	DATOS	ACCESO NO AUTORIZADO A LA BASE DE DATOS PROPIETARIO	Suplantación y cambios no autorizados en la base de datos académica, borrado de datos, disponibilidad del servicio de base de datos	4,0	4,0	4,0	ALTO

Figura 50 Resultado Tratamiento de los Riesgos Colombo Americano.

Como se puede observar todos sus procesos están entre Medio y Alto según la métrica utilizada.

4.5.5.4.4. Tratamiento de los riesgos Escolme

Después de realizar el tratamiento de los riesgos para el Escolme, se obtuvieron los resultados que se presentan en la *Figura 51 Resultado Tratamiento de los Riesgos Escolme*:

ESTA INFORMACION LA TRAE EL SISTEMA NO SE DEBE EDITAR				INGRESE LOS VALORES		ESTA INFORMACION SE CALCULA DE FORMA AUTOMATICA NO EDITAR	
#	ACTIVOS	ACTIVOS	POSIBLE VULNERABILIDAD(DEFINIR POSIBLES VULNERABILIDADES	CALIFICACION		RESULTADO	EVALUACION RIESGO
				PROBABILIDAD	IMPACTO		
1	SERVICIOS	SERVICIOS DE WIFI	Disponibilidad del Servicios de internet WIFI, ingreso a páginas no autorizadas, descarga de programas no autorizados	2,0	2,0	2,0	BAJO
2	SOFTWARE	SOFTWARE ACADEMICO ACADEMUSOFT	Acceso no autorizado al programa académico, borrado de datos	4,0	5,0	4,5	ALTO
3	HARDWARE	SERVIDOR DE CONTABLE	Disponibilidad del servicios o fraude al momento del pago	3,0	3,0	3,0	MEDIO
4	APLICATIVOS	APLICATIVOS DE CORREO	Acceso no autorizado al servidor, disponibilidad del servidor	4,0	3,0	3,5	MEDIO
5	APLICATIVOS	PAGINA WEB INSTITUCIONAL	Disponibilidad de todos los púbicos a la página institucional, todo tipo de ataques informáticos en contra del servidor para impedir el funcionamiento adecuado de la página web	5,0	4,0	4,5	ALTO
6	DATOS	NO ACCESO A LAS BASES DE DATOS PROPIETARIOS	Cambios en la base de datos sin Autorización	3,0	4,0	3,5	MEDIO
7	HARDWARE	SERVIDOR DE DOMINIO	Suplantación de usuarios, borrado de datos, divulgaciones de contraseñas, entre otros	3,0	4,0	3,5	MEDIO
8	SERVICIOS	SERVICIOS DE INTERNET	Disponibilidad del Servicios de internet, ingreso a páginas no autorizadas, descarga de programas no autorizados	3,0	5,0	4,0	ALTO
9	INFRAESTRUCTURA	PROBLEMAS CON LOS EQUIPOS DE COMUNICACIÓN (SWITCHES, ROUTER, FIREWALL, ETC.)	Disponibilidad de los equipos de comunicaciones, ataques internos y externos	5,0	5,0	5,0	ALTO

Figura 51 Resultado Tratamiento de los Riesgos Escolme.

Como se puede observar, la mayor parte de los procesos críticos de Escolme fueron evaluados entre Medio y Alto, solo se evidencia un proceso con evaluación de “Bajo”

Para complementar este proceso, en ambas instituciones se entregó el programa para realizar la evaluación y tratamiento de los riesgos.

4.5.5.4.5. Conclusiones del tratamiento de los riesgos en las instituciones educativas

- Ambas instituciones tienen varios procesos en común, considerados críticos.
- Si bien las herramientas utilizadas en cada institución fueron útiles para la evaluación y tratamiento de los riesgos, es necesario hacer adecuaciones, dependiendo de la organización donde se use.
- La mitigación de los riesgos está limitada a los contextos propios de cada institución.

