GESTIÓN DEL RIESGO DE SI[1] CON BASE EN LA NORMA ISO/IEC 27005:2011, ADAPTANDO LA METODOLOGÍA NIST SP 800-30. PARA EL CASO DE ESTUDIO[2] PROPUESTO.

LUIS JAVIER MORA POTOSÍ

FREDY ALEXANDER CHAVARRO FLORES

Universidad del Cauca

Facultad de Ingeniería Electrónica y Telecomunicaciones

Grupo de I+D en Tecnologías de la Información

Popayán

2016

[1] Seguridad de la información.

[2] Caso de Estudio: Procedimiento Gestión de servicios y servidores de internet de la División TIC de la Universidad del Cauca.

GESTIÓN DEL RIESGO DE SI[3] CON BASE EN LA NORMA ISO/IEC 27005:2011, ADAPTANDO LA METODOLOGÍA NIST SP 800-30. PARA EL CASO DE ESTUDIO[4] PROPUESTO.

Trabajo de Grado para optar al título de Ingeniero en Electrónica y Telecomunicaciones

LUIS JAVIER MORA POTOSÍ

FREDY ALEXANDER CHAVARRO FLORES

Director: **Esp**. **SILER AMADOR DONADO**

Universidad del Cauca

Facultad de Ingeniería Electrónica y Telecomunicaciones
Grupo de I+D en Tecnologías de la Información
Popayán
2016

[3] Seguridad de la información.
[4] Caso de Estudio: Procedimiento Gestión de servicios y servidores de internet de la División TIC de la Universidad del Cauca.

Tabla de contenido

Lista de figuras

Lista de tablas

Lista de acrónimos

DivTIC: División de tecnologías de la información y comunicaciones.

DNS: Domain name system, sistema de nombres de domino.

SIMCA: Sistema integrado de matrícula y control académico.

SSI: Servicios y servidores de internet

NIST SP: National institute of standards and technology special publications, publicaciones especiales del instituto nacional de estándares y tecnología.

OSSTMM: Open source security testing methodology manual, Manual de la metodología abierta de testeo de seguridad.

ISO: International organization for standardization, Organización internacional de normalización.

TICS: Tecnologías de la información y la comunicación.

IEC: International electrotechnical commission, comisión electrotécnica internacional.

RUP: Rational unified process, proceso de desarrollo unificado**.**

UML: Unified modeling language, lenguaje unificado de modelado.

DARCA: División de admisiones, registro y control académico.

PDCA: Plan, do, check, act (Ciclo Deming).

SGSI: Sistema de gestión de la seguridad de la información.

SI: Seguridad de la información.

TI: tecnologías de la información

COP: Coefficient of performance, coeficiente de rendimiento (signo representativo del peso Colombiano).

NIST: National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología de los Estados Unidos)

ITL (Information Technology Laboratory) Laboratorio de tecnologías de la información.

MECI: Modelo Estándar de Control Interno para el Estado Colombiano

DBA: Área de base de datos

CONPES: Consejo Nacional de Política Económica y Social

CISO: (Chief Information Security Officer) - Oficial de Seguridad

UTM: Unified Threat Management, Gestión Unificada de Amenazas

IDS: Intrusion Detection System, sistema de detección de intrusiones

IPS: Intrusion prevention system, sistema de prevención de intrusos

FACNED: Facultad de Ciencias Naturales, Exactas y de la Educación

FIET: Facultad de ingeniería electrónica y telecomunicaciones

SASIGEL: Sistema de Administración de Seguridad de la Información de Gobierno en Línea

MINTIC: Ministerio de tecnologías de la información y las comunicaciones

FEDCIRC: Federal Computer Incident Response Center Reporting a Security Incident

MVR: Metodología de valoración de riesgos

PMR: Proceso de mitigación de riesgos

MAA: Matriz de análisis de activos

INTRODUCCIÓN

La creciente demanda de tecnologías de información y redes de telecomunicaciones ha llevado a las organizaciones a automatizar sus sistemas de información para aumentar la practicidad y eficacia en los mismos, pero a medida que los activos de información se incorporan en redes tanto privadas como públicas aumenta el riesgo de que personas no autorizadas accedan a ella y puedan copiar, reproducir o modificar sus activos y de esta manera alterar el funcionamiento de la organización en aspectos financieros, económicos, comerciales o incluso afectar su prestigio, todo esto debido a que en un sistema de información a medida que va creciendo también aumentan las vulnerabilidades del mismo haciendo mayor la probabilidad de que una amenaza se materialice.

Existen varios tipos de amenazas que pueden comprometer a los activos de información, entre ellas se encuentran las que se generan por fenómenos naturales, condiciones del entorno y las causadas por mano del hombre que pueden ser intencionales o accidentales, por personas de la organización o externas. Por esta razón hoy en día ha surgido la necesidad de implementar una estrategia en las organizaciones que ayude a tomar las mejores decisiones para proteger los activos de información de una manera eficaz y con un costo aceptable de acuerdo al presupuesto y valor de los activos, para ello existen los Sistemas de Gestión de Seguridad de la Información (SGSI) que consisten en una serie de etapas aplicadas a sistemas críticos de información para mantener el riesgo en un nivel aceptable, ya que es muy difícil eliminarlo ya sea por su naturaleza o porque implica un alto costo.

El presente trabajo de grado consiste en desarrollar la fase de plan de un Sistema de Gestión de Seguridad de la Información basado en la norma NTC ISO/IEC 27001:2013 siguiendo la guía de implementación GTC ISO/IEC 27003:2012, aplicando la metodología NIST SP 800-30 para realizar la etapa de valoración de riesgos y finalmente definiendo las opciones de tratamiento de riesgos y seleccionando los objetivos de control y controles al procedimiento crítico “Gestión de Servicios y servidores de internet” el cual se lleva a cabo por el Área de Servicios y Servidores de internet en la División de Tecnologías de Información y Comunicaciones de la Universidad del Cauca. La ilustración 1, muestra la relación existente entre las normas, guía y metodologías usadas.

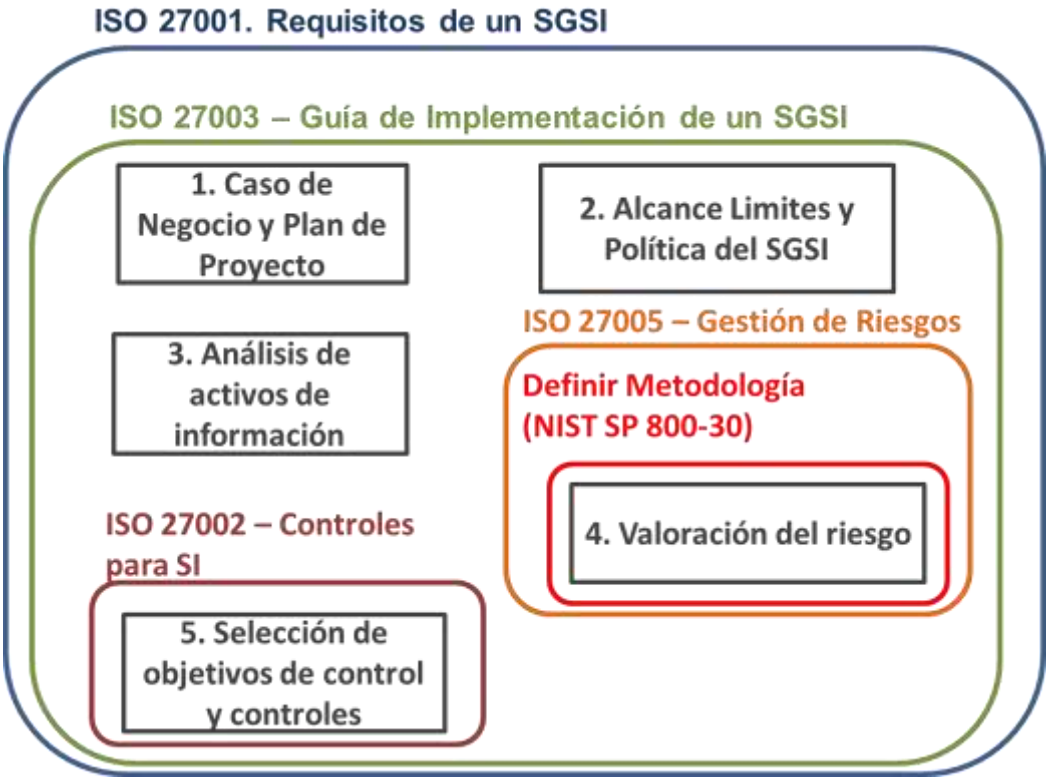

Ilustración 1 Relación de normas, guía y metodología de valoración de riesgos

Los objetivos del trabajo de grados son:

Desarrollar la fase plan de un sistema de gestión de seguridad de la información según la norma NTC-ISO/IEC 27001:2013, adaptando la metodología NIST SP800-30 para la valoración del riesgo en un entorno de servicios TIC.

Objetivos específicos:

- Desarrollar la fase plan de un SGSI, siguiendo las etapas establecidas en la GTC-ISO/IEC 27003 para el análisis y generación de políticas de seguridad de la información para el caso de estudio.

- Adaptar la metodología NIST SP 800-30[2] como mecanismo de valoración del riesgo de los activos del proceso crítico seleccionado, con base en la norma NTC-ISO/IEC 27001, siguiendo la guía de implementación ISO/IEC 27003.

- Ajustar la adaptación propuesta a partir de la aplicación de la metodología al caso de estudio.

1. MARCO TEÓRICO

1.1 NATURALEZA DE UN SGSI

La información hoy en día es un activo muy importante para las organizaciones porque cuando se gestiona adecuadamente, en ella se encuentra gran parte del éxito, pero por el contrario una mala gestión de la misma puede conducir al fracaso tanto de un negocio como de la organización en general. Según las definiciones de ISO/IEC 27000 (ISO, 2014) las tres características o propiedades fundamentales para la preservación de la seguridad de la información son:

- **Disponibilidad:** Propiedad de la información de estar disponible y utilizable cuando la requiera una entidad autorizada.

- **Confidencialidad:** Propiedad de la información de no estar disponible o no ser revelada a individuos, entidades o procesos no autorizados.

- **Integridad:** Propiedad por la cual la información debe conservarse exacta y completa.

Es necesario Gestionar el riesgo para que la información conserve las tres propiedades mencionadas, con la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) se busca primordialmente identificar los riesgos y después establecer las medidas de seguridad para reducirlos. A continuación se nombran algunos de los pasos necesarios para realizar una gestión adecuada.

- Identificación de Activos: Se pueden considerar activos a aquellos elementos que contienen información, como computadores, discos duros, memorias, documentos o personas entre otros. También se consideran activos los elementos que ayuden a que la información conserve sus tres propiedades de seguridad por ejemplo un cuarto que albergue servidores o un sistema contra incendios.

- Identificación de amenazas y vulnerabilidades:

  - Amenaza: Cualquier evento o acción que afecte a la continuidad del negocio
  - Vulnerabilidad: Es una situación que a futuro provocara una amenaza

- Calculo del nivel riesgo: Existen diferentes metodologías para cuantificar el riesgo y según esto determinar qué tan aceptable es, y posteriormente tomar las medidas pertinentes.

- Establecimiento de Controles: A los riesgos que estén por encima de lo aceptable deberá aplicárseles controles de manera planificada, estructurada y organizada puesto que implantar demasiados puede convertirse en un caos.

  - Un SGSI consta de cuatro fases basadas en el modelo PDCA o Ciclo Deming que Alberto Alexander [2] las define como:

- Establecimiento del SGSI. Las tareas principales de esta fase son determinar el alcance del SGSI, identificar los activos de información y tasarlos, análisis y evaluación del riesgo y por último se determinan las opciones de tratamiento de riesgo.

- Implementación del SGSI. Se debe elaborar el plan de tratamiento del riesgo, detallando las acciones que deben emprenderse para implantar las opciones del tratamiento del riesgo escogidas.
- Monitoreo y Revisión. La empresa debe tener los procedimientos y rutinas establecidas, para con ayuda de métrica, revisar el desempeño del SGSI.
- Mejora continua. Se deben tomar las acciones pertinentes para reaccionar a incidentes y tomar también las acciones preventivas de lugar. La idea consiste en llevar el SGSI a la excelencia.

1.2 CONCEPTOS GENERALES DE LA NORMA ISO27001

La norma internacional ISO/IEC 27001 fue emitida por la organización internacional de normalización (ISO) y la comisión electrotécnica internacional (IEC) en octubre de 2005. Es un estándar que establece un sistema de gestión de seguridad de la información haciendo énfasis en la gestión de los riegos. La versión más reciente es la publicada en 2013 ISO/IEC 27001:2013 (information technology – security techniques – information security management systems - requirements) [3]

La norma establece los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un SGSI, esta puede ser implementada en cualquier tipo de organización y se espera que con el paso del tiempo factores como tamaño de la organización, necesidades, objetivos, procesos y requisitos de seguridad cambien sin afectar el funcionamiento del SGSI.

Las organizaciones pueden lograr la certificación en la norma demostrando a nivel internacional que los riesgos son gestionados adecuadamente y los activos mantienen al máximo las tres dimensiones de seguridad: confidencialidad, integridad y disponibilidad.

La serie ISO/IEC 27000 contiene varios documentos algunos de ellos con adopciones en cada país como es el caso de Colombia, donde el instituto colombiano de normas técnicas y certificación, ICONTEC fue el organismo encargado de la revisión, traducción y publicación. A continuación se nombran algunos de los documentos más relevantes de la serie para este trabajo de grado.

ISO/IEC 27000:2014: Glosario con vocabulario usado en la norma y en general en la seguridad de la información.

NTC ISO/IEC 27001:2013: Norma Técnica Colombiana (NTC), especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI. También incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información a la medida de las necesidades de la organización. Los requisitos establecidos en la norma son genéricos y se pretende que sean aplicables a todas las organizaciones, sin importar su tipo, tamaño o naturaleza.

ISO/IEC 27002:2013: Guía de buenas prácticas e implantación de controles.

GTC ISO/IEC 27003:2012: Guía Técnica Colombiana (GTC). Guía para un buen diseño e implantación de un sistema de gestión de seguridad de la información.

En él se describe el proceso de especificación y diseño de un SGSI desde su inicio hasta la producción de los planes de ejecución. Además, se describe el proceso de obtener la aprobación de la gerencia para implementar el SGSI y proporciona orientación sobre cómo planificar el proyecto.