5. CONCLUSIONES PRINCIPALES

- La seguridad de la información se puede lograr desarrollando un adecuado grupo de controles donde se incluyan políticas, procesos y procedimientos, que las organizaciones puedan administrar por medio de software y hardware, con ISO27001:2013, las instituciones educativas y las empresas en general pueden lograr la implementación de un SGSI, aplicado a sus propios contextos y mejorando los niveles de seguridad de la información.

- La seguridad de un sistema informático depende de diversos factores, entre los que se puede destacar la sensibilización de los directivos y responsables de la organización, los conocimientos, capacidades e implicación de los responsables del sistema informático, la mentalización, formación y asunción de responsabilidades de todos los usuarios del sistema, entre otros. Por medio de la implementación de un SGSI, se puede contribuir a que cada uno de estos factores sea impulsado por medio de actividades establecidas en las diferentes etapas de implementación de un SGSI.

- Si una organización es víctima de algún ataque informático, la estabilidad de la compañía y el cumplimiento de sus objetivos corporativos podrían verse afectados de manera significativa, por lo que es necesario adaptar un método que permita minimizar el impacto que este tipo de ataques puede causar. Por medio de la implementación de un SGSI, las organizaciones pueden contar con herramientas para mejorar los niveles de seguridad y estar preparados para enfrentar este tipo de adversidades.

- Después de revisar la XIV Encuesta Nacional de Seguridad Informática, realizada por ACIS en 2014, se puede decir que a nivel de estándares internacionales IS027001:2013, ITIL Y COBIT, siguen incrementado sus niveles de aceptación y uso en las empresas por lo que se convierten en herramientas necesarias para desarrollar diseños de la seguridad de la información.

El modelo PHVA desarrollado por William Edwards Deming se acomoda de forma eficiente a la propuesta de implementación del SGSI permitiendo la mejora continua y la supervisión oportuna en cada una de sus fases.

- Una metodología de análisis de riesgos permite identificar las amenazas y las vulnerabilidades que afectan los activos y calcular el nivel de riesgo. Existen múltiples mecanismos para realizar este proceso, lo importante es que los métodos de determinar los activos de la organización, la identificación de amenazas y vulnerabilidades y tratamiento de las mismas, sea tratado de forma adecuada. Este proceso se puede realizar de forma documentada, precisa, reflexiva y gráfica por medio de las herramientas propuestas en este trabajo de grado, las cuales deben ser adaptadas y personalizadas según las realidades y necesidades de la empresa.

- La propuesta diseñada en este trabajo de grado es una oportunidad para las pequeñas y medianas empresas que deseen implementar un SGSI o que deseen madurar sus procesos de seguridad informática; los diferentes elementos entregados se pueden adaptar y utilizar según las necesidades y los contextos de las empresas.

- El éxito de los SGSI depende de muchos elementos entre los que se pueden resaltar, el apoyo de la alta dirección, una planeación adecuada, la participación de todas las dependencias donde se desea implementar y un seguimiento constante.

- Dependiendo de los procesos que se desean medir, por medio de las herramientas propuestas en este trabajo de grado las empresas medianas y pequeñas, al igual que las empresas del sector educativo, pueden tener elementos que respondan a las características de cada uno de estos puntos.

- Si bien los elementos propuestos en este trabajo de grado pueden ayudar a las empresas medianas y pequeñas al igual que a las empresas del sector educativo a buscar la implementación de un SGSI, si se piensa en un proceso de certificación se recomienda el acompañamiento de empresas especializadas en estos procesos como puede ser SGS Colombia S.A.

- Todos los elementos que se proponen en este trabajo de grado son el producto de meses de evaluación de diferentes sitios web, el análisis detenido de los estándares ISO27001:2013 e ISO27002:2013, herramientas para trabajar con SGSI, análisis de esquemas de implementación de SGSI, Gap de Análisis propuestos por diferentes autores para la evaluación de SGSI, documentos sobre mejores prácticas para implementar SGSI, software licenciados y libres para la implementación de SGSI , libros de seguridad que permitieron dar el enfoque diferenciador al trabajo de grado desde la Seguridad Informática, métodos cuantitativos y cualitativos para medir y tratar los riesgos. Todos estos tuvieron como resultado el esquema propuesto para la implementación de SGSI.

- El programa desarrollado y entregado en este trabajo de grado es uno de los elementos vitales y valores agregados que tiene el mismo, fue desarrollado gracias a la experiencia adquirida en los estudios realizados en el énfasis de seguridad informática de la Maestría en Tecnologías de Información y Comunicación, el conocimiento entregado por todos mis docentes y en especial por la ayuda y todos los conocimientos entregados por el asesor de este trabajo de grado, el PhDc. **Reinaldo Mayol**.

- Otro de los procesos vitales para la implementación de un SGSI, es la concientización al interior de las empresas, la campaña de comunicación debe ser clara y llegar a todos los empleados en un lenguaje sencillo, con piezas gráficas que ayuden en el entendimiento a todos los miembros de la empresa. La campaña

propuesta en este trabajo de grado es un punto de partida para que las compañías adopten sus propias ideas.

- Los procesos que se planean en este trabajo de grado pueden ser utilizados de forma completa o de forma parcial, es decir dependiendo del tipo de empresa es posible que algunos de los elementos propuestos no sean adecuados, pero en otros contextos es también posible que se pueda sacar provecho de cada uno de ellos, buscando el fortalecimiento y preparación en miras de la implementación de un SGSI.

6. BIBLIOGRAFÍA

[1]Sheikhpour, R., & Modiri, N. (2012). A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management. Indian Journal of Science \& Technology, 5(2), 2170-2176. Obtenido de http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=76480030&lang=es&site=ehost-live

[2] Flores Barrios, M. C., del Ángel, M. S., Camacho Díaz, O. D., & Barrera Reyes, M. A. (2011). EVALUACIÓN DEL IMPACTO DE LOS SISTEMAS DE GESTION DE SEGURIDAD DE LA INFORMACIÓN BAJO LA SERIE ISO/IEC 27001 EN EMPRESAS DE LA CIUDAD DE TUXPAN, VERACRUZ. (Spanish). Revista de la Alta Tecnología y Sociedad, 5(1), 44-49. Obtenido de

http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=67073510&lang=es&site=ehost-live

[3] Informe sobre Amenazas a la Seguridad en Internet, 2014, Vol. 19

[4] Mirela, G., & Maria, B. D. (2008). INFORMATION SECURITY MANAGEMENT SYSTEM. Annals of the University of Oradea, Economic Science Series, 17(4), 1358-1363. Obtenido de http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=48755877&lang=es&site=bsi-live

[4] Mirela, G., & Maria, B. D. (2008). INFORMATION SECURITY MANAGEMENT SYSTEM. Annals of the University of Oradea, Economic Science Series, 17(4), 1358-1363. Obtenido de

http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=48755877&lang=es&site=bsi-live

[5] Jeimy J. Cano. (2012) Pronósticos de seguridad de la información. [En Línea]. Disponible: http://www.infosecurityvip.com/newsletter/palabras_feb12.html

[6] National Security Institute. (2004). Improving Security from the Inside Out Improving Security from the Inside Out. [En línea]. Disponible: http://nsi.org/SECURITYsense.html

[7] J. Cano. (17-Jun-2008). Métricas en Seguridad Informática. [En línea]. Disponible:

http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VIII_JornadaSeguridad/07-MetricasSeguridadInformaticaUnaRevisionAcademica.pdf.

[8] D. Páramo Morales. (Jun-2001). Hacia La Construcción De Un Modelo De Cultura Organizacional Orientada Al Mercado. [En línea]. Disponible: http://editorial.unab.edu.co/revistas/rcmarketing/pdfs/r22_art5_c.pdf.