ISO/IEC 27004:2009: Proporciona herramientas para la medición de la seguridad de la información como resultado de un SGSI, especificando los parámetros a medir y ayudando a generar objetivos de rendimiento y criterios de éxito.

ISO/IEC 27005:2011: Gestión de riesgos de la seguridad de la información, metodología para efectuar el tratamiento, admisión y comunicación del riego.

ISO/IEC 27006:2011: Especifica requisitos contenidos en la norma ISO/IEC 17021 e ISO/IEC 27001 y proporciona una guía de auditoria y certificación de un SGSI, busca apoyar la acreditación de organismos de certificación.

ISO/IEC 27011:2008: Es una recomendación que define directrices que fomentan la aplicación de la gestión de seguridad de la información en las organizaciones de telecomunicaciones específicamente.

ISO tiene una numeración reservada que va desde 27000 hasta 27019 y de 27030 a 27044, donde es posible encontrar documentos y guías de ayuda para la aplicación de un SGSI en sectores en específico o para entidades de auditoria o certificación. [4]

Dentro de las múltiples ventajas que una empresa puede obtener con la certificación ISO 27001, el centro de consulta online Advisera [5] destaca:

Cumplimiento con requerimientos legales: Son cada vez más los países que emiten nuevas normas, leyes y requerimientos en torno a la seguridad de la información, la implementación de ISO 27001 proporciona las herramientas para cumplir ese tipo de exigencias.

Obtener una ventaja comercial: El obtener la certificación provee una ventaja frente a las empresas competidoras, ya que a los clientes les interesa mantener en forma segura su información.

Menores costos: El hecho de sufrir accidentes grandes o pequeños se traduce en pérdida de dinero, el implementar un SGSI evita que se produzcan incidentes de seguridad.

Una mejor organización: Es muy común en las empresas tener mal definidos sus procesos y procedimientos resultando confusiones respecto a las funciones de cada empleado, sus obligaciones y responsabilidades. En el desarrollo de un SGSI se soluciona este problema aumentando la productividad de todos en la empresa.

La implantación de un SGSI consta de cuatro fases basadas en el ciclo DEMING o modelo PDCA (plan, do, check, act), este es un modelo enfocado a la mejora continua, para adaptarse a los cambios dentro de la organización y ser eficiente por largos periodos de tiempo.

En la primera fase, la de plan, se determina el alcance del modelo en la empresa, se deben identificar los activos de información y tasarlos, luego hacer el análisis y evaluación del riesgo y determinar que activos de información están sujetos a riesgos. Seguidamente, se deben determinar las opciones para el tratamiento del riesgo [2]. En la segunda fase se llevan a cabo las acciones que deben emprenderse para implantar las opciones de tratamiento del riesgo escogidas. En la tercera fase se revisa y evalúa el desempeño del SGSI. Finalmente, en la cuarta fase se toman las acciones pertinentes para mejorar el SGSI basándose en las fallas encontradas durante la fase tres.

En la Figura 1.1 [6] se muestra con detalle el modelo PDCA enmarcado en la norma ISO/IEC 27001 [7].

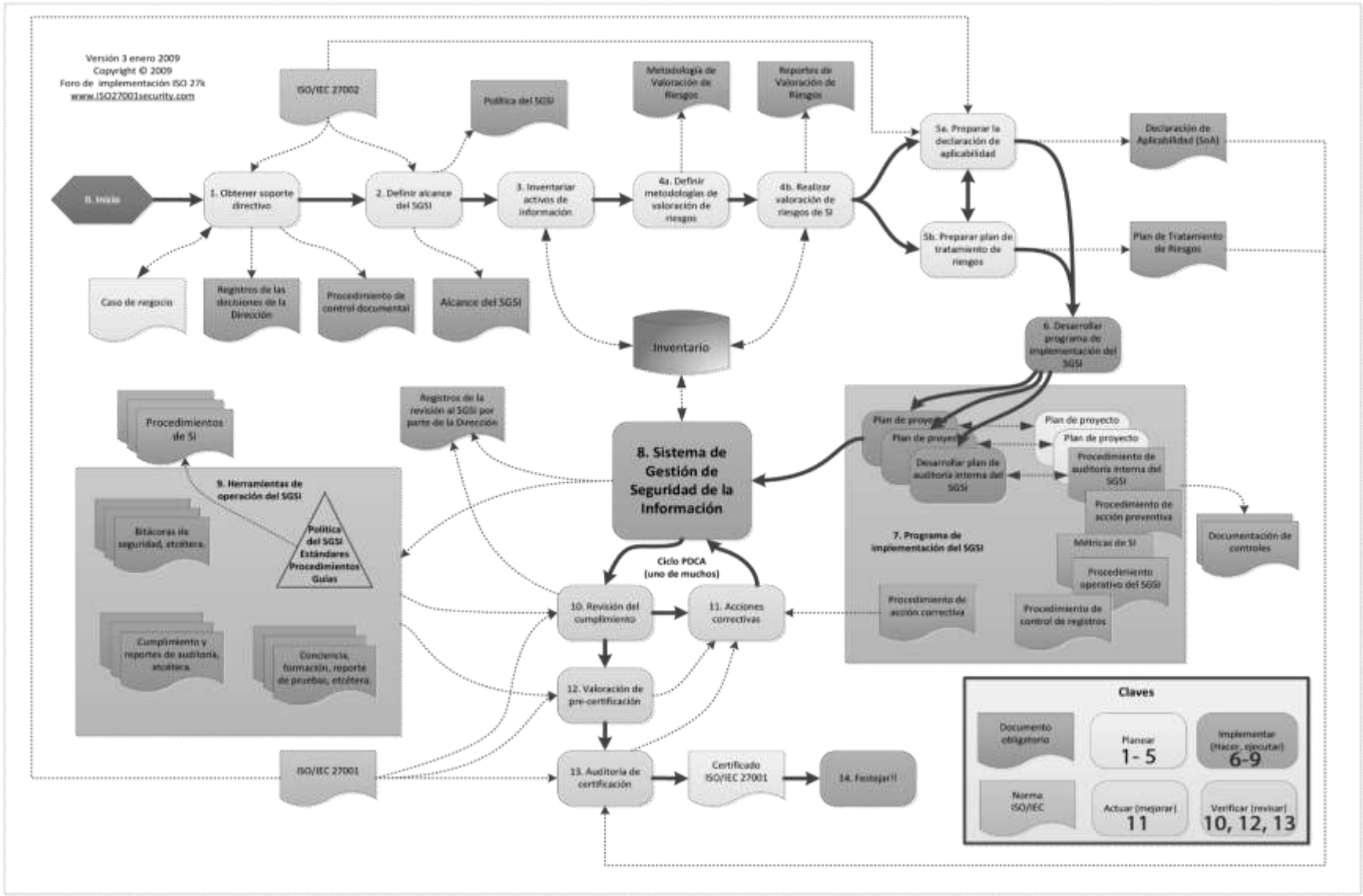

Figura 1-1 Modelo PDCA – ISO 27001

1.3 ALCANCE Y LÍMITES DE UN SGSI

Cada organización tiene una situación particular pues existen variables que las hacen diferentes, como el número de empleados, el número de clientes, tipo de negocio, volumen de información, oficinas, activos físicos y lógicos, entre otros, esto significa que cada una de ellas deberá tener su propio modelo de SGSI. Una etapa es definir que partes, procedimientos o activos de la organización serán incluidas en la gestión y documentar las razones de aquellas partes que se no incluirán.

El estándar ISO/IEC 27001:2005 en la cláusula 4.2.1 sugiere lo siguiente "Definir el alcance y los límites del SGSI en términos de las características del negocio, la organización, su ubicación, activos, tecnología e incluyendo los detalles de y la justificación de cualquier exclusión del alcance".

El alcance y límites ayudan también a priorizar las áreas de la organización que necesitan la implantación del SGSI como primera medida, siendo estas las que por sus funciones y responsabilidades permiten cumplir con la misión institucional, posteriormente se determinara si es necesario que otras áreas entren en el SGSI y se hará progresivamente de acuerdo a las necesidades.

Según la guía técnica colombiana GTC ISO/IEC 27003:2012 [8] para definir el alcance y límites del SGSI se debe tener en cuenta tres tipos de activos que se describen a continuación:

- De la organización: Hace referencia al personal, misión, visión, documentos
- De las TIC's: Recursos tecnológicos que contengan información como sistemas informáticos, servidores, redes de comunicaciones
- Físicos: Hace referencia a las locaciones físicas de la organización como oficinas, cuartos de comunicaciones, almacenes de recursos, sistemas contra incendios, aire acondicionado.

Después de identificar y clasificar los activos se procede a seleccionar los que son críticos y que deben hacer parte del SGSI, los que no se consideran críticos se dejan por fuera de la gestión pero se hace un documento que contiene la razón por la que no se incluyó dentro del alcance y límites del SGSI.

Alexander [2] propone el método de las elipses como herramienta para definir de forma clara y concreta el alcance y límites del SGSI. Este método consiste en formar tres elipses concéntricas, en la elipse interna estará el procedimiento, área o sistema al que se pretende gestionar la seguridad de la información. En la elipse del medio se encuentran las áreas, procedimientos, personas o sistemas que pertenecen a la organización y que se relacionan con el procedimiento de interés y por último en la elipse externa se ubican las relaciones extrínsecas a la organización con el caso de estudio. En la figura 1.2 se ilustra lo anterior.

Figura 1-2 Método de las elipses para definir el alcance y límites del SGSI

En cada relación que exista entre la elipse central y otro elemento del diagrama se debe identificar los activos que hacen parte de dicha relación. Finalmente se seleccionan los activos que son de carácter crítico para incluirlos en el SGSI y documentar las razones de los que no se incluyen, con esto se logra lo exigido en el estándar como Definición de Alcance y Limites del SGSI.

1.4 POLÍTICA DE UN SGSI

Por medio de la política se busca dar un apoyo y lineamientos a la dirección para tomar decisiones respecto a la seguridad de la información. Esta política debe ir de acuerdo a la legislación vigente y a las necesidades propias de cada organización.

Según el instituto nacional de tecnologías de ciberseguridad [9] El documento debe delimitar que se tiene que proteger, de quien y por qué. Debe explicar que es lo que está permitido y que 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.

La política de seguridad debe ser de dominio público y estar disponible en todo momento; además debe ser clara, concisa y redactada en un lenguaje sencillo. Esta define como actuar en caso de accidentes y las responsabilidades de cada uno de los cargos dentro de la organización.

El documento con las políticas debe ser revisado y aprobado por la dirección antes de su publicación.

1.5 ANÁLISIS Y EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN

Siguiendo la guía GTC ISO/IEC 27003, el alcance y límites del SGSI y la política de seguridad de la información obtenida en los puntos anteriores son necesarios para continuar con la siguiente etapa que en la guía tiene el nombre *"Realizar análisis de los requisitos de seguridad de la información",* esta consiste inicialmente en identificar y clasificar los requisitos de seguridad que la organización necesita, enfocados siempre en la misión, visión y continuidad del negocio. Los requisitos de seguridad pueden ser internos es decir aquellos que permiten lograr los objetivos de la organización y los externos que son los que se

exigen por normas legales, reglamentaciones, contratos con clientes, acuerdos con proveedores o condiciones de pólizas de seguro.

Inicialmente se hace una recopilación de información de apoyo sobre las actividades, tareas, responsabilidades, etc., necesarias para realizar un resumen acerca del procedimiento y las aplicaciones y sistemas TIC relacionados.

La siguiente actividad va encaminada a clasificar los activos dentro del alcance y conocer si existen controles o políticas sobre ellos para de esta forma tener una visión del estado actual de seguridad de la información en la organización. En esta etapa se tienen en cuenta términos como:

- **Riesgo:** Es el grado o estimación de que una amenaza se materialice sobre un activo y que produzca daños a la organización.

- **Amenaza:** Evento que al llevarse a cabo produce daños de carácter material o inmaterial a los activos.

- **Vulnerabilidad:** Debilidad que tienen los activos frente a las amenazas.

- **Impacto:** Consecuencia que deja una amenaza materializada sobre un activo.

- **Riego residual:** A pesar de que se gestione la seguridad de la información y se apliquen controles y otras medidas necesarias, siempre existe riesgo al que se le llama residual porque la organización deberá asumir y vigilar

Es necesario hacer un inventario de riesgos, en caso de que este inventario sea muy extenso solo se tendrá en cuenta los riesgos de los activos más críticos, en él se identificaran las amenazas y se analizará el impacto en el caso de que se materialicen. Posteriormente se hará un análisis de las vulnerabilidades de los activos. Una vez identificadas las amenazas y vulnerabilidades se procede a aplicar salvaguardas o controles para mitigar el riesgo.

El resultado del análisis anterior es conocer el nivel de riesgo de la organización el cual debe quedar perfectamente documentado para justificar las medidas que se van a aplicar. Hasta esta etapa se ha logrado identificar y evaluar el riesgo sobre

los activos y el impacto en caso de que se presente algún incidente, también conocer el riesgo residual.

1.6 VALORACIÓN DEL RIESGO

La valoración del riesgo es parte esencial para el desarrollo y operación de un SGSI, en esta etapa se valora la criticidad de cada activo, se identifican las amenazas y su probabilidad de ocurrencia además se determinan las vulnerabilidades de la organización, que podrían ser explotadas en cualquier momento. La norma ISO/IEC 27001 da libertad para escoger la metodología de gestión del riesgo que más se ajuste a las características de la organización. En este caso la metodología seleccionada es NIST SP 800-30, que además concuerda con la metodología del programa Agenda de conectividad, estrategia de gobierno en línea de la Republica de Colombia. [10]

El Instituto Nacional de Estándares y Tecnología de los Estados Unidos conocido por sus siglas en inglés como NIST, es una agencia federal fundada en 1901 para la administración de tecnología del departamento de comercio de los Estados Unidos. Existen varias publicaciones como guías técnicas, estándares y normas en el ámbito tecnológico. Las publicaciones de la serie 800 incluyen informes sobre investigaciones llevadas a cabo por el ITL (Information Technology Laboratory) y documentos guía para la divulgación de temas acerca de la seguridad de la información para ser aplicadas en la industria, el gobierno y organizaciones académicas.

La publicación especial NIST SP 800-30 [11] es una guía para realizar gestión de riesgo en sistemas de información. Esta presenta un proceso basado en tres etapas fundamentales que son la preparación de la evaluación, realización de la evaluación y finalmente el mantenimiento, este proceso se lleva a cabo en 2 grandes pasos, metodología de valoración de riesgos y proceso de mitigación de riesgos.