[9] Davidrajuh, R., "Is Norway an information society?" *Information and Financial Engineering (ICIFE), 2010 2nd IEEE International Conference on*, vol., no., pp.918, 921, 17-19 Sept. 2010 doi: 10.1109/ICIFE.2010.5609503

[10] Apropiación y masificación de las tecnologías de la información y las comunicaciones (TIC) en las cadenas productivas como determinante para la competitividad de las Mipyme, Germán Eliécer Rodríguez Melo, Localización: Criterio Libre, ISSN 1900-0642, Nº. 15, 2011, págs. 213-230

[11] Betarte, G.; Corti, M.E., "Design and implementation of a computer security Diploma," *Computing Conference (CLEI), 2013 XXXIX Latin American* , vol., no., pp.1,6, 7-11 Oct. 2013, doi: 10.1109/CLEI.2013.6670620

URL: http://aplicacionesbiblioteca.udea.edu.co:2262/stamp/stamp.jsp?tp=&arnumber=6670620&isnumber=6670594

[12] ISO/IEC 13335-1:2004 Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management. EEUU.

[13] Rehman, H.; Masood, A.; Cheema, A.R., "Information Security Management in academic institutes of Pakistan," Information Assurance (NCIA), 2013 2nd National Conference on, vol., no., pp.47, 51, 11-12 Dec. 2013, doi: 10.1109/NCIA.2013.6725323 URL: http://aplicacionesbiblioteca.udea.edu.co:2262/stamp/stamp.jsp?tp=&arnumber=6725323&isnumber=6725308

[14]J. J. Cano, “Rastreando la inseguridad de la información,” *Rev. Sist.*, 2006.

[15] Instituto Nacional de Tecnologías de la comunicación (INTECO), «Sistema de Gestión de la Seguridad de la Información. Familia ISO 27000,» Madrid, 2009.

[16] J. J. Cano, Inseguridad de la información, Bogotá: Alfaomega, 2013.

[17] G. Betarte y M. E. Corti, «Design and Implementation of a Computer Security, » XXXIX Latin America Computing Conference (CLEI), Montevideo, 2013.

[18] ICONTEC, GTC-ISO/IEC 27035. TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN, Bogotá: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), 2012.

[19] Centro de Respuesta a Incidentes de Seguridad Informática de Uruguay (CERTUY), «Que es un incidente,» 5 Marzo 2013. [En línea]. Available: http://www.cert.uy/inicio/incidentes/que_es-un-incidente. [Ultimo accesso: 18 Marzo 2015].

[19] D. Lancey, Managing the Human Factor in Information Security: How to Win over Staff and Influence Business Managers, Washington: John Wiley & Sons, 2009, p. 57.

[20] A. Ortiz Orellana, Seguridad de la Información. Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica, Guatemala: Universidad de San Carlos, 2014, p. 134.

[21] M. A. Amautio Gómez, J. Candua y J. A. Mañas, MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de información. Libro II - Catálogo de Elementos., Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.

[22] M. A. Amautio Gómez, J. Candua y J. A. Mañas, MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método, Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.

[23] J. Costas Santos, Seguridad Informática, Bogotá: Ediciones de La U, 2011.

[24] A. Gómez Vieites, Enciclopedia de la Seguridad Informática, México: Alfaomega Grupo Editorial, 2007.

[25] E. O. Reyes Rivas, «Elementos vulnerables en el sistema informático: hardware, software y datos,» [En línea]. Available: http://www.actiweb.es/reyes_278/archivo3.pdf. [Último acceso: 21 04 2015].

[26] ISO27001.ES, «Sistema de Gestión de la Seguridad de la Información,» [En línea]. Available: http://www.iso27000.es/download/doc_sgsi_all.pdf. [Último acceso: 28 abril 2015].

[27] ICONTEC, NTC-ISO-IEC 27001. TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. REQUISITOS, Bogotá: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), 2013.

[28] SIA, «Gestión del SGSI con la herramienta S2GSI,» [En línea]. Available: http://www.sia.es/noticias/sgsi.pdf. [Último acceso: 17 febrero 2015].

[29] H. Rehman, A. Masood y A. Raza Cheema, «Information Security Management in Academic Institutes of Pakistan, » second National Conference on Information Assurance (NCIA), Pakistan, 2013.

[30] Implantación de un SGSI en la empresa, instituto nacional de tecnología de la comunicación, Inteco, en línea: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

[31] J. F. Giménez Albacete, Seguridad en equipos informáticos, Málaga: IC Editorial, 2014.

[32] Á. Gómez Vieites, Seguridad en equipos informáticos, Bogotá: Ediciones de La U, 2013.

[33] J. Areitio, Seguridad de la Información: Redes, Informática y Sistemas de Información, Madrid: Paraninfo, 2008.

[34] ICONTEC, NTC-ISO/IEC 27005. TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN, Bogotá: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), 2008.

[35] A. Ramírez Castro y Z. Ortiz Bayona, «Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios,» Ingeniería, vol. XVI, nº 2, pp. 56-66, 2009.

[36] ISOTOOLS, «Las claves del éxito para la Gestión de Riesgos».

[37] R. Caralli A., J. Stevens F., L. Young R. y W. Wilson R., Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, Pittsburgh: Carnegie Mellon University, 2007.

[38] G. Stoneburner, A. Goguen y A. Feringa, NIST Special Publication 800-30.Risk Management Guide for Information Technology Systems, Gaithersburg: Departament of Commerce United States of America, 2002.

[39] R. Valbuena, «Seguridad en Redes de Telecomunicaciones e Informática,» 18 Julio 2010. [En línea]. Available: http://seguridaddigitalvenezuela.blogspot.com/2010/07/cramm-software-para-el-manejo-de.html. [Último acceso: 24 abril 2015].

[40] J.-L. Rule, D. Buc, O. Corbier, M. Gagné, M. Hazzan, G. Molines, C. Pineault, L. Poulin, P. Sassevilles, C. Taillon y M. Touboul, Mehari 2010, Paris: CLUSIF, 2010.

[41] ICONTEC, NTC 5254. GESTIÓN DE RIESGOS, Bogotá: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), 2006.

[42] INTECO, «Análisis y valoración de los riesgos. Metodologías,» [En línea]. Available:https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/swf/video_08.swf. [Último acceso: 30 abril 2015].

[43] E. Lázaro Bilbao, «Modelo Unificado de Análisis de Riesgos de Seguridad Física y Lógica,» INTECO, Madrid.

[44] Implementación COBIT 5 an Isaca Framewok 2012 ISACA. Available: www.isaca.org

[45] Procesos Catalizadores COBIT 5 AN ISACA FRAMEWORK. Available: www.isaca.org.

[46] ITIL Diseño del Servicio, Publicado por TSO (The Stationery Office) y disponible en: www.tsoshop.co.uk, Primera publicación en 2009, ISBN 9780113312269

[47] E. E. Ureña Leon, «Sistema de Gestión de la Seguridad de la Información - SGSI,» 19 Octubre 2013. [En línea]. Available: http://es.scribd.com/doc/177410728/sistema-de-gestion-de-seguridad-de-la-informacion-SGSI#scribd. [Ultimo acceso: 07 Abril 2015].

[48] ISO/IEC, International Standard 27000. Information technology - Security techniques - Information security management systems - Overview and vocabulary, Switzerland: ISO/IEC, 2014.

[49] BSI GROUP, «Comenzando con la Gestión de Seguridad de la Información ISO/IEC 27001,» [En línea]. Available: http://www.bsigroup.com/es-MX/seguridad-dela-informacion-ISOIEC-27001/introduccion-isoiec-27001/. [Ultimo acceso: 08 Mayo 2015].

[50] ISO, «ISO/IEC 27001:2013. Information technology -- Security techniques -- Information security management systems -- Requirements, » [En line]. Available: http://www.iso.org/iso/catalogue_detail?csnumber=54534. [Último acceso: 30 abril 2015]

[51] J. Avellaneda Cao, «Análisis detallado de la nueva versión ISO27001:2013,» Firma, Proyectos y Formación, S.L, Madrid, 2013.