El objetivo principal de NIST SP 800-30 es permitir que la organización por medio de la gestión de riesgos, lleve el riesgo a un nivel aceptable aplicando medidas y controles. Para logarlo se tratan tres puntos específicos.

1. Mejorar la seguridad de los sistemas de información que almacenan, procesan o transmiten información de la organización.
2. Realizar la gestión de tal forma que las decisiones que se tomen en ella puedan ser justificadas dentro del presupuesto del sistema de información.
3. Mejorar la administración de los sistemas de información basados en los documentos de soporte resultantes de la ejecución de la gestión de riesgos.

La metodología de valoración de riesgos de divide en nueve pasos que se nombran a continuación, cabe resaltar que esta descripción es tomada del documento oficial de la publicación especial NIST SP 800-30 [12].

Paso 1: *Caracterización del sistema*

Consiste en tener una visión global del sistema de información. Para ello se debe identificar el alcance del sistema, sus límites, los recursos que lo constituyen y el personal responsable relacionado con cada elemento. En este paso la guía tiene dos secciones, la primera muestra que tipo de activos son relevantes para tener en cuenta en la caracterización, y la segunda describe algunas técnicas para recopilación de información como encuestas, entrevistas o aplicaciones informáticas que ayudan en la obtención de información pertinente.

Paso 2: Identificación de amenazas

Una amenaza es un evento potencialmente no deseado cuya ocurrencia causaría daños materiales o inmateriales a la organización o a sus activos. Los sistemas de información tienen debilidades que se conocen como vulnerabilidades. Bajo estos conceptos se deben identificar las amenazas teniendo en cuenta que aquellas que no tienen una vulnerabilidad particular para ejercer efecto, no representan riesgo.

La meta de este paso es identificar y clasificar amenazas y fuentes de amenazas presentes en el sistema de TI a evaluar. Las fuentes comunes de amenazas son: naturales, humanas, tecnológicas, operacionales entre otras.

Paso 3: Identificación de vulnerabilidades

Una vulnerabilidad es un defecto o debilidad en los procedimientos de seguridad, diseño, implementación o en los controles internos del sistema que podrían ser

explotadas (activadas accidentalmente o explotadas intencionalmente) y que resulta en una brecha de seguridad o violación de las políticas de seguridad. [19]

Es necesario hacer un análisis de las debilidades o defectos del sistema que pueden ser explotadas por las amenazas. Como resultado de este paso se debe elaborar una tabla descriptiva de las vulnerabilidades.

Para hacer una mejor identificación se recomienda analizar las fuentes de vulnerabilidades. Cabe señalar que los tipos de vulnerabilidades y la metodología para determinar si estas están presentes, depende de la naturaleza de cada sistema de información y la fase en la que se encuentra, es decir si el sistema está en fase de diseño, implementación u operación.

Paso 4: Análisis de controles

Es necesario hacer un análisis sobre los controles de seguridad que existen actualmente en la organización, esto con el fin de determinar cuáles de ellos son adecuados para continuar siendo controles en la nueva gestión de riesgos. Es importante identificar y clasificar los controles existentes

Paso 5: Determinación de probabilidad

Se debe obtener una medida de la probabilidad de que una amenaza logre explotar una vulnerabilidad específica. Para el desarrollo de este paso es necesario utilizar los resultados obtenidos en el paso 2 y paso 3.

Para desarrollar esta actividad se debe tener en cuenta lo siguiente:

- Fuente de la amenaza y su capacidad.
- Naturaleza de. la vulnerabilidad
- Controles actuales y eficacia de los mismos.

Paso 6: Análisis de impacto

Un paso importante para medir el nivel de riesgo es determinar las posibles consecuencias que puede dejar el hecho de que una amenaza explote exitosamente una vulnerabilidad, esto se conoce como impacto. Para hacer el análisis de impacto se debe contar con la siguiente información:

- Misión del sistema: Procesos realizados por el sistema informático

- Criticidad del sistema y los datos: Se tiene en cuenta el valor o importancia del sistema dentro de la organización.

- Sensibilidad del sistema y los datos.

Un evento que atenta contra la seguridad de la información podría afectar en uno o varios de los tres objetivos de seguridad, disponibilidad, integridad o confidencialidad. A continuación se describen brevemente los tres objetivos de seguridad y el impacto que se genera al no ser cumplidos.

- **Pérdida de Integridad:** la integridad del sistema y los datos se refiere al requerimiento de la información de ser protegida ante modificaciones inapropiadas o no autorizadas tanto de forma intencional como accidental. existe la posibilidad de que la información se continúe usando después de haber sido violada su integridad y que la organización no pueda notarlo. Esto puede ocasionar inexactitud en los procesos o procedimientos de la organización, fraudes o tomar decisiones equivocas. La pérdida de integridad puede afectar además a la disponibilidad y confidencialidad.

- **Pérdida de disponibilidad:** Si un sistema de misión crítica no está disponible para sus usuarios finales, se afecta el logro de la misión de la entidad. La pérdida de funcionalidad y degradación de las operaciones, conlleva entre otros a la pérdida de productividad, sanciones legales y parálisis de la cadena de abastecimiento afectando tanto a los usuarios internos como a los clientes.

- **Pérdida de confidencialidad:** La confidencialidad de los datos y sistemas se refiere a la protección contra divulgación no autorizada. El impacto de una divulgación no autorizada puede poner en peligro a la organización y a todas las entidades asociadas a ella. La pérdida de confidencialidad, anticipada o no intencional puede conducir a acciones legales contra la organización.

Paso 7: Determinación del riesgo

El propósito de este paso es evaluar el nivel de riesgo para el sistema de TI. La determinación del nivel de riesgo de una amenaza o vulnerabilidad en particular, se expresa en función de:

- La probabilidad de que una fuente de amenaza determinada intente explotar una vulnerabilidad.

- La magnitud de impacto en caso de que una amenaza recaiga sobre una vulnerabilidad, teniendo en cuenta la criticidad de los activos afectados.

- La idoneidad de los controles de seguridad previstos o existentes para reducir o eliminar el riesgo.

Para medir el riesgo, se debe desarrollar una escala de riesgo y una matriz de nivel de riesgo. A continuación se presenta una matriz estándar de nivel de riesgo y más adelante se describen los niveles de riesgo resultantes.

Paso 8: Recomendaciones de control

Durante este paso del proceso se proporcionan los controles apropiados para mitigar o eliminar los riesgos identificados tratando de no alterar las operaciones organizacionales. El objetivo de las recomendaciones de control es reducir el nivel de riesgo para el sistema de tecnologías de información a un nivel aceptable.

Los siguientes factores deben ser considerados en la recomendación de controles y soluciones alternativas para minimizar o eliminar los riesgos identificados:

• Eficacia de las opciones recomendadas (por ejemplo, la compatibilidad del sistema)

• Legislación y reglamentación

• Política Organizacional

• Impacto Operacional

• Seguridad y fiabilidad.

Las recomendaciones de control son los resultados del análisis y evaluación de riesgos y proporcionan la base para el proceso de mitigación de riesgos, en el que los controles recomendados técnicos y administrativos son evaluados, priorizados e implementados.

Cabe señalar que no todos los controles recomendados se pueden implementar, por lo que es necesario hacer un análisis para determinar cuáles son apropiados en la organización.

Aspectos como el impacto operativo (por ejemplo, afecciones al rendimiento del sistema) y la factibilidad de introducir la opción recomendada (por ejemplo, los requisitos técnicos, la aceptación del usuario), son puntos que se deben tener en cuenta durante el proceso de mitigación de riesgos.

Paso 9: Documentación de resultados

Una vez que se ha completado la evaluación de riesgos (fuentes de amenaza y vulnerabilidades identificadas, riesgos evaluados y la recomendación de controles) los resultados deben ser documentados en un informe oficial o sesión informativa.

Un informe de evaluación de riesgos es un reporte de gestión que ayuda a la alta dirección a tomar decisiones sobre políticas, procedimientos, presupuesto o cambios en el sistema de gestión y operaciones.

A diferencia de un informe de auditoría, que busca irregularidades, un informe de evaluación de riesgos no debe ser presentado de manera acusatoria, sino con un enfoque sistemático y analítico para la evaluación de riesgos, de manera que la alta dirección va a entender los riesgos y asignar recursos para reducir y corregir pérdidas potenciales. Por esta razón, algunos prefieren enfocar las amenazas / vulnerabilidades como observaciones en lugar de hallazgos.

1.7 TRATAMIENTO DEL RIESGO

En la etapa anterior se realizó el análisis y evaluación del riesgo lo cual nos da respuesta a la pregunta ¿Qué riesgos enfrentamos y cuál es su impacto en la organización?, ahora el paso siguiente es tomar las medidas más apropiadas para controlar, minimizar o eliminar esos riesgos y dar respuesta a otra pregunta ¿Cómo enfrentamos los riesgos?, para ello existen cuatro opciones de tratamiento de riesgos descritas por INTECO [13] como:

- **Eliminar el riesgo:** Esto se consigue eliminando los activos a los que este riesgo está asociado. Se trata de una elección generalmente costosa y drástica por lo que suelen buscarse medidas alternativas.

- **Transferir el riesgo:** Consiste en hacer un acuerdo o subcontratación con una entidad externa para que asuma las responsabilidades en caso de que una amenaza se materialice, o adquirir una póliza para que la aseguradora cubra los gastos en caso de que ocurra un incidente.

  - Para elegir esta opción hay que analizar su viabilidad, se debe tener en cuenta que no se pueden trasferir activos altamente confidenciales o en el caso de adquirir un seguro verificar que su valor no sea superior al del propio activo. Dependiendo del tipo de activo deberá realizarse el análisis correspondiente para determinar si es viable o no transferir el riesgo.

- **Asumir el riesgo:** Implica que la organización no va a tomar medidas de protección adicionales contra dicho riesgo pero lo vigilará para que no aumente, además debe satisfacer la Política de Seguridad de la Información, para que mantenga un nivel de riesgo bajo. Esta decisión deberá ser tomada y aprobada por la dirección de la organización.

  Mitigar el Riesgo: Se trata de implantar medidas que protejan a los activos. Cada medida aplicada debe ser documentada y gestionada por la organización.

1.8 DECLARACIÓN DE APLICABILIDAD

La declaración de aplicabilidad SOA (Statement of Applicability) es un documento que define los controles que debe implementar una organización para el tratamiento de sus riesgos. Estos controles, son una selección del anexo A de la norma ISO/IEC 27001, además es posible incluir controles y objetivos de control que no estén enlistados en la norma.

La SOA se desarrolla después de la etapa del tratamiento de riesgos, donde se definen las acciones para mitigar, transferir o aceptar el riego existente, es en ese punto donde se precisan las medidas de seguridad que estarán plasmadas en el SOA, en el documento además se especifica si estas medidas están o no siendo aplicadas.

La declaración de aplicabilidad es un documento de suma importancia ya que es obligatorio para la certificación en ISO/IEC 27001, este será consultado en las auditorias del SGSI para conocer los controles de seguridad que están siendo aplicados para proteger los activos. Además brinda organización y claridad en la gestión de la seguridad.

2. MODELO DE ADAPTACIÓN

Para obtener los resultados correspondientes a la etapa de Valoración de riesgos de la fase de plan del SGSI se propone una adaptación de la Guía de Gestión de Riesgos NIST SP 800-30, la cual se realizó con el fin de evitar redundancia con actividades o resultados obtenidos anteriormente y buscando en todo caso cumplir con los requisitos exigidos por la Norma ISO/IEC 27001:2013 lo cual es necesario para lograr una certificación.

Como se explicó anteriormente en el Capítulo 1, la Guía de Gestión de Riesgos NIST SP 800-30 tiene dos partes principales la MVR y el PMR.

Debido a que el objetivo es desarrollar la fase de plan de un SGSI, se determinó que es conveniente omitir el PMR puesto que esta mayormente enfocado a la implementación de controles para mitigación de riesgos como se describe en la sección 4 de la Guía de Gestión de Riesgos NIST SP 800-30, lo cual corresponde con la fase de ejecución de un SGSI según la definición de Alberto Alexander en su libro Diseño de un Sistema de Gestión de Seguridad de la Información.

Fase de Plan. "*La norma da las pautas para determinar el alcance del modelo de la empresa, identificar los activos de información y tasarlos, luego hacer el análisis y la evaluación del riesgo y determinar que activos de información están sujetos a riesgo. Seguidamente en esta fase se deben determinar las opciones para el tratamiento del riesgo*". Fase de Ejecución. "*En la segunda fase del ciclo Deming, la llamada Implementación del SGSI, se debe elaborar el plan de tratamiento de riesgos, detallando las acciones que deben emprenderse para implantar las opciones de tratamiento del riesgo escogidas*"

En cuanto a la MVR se observa que algunos pasos ayudan a alcanzar ciertos requisitos de un SGSI como se observa en la siguiente tabla:

Ítem	Requisitos para la valoración de riesgos según ISO/IEC 27001:2013	Cumplimiento del requisito con la metodología de valoración de riesgos de NIST SP 800-30
6.1.2 - c	Identifique los riesgos de la seguridad de la información: 1. Identificar los riesgos asociados con la perdida de confidencialidad, integridad y disponibilidad de información dentro del alcance del SGSI 2. Identificar a los dueños de los riesgos	En el paso 2 y 3 de la metodología se identifican los riesgos.
6.1.2 - d	Analice los riesgos de la seguridad de la información 1. Valorar las consecuencias potenciales que resultaran si se materializaran los riesgos identificados en 6.1.2 - c - 1 2. Valorar la probabilidad realista de que ocurran los riesgos identificados en 6.1.2 - c – 1 3. Determinar los niveles de riesgo	En el paso 6 valora el impacto negativo resultante de que una amenaza se materialice. En el paso 5 se valora la probabilidad de ocurrencia de amenazas En el paso 7 se determina el nivel de riesgo.

Tabla 2-1 Cumplimiento de requisitos de la norma aplicando la MVR

Para realizar la adaptación se debe tener claro que se está trabajando con dos marcos de referencia, la Norma y la MVR, por lo que es necesario hacer una comparación e integración de las diferentes etapas y pasos, para tal fin se usó el "Método de integración para soportar la armonización de múltiples modelos y estándares" [15]. Siguiendo el método mencionado se define los términos para aplicarlo de la siguiente forma.

Marco A: Fase de Plan de un SGSI basado en la norma ISO/IEC 27001:2013

Marco B: MVR

EP (Elemento de Proceso) del marco A: Etapas (5) del Marco A

EP (Elemento de Proceso) del marco B: Pasos (9) del Marco B

EPSI (Elementos de Proceso Sensibles a ser Integrados): Todos los EP de los marcos de referencia son EPSI.