[52] C. Gutierrez Amaya, «ISO/IEC 27002:2013 y los cambios en los dominios de control,» Welivesecurity, 12 Diciembre 2013. [En línea]. Available: http://www.welivesecurity.com/la-es/2013/12/12/iso-iec-27002-2013-cambios-dominios-control/. [Ultimo acceso: 07 Mayo 2015].

[53] ISO/IEC, International Standard 27002. Information technology — Security techniques — Code of practice for information security controls, Switzerland: ISO/IEC, 2013.

[54] AUDISIS, «Implementación del Sistema de Gestión de Seguridad de la Información - SGSI,» Bogotá, 2015.

[55] ISO, «ISO/IEC 27005:2011. Information technology -- Security techniques -- Information security risk management, » [En line]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56742. [Ultimo acceso: 28 Abril 2015].

[56] SO, «ISO/IEC 27035:2011. Information technology -- Security techniques -- Information security incident management, » [En line]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44379. [Último acceso: 28 abril 2015].

[57] ICONTEC, NTC-ISO 31000. GESTIÓN DEL RIESGO. PRINCIPIOS Y DIRECTRICES, Bogotá: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), 2011.

[58] Modelo Para Seguridad de la Información en TIC, Jorge Burgos Salazar, Pedro G. Campos. Universidad del Bío-Bío, Avenida Collao 1202, Casilla 5-C P: 4081112. Concepción, Chile

[59] Asociación Colombina de Ingenieros de Sistemas (ACIS) [En línea]. Available: http://52.1.175.72/portal/#about-us

[60] La Encuesta Nacional de Seguridad Informática, capítulo Colombia, realizada por ACIS, a través de Internet, (ACIS) [Online]. Available: http://www.acis.org.co/revistasistemas/index.php/ediciones-revista-sistemas/edicion-131/item/164-tendencias-2014-encuesta-nacional-de-seguridad-informática

[61] Las 15 Certificaciones Mejor Pagadas en 2014 [Online]. Available: http://www.globalknowledge.es/noticias-y-eventos/noticias/las-15-certificaciones-mejor-pagadas-2014/

[62] Norma Técnica NTC-ISO-IEC COLOMBIANA 27001:2013, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

[63] Norma Técnica NTC-ISO-IEC COLOMBIANA 27001:2013, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Cláusula 4.1

[64] Norma Técnica NTC-ISO COLOMBIANA NTC-ISO 31000:2011, Gestión del Riesgo. Principios y Directrices.

[65] Norma Técnica NTC-ISO-IEC COLOMBIANA 27001:2013, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Cláusula 4.2

[66] Serie de plantillas gratis descargadas de ISO27001academy que permiten tener un esquema base propuesto para un proceso determinado del SGSI, Disponible en http://advisera.com/27001academy/es/paquete-de-documentos-sobre-iso-27001/

[67] Norma Técnica NTC-ISO-IEC COLOMBIANA 27001:2013, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Cláusula 4.3

[68] SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN SGSI, Universidad Abierta y a Distancia UNAD, Disponible en: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/41_leccin_16_cmo_definir_el_alcance_del_sgsi.html

Consultado en 01 de Junio de 2015

[68]Guía Técnica Colombiana GTC ISO/IEC 27003:2010, Numeral 6. Definir el Alcance, Los Límites y la Política del SGSI, páginas 15 a 24.

[69]Problemas para definir el alcance de la norma ISO27001:2013, Dejan Kosutic, 27001Academy, Disponible en: http://www.iso27001standard.com/es/blog/2010/06/29/problemas-para-definir-el-alcance-de-la-norma-iso-27001/

Consultado en 01 de Junio de 2015

[70] Norma Técnica NTC-ISO-IEC COLOMBIANA 27001:2013, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Cláusula 4.4

[71] Documento diseñado con base a la matriz de preguntas y respuestas presentadas con herramienta de análisis por 27001 Academy Disponible en http://advisera.com/27001academy/free-tools/free-iso-27001-gap-analysis-tool/

[72] Herramienta Diagnostico construido en Microsoft Excel por el autor del proyecto, permite por medio de preguntas con valoración única, saber el nivel de adaptación que se tiene frente a un SGSI.