Como criterios de integración se usaron los definidos por el autor, puesto que en este caso se presenta que un marco de referencia absorbe al otro en algunos EP por su nivel más avanzado de detalle. Los criterios son los siguientes:

Criterios de Integración:

"*Cuando la descripción de un EPSI definido en un marco A está soportado y contenido en la descripción de un EPSI definido en un marco B:*

i). Cuando el EPSI del marco A ofrece una descripción más detallada que el EPSI del marco B, el EPSI de B podría ser absorbido por el EPSI de A.

ii). Cuando el EPSI del marco A ofrece una descripción igual (en detalle) que la descripción del EPSI del marco B, el EPSI de B podría ser absorbido por el EPSI de A o viceversa.

iii).Cuando el EPSI del marco A ofrece una descripción con menos detalle que el EPSI del marco B, el EPSI de A podría ser absorbido por el EPSI de B"

A continuación se muestra en la tabla 2-2 Relación de EPSI de los marcos de referencia, las relaciones entre los EPSI de los marcos de referencia, seguidamente se aplicara el proceso definido en el método de acuerdo a su ilustración [15], Figura 2-1. Proceso de comparación e integración y de acuerdo a los criterios de integración definidos anteriormente.

Relación	EPSI Marco A	EPSI Marco B
1	• Caso de negocio y Plan de Proyecto. • Alcance, Limites y Política del SGSI	• Paso 1
2	• Análisis de activos de información	• Paso 6
3	• Valoración de Riesgos	• Paso 2 • Paso 3 • Paso 4 • Paso 5 • Paso 7
4	• Selección de objetivos de control y controles	• Paso 8
5	• Entregables	• Paso 9

Tabla 2-2 Relación de EPSI de los marcos de referencia

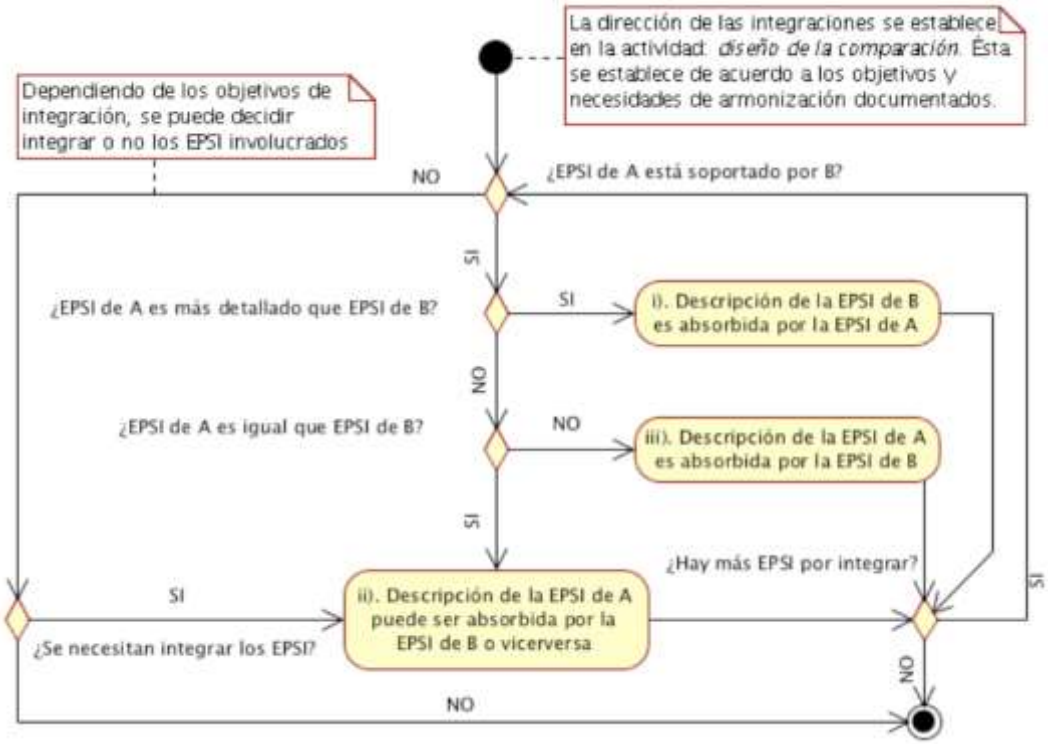

Figura 2-1 Proceso de comparación e integración

Para definir sin el EP de un marco es más detallado que el EP del otro marco, se usó la siguiente documentación.

- Para EP del Marco A: Norma ISO/IEC 27001:2013 y Guía Técnica ISO/IEC 27003:2012
- Para EP del Marco B: Guía de Gestión de Riesgos NIST SP 800-30

Después de realizar el proceso para cada una de las relaciones definidas en la Tabla 2-2 Relación de EPSI de los marcos de referencia, se obtuvo el resultado mostrado en la tabla 2-3. Integración de Marcos de Referencia.

EPSI Relacionados		**EP a usar según criterios de integración**	**Documentación de soporte**
Macro A	**Marco B**		
Caso de negocio y Plan de Proyecto.	Paso 1	Caso de negocio y Plan de Proyecto.	Numeral 4.1 a 4.3 de la norma ISO/IEC 27001:2013
Alcance, Limites y Política del SGSI		Alcance, Limites y Política del SGSI	Numeral 5 y 6 de la GTC ISO/IEC 27003:20112
Análisis de activos de información	Paso 6	Análisis de activos de información	Numeral 7.3 de la GTC ISO/IEC 27003:2012
Valoración de Riesgos	Paso 2	Paso 2	Paso 2 de la MVR
	Paso 3	Paso 3	Paso 3 de la MVR
	Paso 4	Paso 4	Paso 4 de la MVR
	Paso 5	Paso 5	Paso 5 de la MVR
	Paso 7	Paso 7	Paso 7 de la MVR
Selección de objetivos de control y controles	Paso 8	Selección de objetivos de control y controles	Numeral 6.1.2 de la norma ISO/IEC 27001:2013
			Numeral 8.3 de la GTC ISO/IEC 27003:2012
Información Documentada	Paso 9	Información Documentada	Numeral 7.5 de la norma ISO/IEC 27001:2013

Tabla 2-3Integración de Marcos de Referencia.

Con los resultados obtenidos se determina cuáles son los EP a usar en la adaptación de la MVR, pero es necesario analizarlos para implementar algunas mejoras, para ello se hizo un análisis de las recomendaciones de cada paso de la MVR y también a partir de experiencias adquiridas en el presente trabajo se propone las siguientes adaptaciones adicionales.

Paso de la MVR	Descripción	Adaptaciones adicionales	Justificación
Paso 4. Análisis de Controles. Tabla 3-3. Criterios de seguridad	La MVR recomienda usar la tabla 3-3. Criterios de seguridad como una lista de chequeo en el paso 3 para identificar vulnerabilidades	Tomando como base la tabla 3-3. Criterios de Seguridad de la MVR, se creó la tabla 3-14, a la cual se le agrego una columna para buscar a cada medida de seguridad implementada en la organización un control equivalente del estándar ISO/IEC 27002	La tabla en mención tiene varios criterios de seguridad que facilitan la identificación de controles en una entrevista y en revisión de información otorgada por la organización
Paso 5. Determinación de la Probabilidad. Tabla 3-4 Definición de Probabilidades	La MVR recomienda valorar como alto medio o bajo la probabilidad de ocurrencia teniendo en cuenta la capacidad de la fuente de amenaza para hacer daño al sistema y al mismo tiempo la efectividad de controles o medidas de seguridad implantadas.	Usar el mecanismo usado en el Risk Assessment Instructions de Virginia Information Technologies Agency (VITA) en el cual se hace la valoración de la probabilidad de ocurrencia de un amenaza valorando de forma separada la capacidad de la fuente de amenaza para hacer daño al sistema y la efectividad de los controles o medidas de seguridad implantados y finalmente haciendo un cruce de las valoraciones obtenidas usando la tabla 3.17 propuesta por VITA. Recomendamos que los criterios de valoración se diseñen de acuerdo a la información existente en la organización mas adelante en el capítulo de ajuste se muestra los criterios creados para este caso.	En este paso se debe hacer entrevistas al personal de la organización para obtener una valoración y las preguntas son más concretas y menos complejas si se hacen de forma separada las concernientes a capacidad de la fuente de amenaza y efectividad de controles, además es posible que la organización tenga registros de efectividad de controles sin tener en cuenta la capacidad de la fuente de amenaza o viceversa

Paso 6. Análisis de Impacto	La MVR recomienda valorar la perdida de disponibilidad, integridad y confidencialidad para medir la magnitud del impacto	Se usará la criticidad de activos obtenida en la etapa de Análisis de activos. Para determinar el impacto se debe relacionar cada amenaza con los activos a los que afecta. Se propone hacer un promedio de las criticidades de los activos relacionados a cada amenaza para determinar la magnitud del impacto de cada amenaza en caso de que se materialice.	El promedio de las criticidades de los activos relacionados a una amenaza permite seguir trabajando con el mismo número de datos con el que se venía trabajando en los pasos anteriores, esto debido a que existe la posibilidad de que una amenaza afecte a varios activos al mismo tiempo y aumenta el volumen de las tablas y el trabajo se torna más complejo y confuso.

Tabla 2-4 Adaptaciones Adicionales

Finalmente se muestra en la Figura 2-2. Adaptación de la Metodología de Valoración de Riesgos el proceso completo para realizar la adaptación que se propone en este trabajo con el respectivo orden secuencial, los documentos que se tendrán en cuenta debido a su buen nivel de detalle y adaptaciones adicionales de mejora.

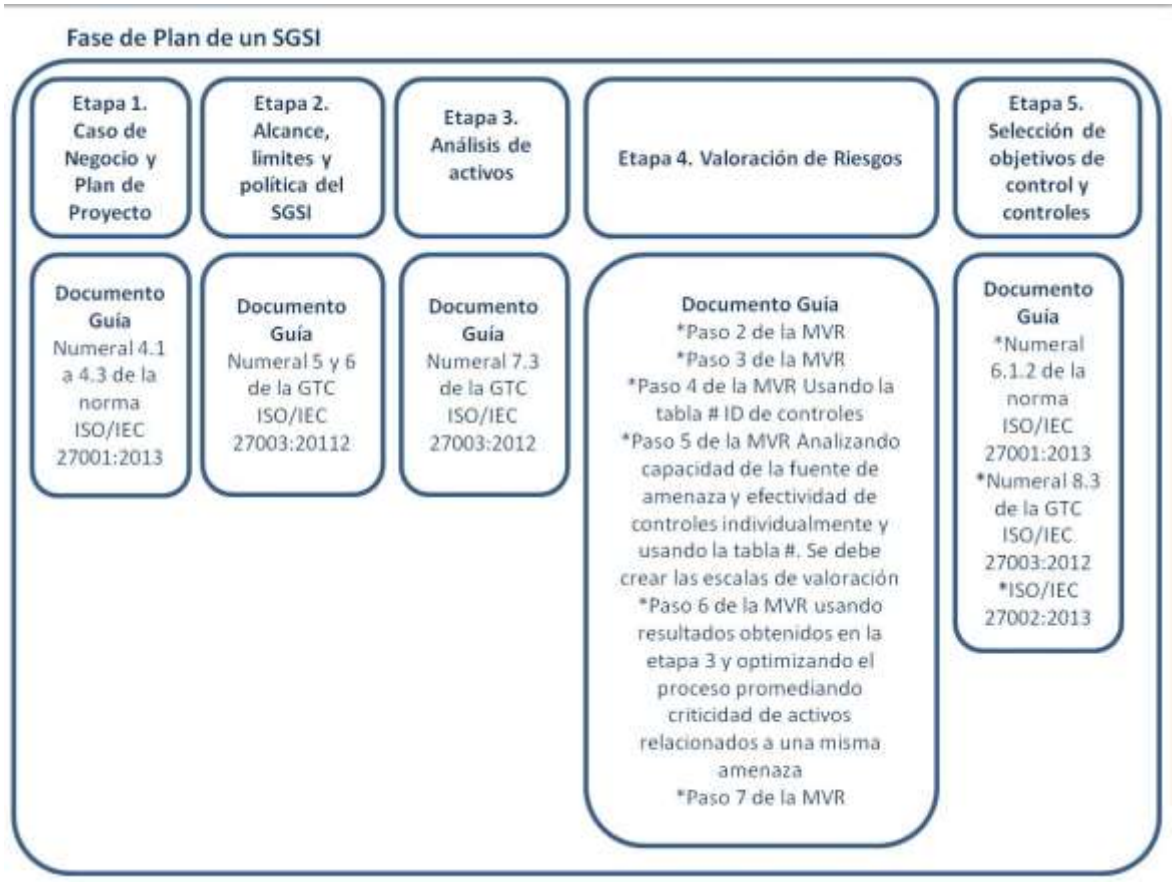

Figura 2-2 Adaptación de la Metodología de Valoración de Riesgos

A continuación se hace una breve descripción de lo que se quiere alcanzar en cada una las etapas mostradas en la figura 2-2.

- Etapa 1. Caso de Negocio y Plan de Proyecto: Contextualización con la empresa. Proponer a la organización las actividades a desarrollar, cronograma y costos.

- Etapa 2. Alcance Limites y Política del SGSI: Definir las partes de la organización que entran en el SGSI

- Etapa 3. Análisis de activos: Realizar en detalle un análisis e inventario de los activos dentro del alcance. Determinar criticidad de activos. Elaborar la MAA como se describe en el numeral 3.9 de este capitulo

- Etapa 4. Valoración de Riesgos: Identificar los riesgos presentes en la organización y determinar su nivel.

- Etapa 5. Selección de objetivos de control y controles: Determinar las opciones para tratar los riesgos y seleccionar controles para los aquellos que se van a mitigar.

3. ESTUDIO DE CASO

Se utilizará el método de caso de estudio siguiendo el modelo propuesto en (*Using a protocol template for case study planning, Brereton*) y las directrices propuestas en (*From chaos to the systematic harmonization of multiple reference models, Pardo, Pino*) En las siguientes subsecciones se describen los estudios en términos de Antecedentes, diseño, criterios para selección de casos, procedimientos y roles del caso, recolección de datos, análisis de resultados y lecciones aprendidas.

3.1 ESTADO DEL ARTE

En la DivTic[5] de la Universidad del Cauca se llevan a cabo procesos de apoyo para todas las dependencias de la comunidad universitaria y maneja equipos y software que contienen información de mucha importancia como por ejemplo el Sistema Integrado de Matricula y Control Académico (SIMCA) en el cual se encuentra el historial de la actividad académica de estudiantes y docentes, la página web de la institución, servidores dns y datos o conexiones con entidades bancarias entre otros. Actualmente la DivTic no cuenta con un sistema de gestión de seguridad de la información que ayude a conservar la Confidencialidad, Integridad y Disponibilidad de los datos en la Universidad así como tampoco se tiene una medida del valor de sus activos, y por tanto no es consciente de sus vulnerabilidades y riesgos.

Es por esto que en la universidad del Cauca se hace necesaria la implantación de un sistema de gestión de seguridad de la información enmarcado en la norma ISO/IEC 27001 Ahora bien, en el desarrollo del SGSI es necesario decidir con que metodología de valoración de riesgos trabajar, entre las más utilizadas se encuentran Magerit, Octave, Mehari, Cramm, Ebios y Nist Sp 8800-30. Cada una con ventajas y desventajas de acuerdo al tipo de organización en que se aplica.

[5] División de Tecnologías de la Información y Comunicaciones

- **A nivel internacional**

Implementación de la guía NIST SP 800-30 mediante la utilización de OSSTMM [16]

En este trabajo de grado se propone una aplicar el manual de metodologías OSSTMM para evaluar la seguridad de la información usando la guía NIST SP 800-30 para realizar el análisis y la evaluación del riesgo aprovechando que no se tiene en cuenta la subjetividad en la valoración de los activos y los riesgos.

Propuesta De Aplicación De Una Metodología Para La Seguridad Informática En La División De Ciencias Básicas [17]

Trabajo de grado que propone una serie de controles de seguridad para mitigar los riesgos encontrados en el caso de estudio utilizando la metodología NIST SP 800-30 y el estándar ISO 27002:2005. En el trabajo se realiza una comparación de varias metodologías de gestión de riesgo llegando a la conclusión de que NIST SP 800-30 es la que mejor se adapta.

Plan De Gestión De Seguridad De La Información Basada En Tics Para La Facultad De Ingeniería De Sistemas De La Escuela Politécnica Nacional [18]

En el trabajo de grado los autores realizaron una planeación de un SGSI en TICS definiendo el alcance y límites del plan para determinar la política del SGSI. Adicionalmente hicieron un análisis de los requerimientos organizacionales para especificar los controles aplicables. Finalmente presentan unas recomendaciones para la implantación y continuidad del SGSI en el caso de estudio.

Análise Comparativa de Metodologias de Gestão e de Análise de Riscos sob a Ótica da Norma NBR-ISO/IEC 27005 [19]

En este trabajo de grado el autor realiza un análisis comparativo de varias Normas, metodologías y herramientas usadas para la gestión y análisis de riesgos resaltando los puntos fuertes de cada una dentro de un cuadro comparativo. Finalmente se destaca una convergencia de integración entre las principales metodologías existentes.

Desarrollo de una aplicación para la gestión de riesgos en los sistemas de información utilizando la guía metodológica NIST SP 800-30 caso práctico: "Liceo Del Valle" [20]

Trabajo de grado en el que se desarrolla un software, utilizando RUP como metodología de desarrollo y UML como herramienta de modelado, que ayuda a la implantación de un sistema de gestión de riesgos siguiendo la metodología NIST SP 800-30. En principio se hace un análisis de la metodología para aplicarla a un caso práctico.

- **A nivel nacional**

Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. [21]

En el artículo se presenta una metodología para la gestión del riesgo tecnológico desarrollada por el autor quien argumenta que las normas ISO 31000 e ISO/IEC 27005 indican "que" se requiere para la gestión de riesgos mas no el "cómo" realizar la gestión por tanto es necesario adoptar una metodología para cada caso en particular.

Análisis De Riesgos En Seguridad De La Información [22]

En el artículo se exponen seis metodologías de análisis de riesgos (OCTAVE, MEHARI, MAGERIT, CRAMM, EBIOS y NIST SP 800-30) y se comparan teniendo en cuenta varios puntos relevantes, destacando a NIST-SP 800-30 en nueve de los once puntos de comparación, argumentando un déficit en el establecimiento de parámetros y necesidades de seguridad finalmente califica a la metodología con un enfoque técnico y la resalta como una excelente guía de administración, evaluación y mitigación de riesgos.

Gestión del riesgo en la seguridad de la información con base en la norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la metodología OCTAVE-S. Caso de estudio: Proceso de Inscripciones y Admisiones en la División de Admisión Registro y Control Académico (DARCA) de la Universidad del Cauca [23]

En este trabajo de grado los autores realizaron la gestión del riesgo al proceso Inscripciones y Admisiones en la División de Admisiones Registro y Control Académico (DARCA) de la Universidad del Cauca.

En él se puede observar la documentación y planeación del proceso de SGSI, bajo la norma NTC ISO/IEC 27005:2011 de Gestión de Riesgos como estándar de seguridad de la información y adicionalmente los autores realizaron una adaptación a la Metodología OCTAVE-S para el de estudio.

Se ha seleccionado probar la metodología NIST SP 800-30, ya que es gratuita, su ámbito de aplicación es internacional y ha sido desarrollada por el instituto nacional de estándares y tecnología (NIST) uno de los más importantes y reconocidos a nivel mundial. Sin embargo resulta el siguiente interrogante:

¿Es posible adaptar la metodología de valoración de riesgos NIST SP 800-30 a la fase de plan de un SGSI basado en la norma ISO/IEC 27001, ajustándola a una organización que trabaja en entornos TIC?

3.2 DISEÑO

El diseño del estudio de caso se clasifica por el número de casos y la unidad de análisis, según Stake [24], al tener un solo estudio de caso siendo este la Universidad del Cauca y como única unidad de análisis la DivTIC, la clasificación es simple y holística.

3.3 SELECCIÓN DE CASO

La universidad del cauca en su necesidad de conservar su prestigio y competitividad como institución educativa reconocida a nivel nacional, decidió i implementar el proyecto “sistema de gestión de seguridad de la información de la universidad del cauca” para el cual ya estaban definidas y priorizadas las áreas específicas en donde se desarrollaría el proyecto. Por parte de los responsables del proyecto mencionado se asignó como estudio de caso la División de tecnologías de información y comunicaciones.

3.4 PROCEDIMIENTOS DE CAMPO

El procedimiento se basa en el modelo PDCA, específicamente en la fase de plan, que inicia con una contextualización de la organización, se definen las áreas o procedimientos de la organización que requieren ser protegidos, posteriormente se hace un análisis de los activos fundamentales para la continuidad del negocio. Luego se realiza una valoración de los riesgos presentes y finalmente se determinan las opciones de tratamiento de riegos. Cabe mencionar que los puntos mencionados se deben desarrollar en una secuencia definida para cualquier SGSI y se debe seguir para obtener los resultados.

3.5 RECOLECCIÓN DE DATOS

3.5.1 Identificación de datos a ser recolectados

En la tabla 3-1 se muestran los datos más relevantes dejando en claro que en el proceso se obtienen muchos más datos específicos relacionados a cada etapa del desarrollo.

Etapa	Datos
Descripción de procesos y procedimientos	Modelo de operación de procesos Esquema del mapa de procesos y procedimientos Descripción y actividades del procedimiento
Caso de negocio y plan de proyecto	Organigrama de la DivTIC Recursos y presupuesto para el proyecto
Alcance y límites	Interfaces y dependencias del SGSI con otras partes de la organización.

	Relaciones entre procedimientos de la DivTIC y otras áreas de la universidad así como con entidades externas.
Análisis de activos de información	Activos de información y sus características
Valoración del riesgo	Cómo funciona la organización Amenazas Vulnerabilidades Controles existentes
Selección de objetivos de control y controles	Prioridades de la organización

Tabla 3-1 Recolección de datos

3.5.2 Plan de recolección de datos

La recolección se hizo por medio de entrevistas, encuestas a la dirección y personal del área de servicios y servidores de internet que son los responsables del procedimiento trabajado.

Además se revisaron documentos y reportes logrando así obtener información indispensable para el desarrollo del trabajo., finalmente se diseñó una matriz de inventarios que facilitó la obtención de activos de información y todas sus características.

3.5.3 Almacenamiento de datos

En un SGSI es de obligatorio cumplimiento almacenar los datos en documentos entregables previamente definidos, adicionalmente se diseñaron tablas y gráficas para un correcto almacenamiento y análisis de los datos obtenidos.

3.6 OBTENCIÓN DE RESULTADOS Y RECOMENDACIONES DE APLICACIÓN

NOTA: Para no comprometer la seguridad de la organización, en este documento no se muestran los análisis y resultados de carácter confidencial, pero se creó un ejemplo con amenazas, vulnerabilidades y controles genéricos con el fin de mostrar al lector la forma en que aplican los procesos para desarrollar las diferentes etapas y el uso de las tablas creadas en este trabajo para consignar los datos. En este trabajo se desarrollaron todos los entregables requeridos y fueron entregados a la organización, si existe interés por conocerlos en detalle se debe comunicar con la División de Tecnologías de la Información y Comunicaciones de la Universidad del Cauca

En este capítulo se describe como se llevó a cabo la adaptación propuesta ajustándola al caso real Procedimiento Gestión de Servicios y Servidores de Internet de la DivTIC de la Universidad del Cauca, y se muestran una serie de recomendaciones, producto de la experiencia del desarrollo de este trabajo que servirán como base para aplicar la adaptación propuesta en otras organizaciones que trabajen con ambientes TIC.

3.6.1 Descripción del procedimiento

3.6.1.1 Estructura de procesos y procedimientos de la Universidad del Cauca

De acuerdo a El Modelo Estándar de Control Interno para el Estado Colombiano MECI y la norma técnica de calidad GP1000, la Universidad del Cauca está implantando el "sistema interno de gestión de la calidad" como herramienta ideal para dirigir y evaluar el desempeño institucional, en términos de calidad y satisfacción social en la prestación de servicios; tal y como se decreta en la ley 872 de 2003 [14], en cumplimiento con la norma, se identifican, priorizan y documentan de forma clara los procesos estratégicos determinantes en la calidad de manera metódica se ha hecho la gestión y modelo de operación por procesos, definiendo inicialmente cuatro macro procesos, figura 3-1.

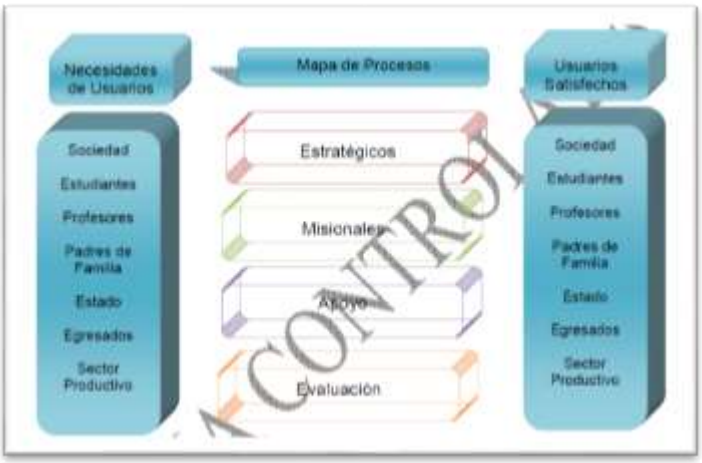

Figura 3-1 Estructura del mapa de procesos de la universidad del Cauca

Dentro de cada macro proceso se incluyen una serie de procesos, para nuestro caso de estudio nos concentraremos en el proceso "Gestión Administrativa" este, junto al proceso "Gestión de la Cultura y el Bienestar" conforman el macro proceso de Apoyo, como se muestra en la Figura 3-2.

Figura 3-2 Esquema del mapa de procesos de la Universidad del Cauca

El proceso gestión administrativa, tiene como objetivo principal administrar todos los recursos universitarios de manera eficiente, eficaz, efectiva y transparente, de modo que apoyen el cumplimiento de los objetivos institucionales, dentro de los principios de ética universitaria y autonomía responsable. De este, se desglosan doce subprocesos, que se enumeran a continuación:

- Apoyo Administrativo
- Gestión del talento humano
- Gestión de la salud ocupacional
- Gestión financiera
- Gestión de la infraestructura y el mantenimiento físico
- Gestión jurídica
- Gestión de bienes y servicios
- Gestión de recursos tecnológicos
- Gestión de admisiones, registro y control académico
- Gestión documental
- Gestión de recursos bibliográficos
- Gestión de la seguridad y movilidad

El subproceso Gestión de Recursos tecnológicos tiene como objetivo suministrar los medios y herramientas necesarios para soportar el funcionamiento de los servicios tecnológicos de información y comunicación en la institución. [17]

En este punto inicia la labor de este trabajo de grado, seleccionando el procedimiento crítico dentro del área de recursos tecnológicos perteneciente a la DivTIC; los 26 procedimientos que conforman al subproceso son:

1) Administración del centro de datos.
2) Gestión de servidores y servicios de internet.
3) Gestión del servicio de acceso a internet.
4) Atención al usuario.
5) Soporte y mantenimiento de sistemas de información.
6) Implementación de nuevos servicios de infraestructura de red.
7) Desarrollo y mantenimiento de aplicaciones.
8) Apropiación tecnológica “Proteo”.
9) Adquisición de licencias de software para el Data Center.

10) Plan de contingencia.
11) Gestión de proyectos de TIC para la universidad del cauca.
12) Adquisición de aplicaciones informáticas.
13) Diseño y desarrollo de productos web.
14) Vinculación de monitores.
15) Control de acceso físico a la división TIC.
16) Creación de una nueva instancia en la base de datos.
17) Creación o modificación de datos y objetos en la base de datos.
18) Creación y verificación de copias de seguridad de bases de datos.
19) Recuperación de una instancia.
20) Auditoria de la seguridad de la información.
21) Creación y verificación de copias de seguridad en los sistemas de información.
22) Seguridad de las redes de información.
23) Monitoreo de dispositivos de la red de información.
24) Acceso físico a centros de cableado.
25) Configuración e instalación de dispositivos de red de información.
26) Optimización del funcionamiento de los dispositivos de la red de información.

Luego de una evaluación por parte de las directivas de la DivTIC, se determinó que el procedimiento Gestión de servicios y servidores de internet es el de mayor importancia e impacto en el área y por tanto el procedimiento en el que se debe centrar el SGSI.