[73] Norma Técnica NTC-ISO-IEC COLOMBIANA 27001:2013, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Cláusula 5.1

[74] Implantación de un SGSI en la empresa, INTECO Instituto Nacional de Tecnologías de la Comunicación, España. Páginas 16-18 Disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

[75]“An Introduccion to ISO/IEC 27001:2013”. David Brewer, Police Defined by ISO/IEC 27001:2013 Annex A Controls, Pag. 38-40

[76] Formato e implementación de políticas de seguridad y privacidad de la información propuesto por el Ministerio de las TIC. Disponible en http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

[77] Ejemplos de Políticas Generales Seguridad de la información desarrollados por la empresa SOPHOS Disponible en: https://www.sophos.com/es-es/search-results.aspx?search=politicas de seguridad

[78] Norma Técnica NTC-ISO-IEC COLOMBIANA 27001:2013, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Cláusula 5.3

[79] Formato diseñado con base a la propuesta de SGSI desarrollado en UNIVERSIDAD PEDAGÓGICA Y TECNOLÓGICA DE COLOMBIA, sección Roles y Responsabilidades. Pág. 16-28

[80] Norma Técnica NTC-ISO-IEC COLOMBIANA 27001:2013, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Cláusula 6.1.

[81] Norma Técnica NTC-ISO-IEC COLOMBIANA 27001:2013, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. ANEXO A pág. 13

[82] Norma Técnica NTC-ISO-IEC COLOMBIANA 27001:2013, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Cláusula 6.2.

[83] Norma Técnica NTC-ISO-IEC COLOMBIANA 27001:2013, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Cláusula 7.2.

[84] Norma Técnica NTC-ISO-IEC COLOMBIANA 27001:2013, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Cláusula 7.3.

[85] Norma Técnica NTC-ISO-IEC COLOMBIANA 27001:2013, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Cláusula 7.4.

[86] Norma Técnica NTC-ISO-IEC COLOMBIANA 27001:2013, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Cláusula 8.1.

[87] Norma Técnica NTC-ISO-IEC COLOMBIANA 27001:2013, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Cláusula 9.1.

[88] Norma Técnica NTC-ISO-IEC COLOMBIANA 27001:2013, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Cláusula 9.2.

[89] Arean Hernando Velasco Melo. El derecho informático y la gestión de la seguridad de la información una perspectiva con base en la norma ISO27001 Pág. 10

[90] SUPERINTENDENCIA INDUSTRIA Y COMERCIO. ¿Qué es la Propiedad Intelectual? {En línea}. Disponible en: (http://www.sic.gov.co/drupal/que-es-la-propiedad-intelectual)

[91] CENTRO COLOMBIANO DEL DERECHO DE AUTOR. "Derecho de autor" {En línea}. Disponible en: (http://www.cecolda.org.co/index.php/derecho-de-autor/preguntas-freuentes)

[92] DECISION ANDINA 351 DE 1993. “REGIMEN COMUN SOBRE DERECHO DE AUTOR Y DERECHOS CONEXOS" {En línea}. Disponible en: (https://www.medellin.gov.co/irj/go/km/docs/wpccontent/Sites/Subportal%20del%20Ciudadano/Convivencia%20y%20seguridad/Secciones/Plantillas%20Gen%C3%A9ricas/Documentos/2012/Decisi%C3%B3n%20Andina%20351%20de%201993.pdf)

LEY 23 DE 1982. {En línea}. Disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3431)

[93] LEY 23 DE 1982. {En línea}. Disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3431)

[94] LEY 44 DE 1993. {En línea}. Disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3429)

[95] DECRETO 460 DE 1995. {En línea}. Disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=10576)

[96] LEY 545 de 1999. {En línea}. Disponible en: (http://www.wipo.int/wipolex/es/text.jsp?file_id=230578#LinkTarget_741)

[97] LEY 603 DE 2000. {En línea}. Disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=13960)

[98] LEY 599 de 2000 código penal colombiano. {En línea}. Disponible en: (http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000_pr010.html)

[99] UNIVERSIDAD DE CANTABRIA. "Propiedad industrial" {En línea}. Disponible en: (https://www.unican.es/unidades/idi/oficina-valorizacion/Que-es-la-Propiedad-Industrial.htm)

[100] ORGANIZACION MUNDIAL DE LA PROPIEDAD INTELECTUAL. "Ley N° 1648 de 12 de julio de 2013" {En línea}. Disponible en: (http://www.wipo.int/wipolex/es/details.jsp?id=13491)

[101]DECISIÓN 486. "Régimen Común sobre Propiedad Industrial LA COMISIÓN DE LA COMUNIDAD ANDINA." {En línea}. Disponible en: (http://www.viceinvestigacion.unal.edu.co/VRI/files/propiedad_intelectual/decision486.pdf)

[102]REDDE EMPRESARIOS VISA. "Guía Práctica para el Desarrollo de Plataformas de Comercio Electrónico" {En línea}. Disponible en: (http://www.redempresariosvisa.com/Ecommerce/Article/que-es-e-commerce-o-comercio-electronico)

[103]CERTICÁMARA. "Firma digital" {En línea}. Disponible en:

(https://web.certicamara.com/productos-y-servicios/certificados-de-firma-digital/)

[104]LEY 527 DE 1999. {En línea}. Disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276)

[105]DECRETO 1747 DE 2000. {En línea}. Disponible en:

(http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4277)

[106]RESOLUCIÓN 26930 DE 2000. {En línea}. Disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=5793)

[107]SUPERINTENDENCIA INDUSTRIA Y COMERCIO. "Sobre la protección de datos personales" {En línea}. Disponible en: (http://www.sic.gov.co/drupal/sobre-la-proteccion-de-datos-personales)

[108] LEY ESTATUTARIA 1581 DE 2012.

[109] LEY ESTATUTARIA 1266. {En línea}.Disponible en: (http://www.bancoldex.com/documentos/1291_Ley_1266_de_2008_(Habeas_Data).pdf)

[110] LEY ESTATUTARIA 1266 DE 2008. {En línea}. Disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488)

[111] LEY 1273 de 5 de enero de 2009. {En línea}. Disponible en: (http://www.informatica-juridica.com/anexos/legislacion-de-colombia-ley-1273-de-5-de-enero-de-2009-por-medio-de-la-cual-se-modifica-el-codigo-penal-se-crea-un-nuevo-bien-juridico-tutelado-denominado-quot-de-la-proteccion-de-la-informacion-y-de-los-datos-quot-y-se-preservan-integralmente-los-sistemas-q/)

LISTA DE ANEXOS

A continuación se presenta una lista donde se relacionan todos los recursos que se anexarán a este proyecto de grado, con el fin de contribuir a la visión general de los SGSI en las diferentes instituciones educativas y empresas en general, cada uno de estos formatos debe ser acondicionado según las necesidades propias y los contextos donde sean utilizados:

Anexo 1 XIV Encuesta Nacional de Seguridad Informática

Anexo 2 Plan_del_proyecto

Anexo 3 Documento_sobre_el_alcance_del_SGSI

Anexo 4 Diagnóstico Inicial

Anexo 5 Diagnostico Cuantitativo de SGSI

Anexo 6 Política_de_seguridad_de_la_información

Anexo 7 Ejemplo de Políticas de Seguridad de la Información

Anexo 8 Roles y Responsabilidades

Anexo 9 Gestión de Riegos de SGSI

Anexo 10 Toma De Conciencia y Comunicación

Anexo 11 Documentación

Anexo 13 Auditoria

Anexo 14 Revisión Por La Dirección

Anexo 15 Controles ISO27001:2013

Anexo 16 Normatividad SGSI