3.6.1.2 Procedimiento gestión de servicios y servidores de internet

Según el documento PA-GA-5.3.PR-2 [7] procedimiento Gestión de Servidores y Servicios de Internet, en el que se describe detalladamente el procedimiento gestión de servicios y servidores de internet, el objetivo principal de este es "Administrar, operar y mantener los servidores y servicios de internet e intranet de la División TIC, que prestan servicios a toda la comunidad universitaria"

El procedimiento se desglosa en una serie de actividades que proporcionan una guía operacional que busca precisar la forma correcta de lograr el objetivo propuesto. Las actividades son:

1) Registrar la solicitud inicial de servidores y servicios de internet.
2) Estudiar el requerimiento, la viabilidad y la determinación de instalación y reserva de recursos.
3) Instalar, aprovisionar y asignar los recursos software y hardware.
4) Ejecutar pruebas de funcionamiento del servidor o servicio y su funcionalidad.
5) Reservar los recursos de red, realizar la asignación de dominios, direccionamiento y configuraciones asociadas.
6) Reservar los recursos de bases de datos.
7) Verificar el funcionamiento total y validar los resultados en producción.
8) Determinar los esquemas de seguridad asociados.
9) Determinar las conexiones en la intranet e internet según el procedimiento de administración de acceso a internet.
10) Generar los manuales internos de implementación, operación y mantenimiento.
11) Monitorear el funcionamiento del servidor y/o servicio.
12) Realizar y verificar copias de seguridad.
13) Implementar mejoras, parches, adecuaciones y adiciones al servicio.

3.6.2 Caso de negocio y plan de proyecto

Lo primero que se sugiere es que para seleccionar el o los procedimientos críticos, sea la organización quien los elija de acuerdo a sus criterios y tomarlos como base para iniciar el trabajo ya que es la organización quien mejor conoce sus procedimientos. Se debe iniciar el proyecto y cuando se llegue a la etapa de Alcance y Límites del SGSI en la elaboración del diagrama de las elipses se confirmara si realmente ese procedimiento es crítico o no.

Para el desarrollo de la primera etapa de la fase de plan se recomienda acordar una primera reunión con la dirección en la que el tema central será las prioridades de la organización para desarrollar un SGSI. En ella se informa sobre los beneficios de la implantación de un SGSI en la organización. También se habla de forma general, como se pueden llevar a cabo las siguientes reuniones,

disponibilidad del personal, días o fechas en los que es más fácil para la organización hacer las reuniones. Para la dirección de la organización se recomienda que sea en la primera reunión en la que se exija al personal que va a implantar el SGSI un acuerdo de confidencialidad, necesario para continuar con el desarrollo del proyecto en el que cada vez se entrega información de mayor grado de confidencialidad. Al personal encargado de llevar a cabo el SGSI en la organización re recomienda aclarar el mayor número de dudas posibles en esta reunión ya que es en la cual se obtiene una visión amplia y general de la organización.

Después de realizar la primera reunión y con una visión más clara se procede a realizar los tres pasos esenciales de esta atapa.

3.6.2.1 Prioridades de la organización para desarrollar un SGSI

En ocasiones las organizaciones tienen definidas y documentadas sus prioridades en cuanto la seguridad de la Información. Para este caso estaban definidas y fueron tomadas del formato Política del SGSI [28], estas pueden ser usadas por las entidades públicas y privadas colombianas, debido a que así lo determino el Ministerio de las TICs a través de su programa Estrategia para Gobierno el Línea. A continuación se muestran las prioridades de la organización para desarrollar un SGSI que también se pueden tomar como base para crear o definir las de otra organización:

a) Minimizar el riesgo en las funciones más importantes de la institución
b) Cumplir con los principios de seguridad de la información
c) Cumplir con los principios de la función de la dirección universitaria
d) Mantener la confianza de todos sus estamentos universitarios
e) Apoyar la innovación tecnológica
f) Implementar el Sistema de Gestión de Seguridad de la Información – SGSI

g) Proteger los activos tecnológicos

h) Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información

i) Fortalecer la cultura de seguridad de la información en sus estamentos universitarios, contratistas y proveedores

j) Garantizar la continuidad de la Institución frente a incidentes

3.6.2.2 Alcance preliminar del SGSI

Para definir el Alcance preliminar se obtuvo información por medio de entrevistas con la dirección acerca de los activos o áreas de la organización que requieren ser protegidos con el SGSI. Como su nombre lo indica debe ser de forma general ya que más adelante se desarrollará un análisis detallado de los activos dentro del SGSI.

- Área de Servicios y Servidores de Internet de la DivTIC Unicauca
- Oficinas y áreas de trabajo Físicas del Área SSI,
- Centros de datos del Área SSI: Centro de datos TIC e IPET
- Servidores
- Enclosure
- Firewalls
- Equipos terminales
- Equipos de telecomunicaciones
- Personal del Área SSI

3.6.2.3 Roles y responsabilidades

La organización debe tener claro que existen unos roles y responsabilidades básicos para el éxito del SGSI. A continuación se presenta la Tabla 3-1 que muestra los roles y responsabilidades para un SGSI en cualquier área o dependencia de la Universidad del Cauca, tomada del Proyecto “Implantación y Certificación del SGSI de la Universidad del Cauca, aprobado mediante la

Resolución 005 del 7 de Enero de 2015. La tabla contiene las responsabilidades genéricas que se deben asumir en un SGSI, por lo que puede usarse como ejemplo para definir los roles en el SGSI de otra organización.

Rol	Breve descripción de la responsabilidad
Nivel Directivo	
Comité de dirección de la Universidad del Cauca	Responsable con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento, mejora, auditorías y certificación del SGSI y la Asignar tiempo y recursos para que sus activos de información estén lo suficientemente protegidos.
Nivel Estratégico	
Comité de seguridad de la Información	Responsables de los temas relacionados con la seguridad de la información, asignar responsables, tareas, actividades y tomar decisiones en cuanto a seguridad de la información se refiere respaldado por el COMITÉ DE DIRECCIÓN, buscando siempre la mejora del SGSI.
Nivel Táctico	
CISO (Oficial de Seguridad de la Información)	Responsable máximo de planificar, desarrollar, controlar y gestionar las políticas, procedimientos y acciones con el fin de mejorar la seguridad de la información dentro de sus pilares fundamentales de confidencialidad, integridad y disponibilidad.
Nivel Técnico Y operativo	
Líderes Técnicos de las Aplicaciones	Profesionales adscritos a la División de las TIC de la Universidad, responsables de mantener operando las respectivas Aplicaciones software y de ayudar a los usuarios finales a ser más eficaces en el desempeño de su labor.
Administrador de Base de datos	Profesionales adscritos a la División de las TIC de la Universidad, responsables del normal funcionamiento de las respectivas Bases de Datos de las correspondientes Aplicaciones de los Sistemas de Información Institucionales.

Líderes Funcionales de las aplicaciones	Todas las Aplicaciones utilizadas en la Universidad, deben contar con su respectivo Líder Funcional que garantice la calidad e integridad de la información. Estos funcionarios son responsables de los correspondientes activos de información institucionales. Los Líderes Funcionales de las Aplicaciones son los respectivos Jefes de las Dependencias universitarias o sus delegados
Usuarios Finales de las aplicaciones	Los usuarios finales de las Aplicaciones, corresponden a los funcionarios de cada Dependencia de la Universidad, que registran y actualizan la información en forma permanente en su respectiva Aplicación que hace parte de los Sistemas de Información Institucionales

Tabla 3-2 Roles y responsabilidades

3.6.2.4 Caso de negocio y plan de proyecto.

Para realizar el plan de Proyecto se tuvo en cuenta las etapas y descripciones de la Guía de Implementación de un SGSI, ISO/IEC 27003:2012. Esto para garantizar que el SGSI cumplirá con todos los requisitos exigidos a la hora de recibir una auditoria para certificación.

En este trabajo se dividió el SGSI en 13 actividades, pero cada organización tiene la libertad de definir su propio cronograma.

- **FASE 1: Revisión y recolección.**

  - **Actividad 1:**Revisión y recolección de información relacionada con sistemas de gestión de seguridad de la información, las diferentes normas ISO aplicables y la metodología NIST SP 800-30; se espera realizar una síntesis que permita la construcción de una base de conocimientos apropiada para el desarrollo del trabajo.

- **FASE 2: Planificación.**

- **Actividad 2:** Obtención de la aprobación de la dirección para iniciar un proyecto de SGSI.

- **Actividad 3:** Definir el alcance y los límites de la organización. Identificar las áreas de la organización tales como procesos, ubicaciones físicas, sistemas de información y personas involucradas con la organización.

- **Actividad 4:** Definir el alcance y los límites de las tecnologías de la información y las comunicaciones (TIC). Identificar los procesos de negocio de sistemas de información y los elementos relacionados con Tics. Esto incluye todas las partes de la organización que almacenan, procesan o transportan información.

- **Actividad 5:** Definir el alcance y los límites físicos. Identificar instalaciones, locales, oficinas, etc., de la organización que se recomienda que formen parte del SGSI.

- **Actividad 6:** Integrar cada alcance y los límites para obtener el alcance y los límites del SGSI. Con los alcances de la organización, tecnologías de la información y comunicaciones y el de los límites físicos se determina el alcance del SGSI con el objetivo de conocer claramente que áreas o sistemas están dentro del SGSI y cuáles no.

- **Actividad 7:** Definición de la política del SGSI y obtención de la aceptación de la dirección. Establecer los objetivos del SGSI, el enfoque general, una guía para lograr los objetivos y el criterio para evaluación de riesgos. Aclarar las responsabilidades de la alta dirección con respecto al SGSI y obtener la aprobación de la misma.

- **Actividad 8:** Definir los requisitos de seguridad de la información para el procedimiento del SGSI. Se debe hacer una identificación preliminar de los activos de información importantes. También se debe identificar las visiones de la organización. Analizar las formas actuales de procesamiento de la información,

aplicaciones, redes de comunicación, ubicación de las actividades y recursos de tecnologías de la información. Identificar todos los requisitos esenciales. Identificación del nivel de toma de conciencia sobre seguridad de la información.

- **Actividad 9:** Identificar los activos dentro del alcance del SGSI. Identificar la criticidad del procedimiento y de los activos de información, también las aplicaciones de tecnologías de información que apoyan al procedimiento.

- **Actividad 10:** Realizar una evaluación de la seguridad de la información. Comparar el estado actual de seguridad de la información de la organización con los objetivos que desea alcanzar.

- **Actividad 11:** Realizar la valoración de riesgos. Identificar amenazas y sus fuentes, controles existentes y planificados, vulnerabilidades y las consecuencias que pueden tener sobre los activos. Evaluar el impacto sobre el negocio, probabilidad de distintos escenarios de incidentes. Estimar nivel de riegos. Comparar los niveles de riesgo con los criterios de valoración y aceptación de riesgos.

- **Actividad 12:** Seleccionar los objetivos de control y los controles. Especificar la relación entre los riesgos y las opciones para tratarlos.

- **FASE 3: Documentación.**

- **Actividad 13:** Revisión y entrega de documentación.

Una vez definidas las actividades a realizar se debe elaborar un cronograma para presentarlo a la organización. Para nuestro caso se definió el tiempo de duración de cada una de las actividades con la ayuda del experto en el tema de seguridad de la Información, Ing. Esp. Siler Amador Donado, a quien agradecemos por su inmensa colaboración.

La tabla 3-3 muestra el cronograma propuesto a la dirección de la organización.

Nota: La tabla 3-3, es un bosquejo de como presentar el cronograma, pero se debe tener en cuenta que para la organización es muy importante tener esta información lo mejor detallada posible, con fechas exactas de inicio y terminación de actividades

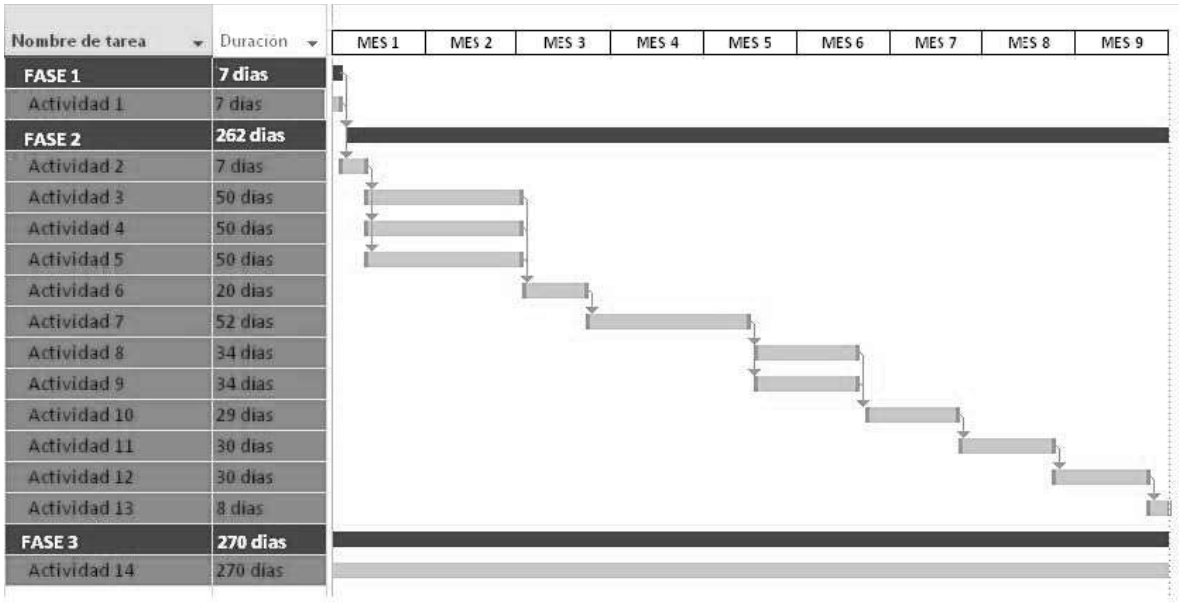

Tabla 3-3Cronograma de actividades

Para proponer el caso de negocio a la dirección se recomienda consultar expertos en el tema de costos de un SGSI y preferiblemente contar con ellos a la hora de una posible negociación con la organización. Este trabajo por su naturaleza de tipo académico, está enfocado a proponer una adaptación y ajuste de una metodología para la valoración de riesgos, por tal razón no realizo un estudio de costos, pero cabe mencionar que es una actividad que se debe presentar formalmente.

Finalmente se debe elaborar el documento entregable de esta etapa con la información obtenida a lo largo del proceso.

3.7 ALCANCE Y LÍMITES DEL SGSI.

Como se definió en el capítulo de Adaptación esta etapa se aplicará de acuerdo a los detalles descritos en el numeral 5 y 6 de la GTC ISO/IEC 27003:2012.

3.7.1 Alcance y los límites de la organización

La organización debe definir el o los procedimientos críticos a los cuales se quiere implantar el SGSI. Para este caso la DivTIC seleccionó el procedimiento Gestión de Servicios y Servidores de Internet, al final de esta actividad se puede concluir si el procedimiento seleccionado es o no el más crítico.

Para determinar el Alcance y Limites de la organización se llevó a cabo el método de las elipses propuesto por Alexander [29], con el cual se busca hacer un análisis grafico de los procedimientos de la organización para facilitar posteriormente la identificación de los activos dentro del SGSI, además nos permitirá conocer la criticidad de cada procedimiento.

La elaboración del diagrama de las elipses se hace teniendo en cuenta las relaciones existentes entre los procedimientos de la organización y áreas o dependencias tanto internas como externas a la organización. De esta manera el diagrama tendrá una elipse concéntrica que incluye los procedimientos de la organización, para este caso los del Área de SSI, la elipse intermedia incluye las dependencias de la universidad que se relacionan con los procedimientos del área de SSI y la elipse más grande contiene las entidades externas relacionadas con el área de SSI. Las relaciones se marcan con flechas la figura 3-3 muestra el diagrama de las elipses para los procedimientos del Área SSI.

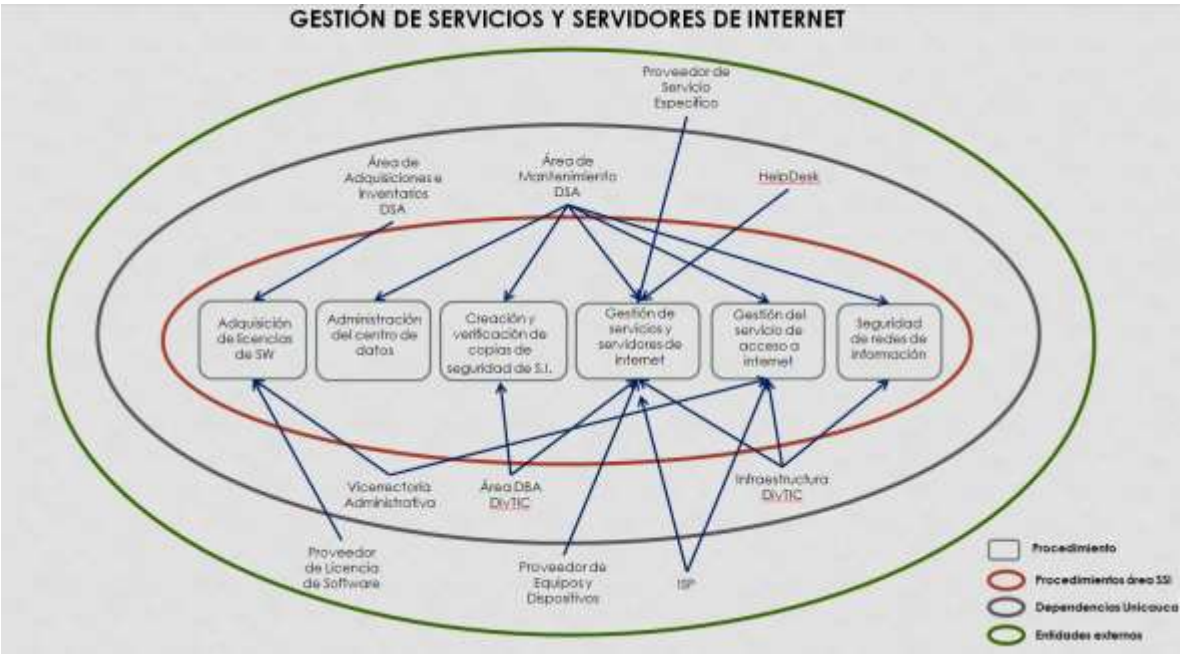

Figura 3-3 Diagrama de las elipses

Cada organización el libre de elegir el criterio por el cual seleccionara al o los procedimientos más críticos, para este caso se tuvo en cuenta el siguiente:

"Numero de relaciones del procedimiento con otras áreas o dependencias en el diagrama de las elipses". Se definió de esta forma debido a que las flechas indican flujo de información que es lo que se quiere asegurar.

Según el diagrama, el procedimiento con más relaciones es el de Gestión de Servicios y Servidores de Internet que tiene siete relaciones con áreas o dependencias tanto internas como externas a la Universidad del Cauca. Esto confirma que la dirección tuvo una elección acertada acerca del procedimiento crítico. Cabe resaltar que se puede seleccionar más de un procedimiento, pero por el tiempo limitado para el desarrollo de este trabajo solamente se seleccionó uno.

En caso de que el procedimiento seleccionado inicialmente por la organización no concuerde según el criterio definido, se recomienda realizar una reunión e indicar a la dirección que según el desarrollo de esta etapa se concluyó que existe otro procedimiento en el cual hay mayor flujo de información.

3.7.2 Alcance y los límites de las tecnologías de la información y las comunicaciones (TIC)

Se recomienda para realizar esta actividad tener en cuenta los activos relacionados con infraestructura tecnológica obtenidos anteriormente en la lista del alcance preliminar, esto no significa que se deba trabajar solamente con ellos sino que es una lista que va enriqueciendo y detallando poco a poco, aunque en esta actividad aún queda una lista general, en la etapa de análisis de activos se obtendrá una lista con un nivel de detalle avanzado. En este punto es recomendable clasificar los activos hardware de los de software y agregar en lo posible una columna con los responsables de los activos. Se creó la tabla 3-4. Que muestra un ejemplo para consignar los activos TIC para el caso de aplicación.

Tipo de Activo	Activos	Responsable
Hardware	Servidores Rack	Profesional 1
	Servidores Blade	
	Matriz de Almacenamiento	
	UPS	Técnico 1
	Enclosure	Técnico 2
	Firewalls	Profesional 2
Software	Sistemas de monitoreo	Técnico 3
	Sistemas de gestión de ancho de banda	Profesional 3
	Sistema de gestión de firewalls	Profesional 2
	Bases de datos	Profesional 3
	Firmas y antivirus	Profesional 2

Tabla 3-4 Lista preliminar de activos de información

3.7.3 Alcance y los límites físicos

Es recomendable que la organización cuente con planos de sus instalaciones físicas, sistema de acueducto, aire acondicionado y red eléctrica entre otros ya que servirán como soporte en la elaboración de planes de contingencia o continuidad del negocio en caso de incidentes o desastres mayores. Si la

organización no cuenta con información detallada de este tipo, se debe sugerir que la adquieran.

Para este caso la organización contaba con información muy general, por lo que se hizo la recomendación respectiva.

Los resultados obtenidos para esta etapa fueron los siguientes:

La organización cuenta con instalaciones físicas ubicadas en el Edificio Facultad de Ciencias Naturales, Exactas y de la Educación, Carrera 2 #3N-111, piso 2, Popayán, Colombia, *Figura 3-4,* en el cual se encuentran las oficinas de la DivTIC y un cuarto de servidores y telecomunicaciones.

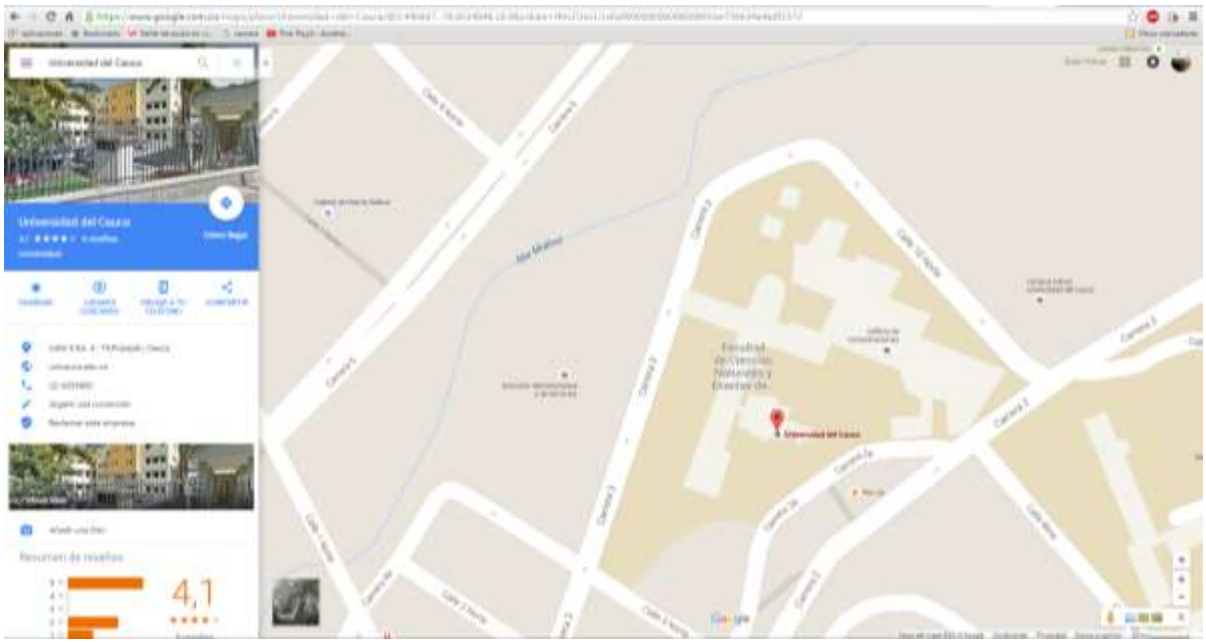

Figura 3-4 Ubicación geográfica de la organización

Fuente:https://www.google.com.co/maps/place/Universidad+del+Cauca/@2.4462974,76.6008165,18.96z/data=!4m2!3m1!1s0x0000000000000000:0xe759634a4adf3372

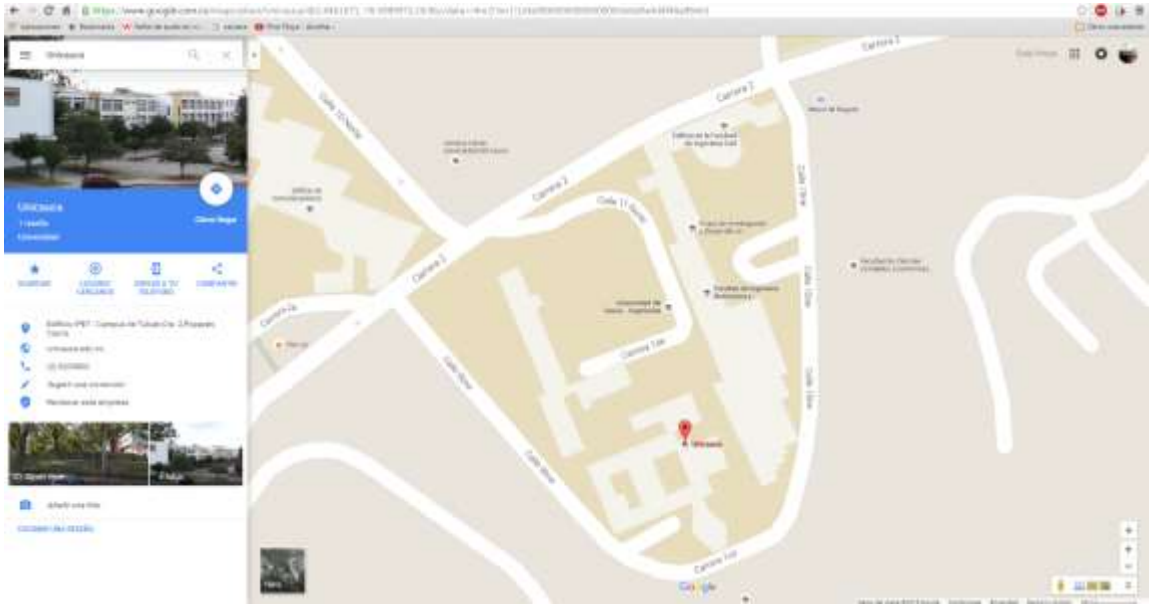

Figura 3-5 Ubicación geográfica FIET

Fuente:https://www.google.com.co/maps/place/Unicauca/@2.4461071,76.5989972,18.96z/data=!4m2!3m1!1s0x0000000000000000:0x6d0a4d4f46a89e63

Un segundo cuarto de servidores y telecomunicaciones está ubicado en el edificio del instituto de posgrados de la facultad de Ingeniería Electrónica y Telecomunicaciones, Calle 5 No. 4 - 70, Popayán, Colombia. *Figura 3-5.*

3.7.4 Integración de alcance y los límites del SGSI

La integración consiste en realizar el documento entregable de forma clara y concisa con toda la información obtenida en los tres alcances anteriores

.

3.8 Política de seguridad de la información

La elaboración de una política de seguridad de la información, puede tornarse algo tediosa para una organización que aún no la tiene definida o cuando el personal no cuenta con una amplia experiencia en redacción de este tipo de política. Para el caso de entidades tanto públicas como privadas de Colombia, el gobierno nacional a través del Ministerio de las TICs ha definido en su programa Estrategia

para Gobierno en Línea un modelo o plantilla para la elaboración de una Política de seguridad de la información [28], la cual se puede usar como base, ya que esta creada de acuerdo a los requisitos establecidos por la norma ISO/IEC 27001:2013.

Para el caso de aplicación se definió la Política de Seguridad que aplicará para cualquier área o dependencia de la Universidad del Cauca y fue aprobada por medio de la resolución 785 del 7 de Octubre de 2015.

A continuación se muestra un modelo general de Política de Seguridad de la Información que puede ser aplicado a cualquier entidad pública en Colombia.

La organización, para el cumplimiento de su Misión, Visión, plan estratégico y apegado a sus valores institucionales, establece la función de la seguridad de la Información en la organización, con los objetivos de:

a) Minimizar el riesgo en las funciones más importantes de la Institución
b) Cumplir con los principios de seguridad de la información
c) Cumplir con los principios de la dirección universitaria
d) Mantener la confianza de todos sus estamentos universitarios
e) Apoyar la innovación tecnológica
f) Implementar el sistema de gestión de Seguridad de la Información – SGSI
g) Proteger los activos tecnológicos
h) Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información
i) Fortalecer la cultura de seguridad de la información es sus estamentos universitarios, contratistas y proveedores
j) Garantizar la continuidad de la institución frente a incidentes

Alcance y Aplicabilidad: La política del SGSI de la Universidad del Cauca, aplica a toda la institución, sus estamentos universitarios, contratistas, proveedores y ciudadanía en general.

Nivel de cumplimiento: La política debe cumplirse en un 100% para todas las personas cubiertas por el alcance y su aplicabilidad.

Documentos de referencia, obligaciones legales, regulatorias y contractuales.

- NTC ISO/IEC 27001:2013.
- GTC ISO/IEC 27003:2012.
- Formato política SGSI - modelo de seguridad de la información para la estrategia de gobierno en línea.
- Ley 527 de comercio electrónico y firma digital del 18 de Agosto de 1999.
- Ley 1266 habeas data del 31 de Diciembre de 2008.
- Ley 1273 de delitos informáticos del 5 de Enero de 2009.
- Ley 1581 para protección de datos personales del 17 de Octubre de 2012.
- Decreto 1704: Seguridad de los operadores de servicios de telecomunicaciones del 15 der Agosto de 2012.
- Decreto 1377: Protección de datos personales del 25 de Junio de 2013.
- Decreto 2573: Lineamientos generales de la estrategia de gobierno en línea del 12 de Diciembre de 2014.

A continuación se definen las políticas de seguridad que soportan el SGSI de la organización:

- La organización ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información – SGSI, soportado en lineamientos claros alineados a las necesidades institucionales y a los requerimientos regulatorios.

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los estudiantes, administrativos, docentes, contratistas y proveedores.

- La organización protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- La organización protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- La organización controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- La organización implementará control de acceso a la información, sistemas y recursos de red.

- La organización garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- La organización garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- La organización garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

- La organización garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

Se puede observar que el modelo de Política de Seguridad de la Información cuenta con objetivos, alcance y aplicabilidad, nivel de cumplimiento, Documentos de referencia, obligaciones legales, regulatorias y contractuales y además tiene un enfoque general para para lograr los objetivos de un SGSI, lo cual muestra que cumple con los requisitos exigidos el numeral 5.2 de la norma ISO/IEC 27001:2013 referente a Política de Seguridad de la Información.

3.9 Análisis de activos de información

Con el fin de obtener una lista detallada de activos y para hacer más rápido el proceso, se elaboró, con ayuda de personal encargado de la Estrategia para Gobierno el Línea del Ministerio de lasa TICs, una matriz a la que llamamos MAA (Matriz de Análisis de activos), en la que se describe cada uno de los activos. Para

esto era necesario complementar la lista de activos obtenida en alcance y límites de las TICs, haciendo un inventario más específico de los activos. A continuación se agregaron campos en la matriz que sirven para detallar la función y el valor de cada activo para la organización. Los campos de la MAA son los siguientes, cabe aclarar que una organización puede agregar campos que ayuden a describir mejor los activos de su caso particular.

Términos y definiciones:

- **Proceso:** Área o proceso que pertenece el activo de información.

- **Propietario:** Es una parte designada de la organización, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de definir quienes tienen acceso y que pueden hacer con la información y de determinar cuáles son los requisitos para que la misma se salvaguarde ante accesos no autorizados, modificación, pérdida de la confidencialidad o destrucción deliberada, y al mismo tiempo de definir que se hace con la información una vez ya no sea requerida.

El término “Propietario” no implica que la persona tenga realmente los derechos de propiedad de los activos.

- **Nombre del Activo:** Es un campo que define la manera como se va a reconocer el activo de información en el proceso y la entidad, con un nombre particular y diferenciable.

- **Descripción (funcionalidad):** Información adicional que permita identificar de manera única el activo de información o su importancia dentro de la entidad o proceso.

- **Activos de información asociados:** Es posible que dos activos estén fuertemente relacionados, por ejemplo un activo software está relacionado con el servidor en el que está instalado.

- **Tipo:** Se define el tipo al cual pertenece el activo. Entre los cuales tenemos: Información, software, hardware, Servicios e intangibles.

- **Información:** tipos de activo como: datos, sistemas de información e información almacenada o procesada física o electrónicamente como por ejemplo: las bases de datos, archivos de datos, contratos, acuerdos, documentación del sistema, información sobre investigaciones, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, pruebas de auditoría e información archivada física o electrónicamente.

- **Software:** tipos de activos como: herramientas de ofimática, herramientas de propósito específico, herramientas de desarrollo, utilidades, aplicaciones para acceso a la información.
- **Hardware o Físico:** Son activos cómo por ejemplo: Equipos de computación, equipos de comunicaciones, medios removibles, instrumentos particulares para la ejecución del proceso y otros equipos físicos.

- **Servicios:** Servicios de computación y comunicaciones. (Ejemplo: Acceso a Internet, páginas de consulta, acceso a la red, etc.), servicios de outsorcing.

- **Atributos:** Cada activo de información se le relaciona uno o más atributos, los cuales permiten identificar su sensibilidad y justificar el valor asignado al activo y adicionalmente permitirán obtener elementos que permitan darle un tratamiento adecuado. Para la matriz de inventario los atributos son los siguientes:

Ítem	Atributo	Descripción
1	A1	Activo de información de clientes o terceros que debe protegerse de accesos no autorizados, pérdida de integridad o indisponibilidad.
2	A2	Activo de información que debe ser restringido a un número limitado de funcionarios.
3	A3	Activo de información que debe ser restringido a personas externas.
4	A4	Activo de información que puede ser alterado o comprometido para fraudes o corrupción.
5	A5	Activo de información que es muy crítico para las operaciones internas.
6	A6	Activo de información que es muy crítico para para la prestación de servicio a terceros, tales como ciudadanos, organismos de control u otras organizaciones.

7	A7	Activo de información que ha sido declarado de conocimiento público por parte de la persona con autoridad para hacerlo o por alguna norma jurídica.

Tabla 3-5Atributos de activos de información

- **Niveles de clasificación y de confidencialidad de los activos de información:** Los niveles de clasificación de los activos de información son los siguientes:

  - **Pública: L**a información pública es aquella que ha sido declarado de conocimiento público por parte de la persona con autoridad para hacerlo o por alguna norma jurídica. Esta información puede ser entregada o publicada sin restricciones a terceros, funcionarios o cualquier persona sin ocasionar daños a terceros ni a los procesos de negocio de la institución.

  - **Confidencial: L**a información confidencial es toda aquella que no es pública. Y a la información pública solo pueden tener acceso las personas que han sido declaradas usuarios legítimos de esta información con privilegios asignados.

  - **Restringida:** Información que es utilizada por solo un grupo de funcionarios de la institución para realizar sus labores y que no puede ser conocida por otros funcionarios o terceros sin previa autorización. En caso de ser conocida, utilizada o modificada por personas no autorizadas impactaría de manera grave a los procesos de la entidad.

En la MAA se agregaron campos en lo que se puede hacer una valoración de la criticidad de cada uno de los activos en términos de perdida de confidencialidad, integridad y disponibilidad. Para ellos se usaron los criterios y definiciones, mostrados a continuación y tomados de la MVR

- **Criticidad:** Para valorar y priorizar los activos de información es de vital importancia darles un valor de confidencialidad, integridad y disponibilidad.

- **Confidencialidad:** Protección para que el activo de información sea accesible solamente por aquellas personas autorizadas. En este campo en el inventario se presenta uno de los siguientes valores:

Criterio	Nivel	Definición
3	Alto	El conocimiento o divulgación no autorizada de este activo de información impacta negativamente a la institución.
2	Medio	El conocimiento o divulgación no autorizada de este activo de información impacta negativamente de manera importante al proceso.
1	Bajo	El conocimiento o divulgación no autorizada de este activo de información impacta negativamente de manera leve al proceso.

Tabla 3-6Valoración de confidencialidad

- **Integridad:** La propiedad de salvaguardar la exactitud e integridad de los activos.

Criterio	Nivel	Definición
3	Alto	La pérdida de exactitud y estado completo de la información y de los métodos de procesamientos impacta negativamente a la institución.
2	Medio	La pérdida de exactitud y estado completo de la información y de los métodos de procesamientos impacta negativamente de manera importante al proceso.
1	Bajo	La pérdida de exactitud y estado completo de la información y de los métodos de procesamientos impacta negativamente de manera leve al proceso.

Tabla 3-7Valoración de integridad

- **Disponibilidad:** Garantizar que los usuarios autorizados tengan acceso a los activos de información cada vez que los requieren.

Criterio	Nivel	Definición
3	Alto	La falta de la información impacta negativamente a la institución.
2	Medio	La falta de la información impacta negativamente de manera importante al proceso.
1	Bajo	La falta de la información impacta negativamente de manera leve al proceso.

Tabla 3-8Valoración de disponibilidad

3.10 Valoración del riesgo.

Continuando con el modelo propuesto para desarrollar la fase de plan de un SGSI, se llega a la etapa en donde se concentra la mayor parte de la adaptación.

Por las razones explicadas en el capítulo de adaptación a continuación se aplicará el Paso 2 de la MVR, Identificación de Amenazas

3.10.1 Identificación de amenazas

Iniciar la identificación de amenazas no es una tarea fácil debido a que existen muchos tipos de ellas, por esto se recomienda usar listas de amenazas potenciales comunes para organizaciones que trabajan con ambientes TIC, estas servirán como base para desarrollar este paso.

Para este caso usamos las listas de amenazas comunes del Anexo C del estándar ISO/IEC 27005 que pueden servir como base para cualquier organización que trabaje en ambientes TIC.

Con los miembros de la organización se seleccionaron en las tablas 3-9 y 3-10 aquellas amenazas potencialmente peligrosas para los sistemas de información.

TIPO	AMENAZA
Daño Físico	Fuego
	Daño causado por agua
	Contaminación
	Accidentes mayores
	Destrucción de equipo o Datos
	Polvo, corrosión, congelamiento
Eventos Naturales	Fenómenos climáticos
	Fenómenos sísmicos
	Fenómenos volcánicos
	Inundaciones
Pérdida de servicios esenciales	Fallos en el aire acondicionado o sistema de suministro de agua
	Pérdida del suministro eléctrico
	Fallos en sistemas de telecomunicaciones
Perturbaciones por radiación	Radiación electromagnética
	Radiación térmica
	Pulsos electromagnéticos
Exposición de la información	Código malicioso
	Espionaje remoto
	Espionaje
	Robo de datos o documentos
	Robo de equipos
	Recuperación de información en medios reciclados o desechados
	Revelación de información
	Datos de fuentes no confiables
	Manipulación indebida de hardware
	Manipulación indebida de software
	Detección de ubicación
Fallas técnicas	Falla en equipos
	Mal funcionamiento de equipos
	Saturación del sistema de información
	Mal funcionamiento de software
	*Falta de mantenimiento del sistema de información
Acciones no	Uso no autorizado de equipos

autorizadas	Copia no autorizada de software
	Uso de software falsificado
	Corrupción de datos
	Procesamiento ilegal de datos
Compromiso de funciones	Errores de operador
	Abuso de privilegios
	Forja de derechos
	Negación de acciones
	Indisponibilidad del personal

Tabla 3-9 Amenazas comunes en ambientes TIC. ISO/IEC 27005:2008.

Se debe tener especial atención en las fuentes de amenazas humanas, la tabla siguiente muestra amenazas de tipo humano más comunes.

FUENTE DE AMENAZA	MOTIVACION	AMENAZA
Hacker - Cracker	*Reto *Egocentrismo *Rebeldía	*Ingeniería Social *Intrusiones en el sistema *Robo de información *Atenta contra la integridad de la información *Acceso no autorizado al sistema
Criminal Informático	*Destrucción de Información *Revelación ilegal de información *Lucro *Alteración de datos no autorizada	*Crimen Informático (Ciberacoso) *Reproducción, interpretación e intercepción de información *Spoofing (un atacante se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación)
Espionaje Industrial (Competencia, Gobiernos)	*Ventaja Competitiva *Espionaje económico	*Explotación económica *El robo de información *Intrusión en la privacidad personal *Ingeniería social *Penetración del sistema

		*Acceso no autorizado al sistema (Acceso no autorizado a información clasificada, propietaria o a la tecnología relacionada.)
Intrusos (Personas poco entrenadas, maliciosas, negligentes, fraudulentas, empleados despedidos o descontentos)	*Curiosidad *Egocentrismo *Inteligencia *Lucro *Venganza * Errores sin intención y omisiones. (Errores de entrada de datos o de programación)	*Asalto a un empleado *Chantaje *Acceso a Información propietaria *Fraude y robo *Entrada falsificadas, datos corruptos *Interceptación *El código malicioso (por ejemplo, virus, troyanos) *Venta de información personal *errores del sistema *Intrusiones en el Sistema *sabotaje del sistema *Acceso no autorizado del sistema

Tabla 3-10Amenazas humanas comunes en ambientes TIC. ISO/IEC 27005:2008

En este documento a manera de ejemplo y para que el lector comprenda la forma como se realiza el proceso y la consignación de datos usaremos nombres genéricos para las amenazas de la siguiente forma:

Amenaza
Amenaza 1
Amenaza 2
Amenaza 3
Amenaza 4
Amenaza 5
Amenaza 6
Amenaza 7
Amenaza 8

Tabla 3-11Amenazas Identificadas

3.10.2 Identificación de Vulnerabilidades

Para este paso, al igual que el anterior, se recomienda usar tablas de vulnerabilidades comunes para organizaciones que trabajan en ambientes TIC lo cual facilita el proceso de identificación. El Anexo D del estándar ISO/IEC 27005 sirve como base para iniciar este paso.

Para este caso los miembros de la organización seleccionaron las vulnerabilidades presentes en los sistemas de información, pero por motivos de seguridad en este documento tendrán los siguientes nombres genéricos.

Vulnerabilidad
Vulnerabilidad 1
Vulnerabilidad 2
Vulnerabilidad 3
Vulnerabilidad 4
Vulnerabilidad 5
Vulnerabilidad 6

Tabla 3-12Vulnerabilidades y amenazas asociadas

Después de haber identificado las vulnerabilidades presentes en la organización, lo más importante es relacionar cada vulnerabilidad con la amenaza que la puede explotar, a continuación se muestra una tabla creada para hacer la relación de amenazas y vulnerabilidades que puede ser usada para mostrar los resultados de este paso y reflejarlos en el documento entregable correspondiente.

Vulnerabilidad identificada	Amenaza Relacionada	Tipo Fuente de Amenaza
Vulnerabilidad 1	Amenaza 1	Entorno
Vulnerabilidad 2	Amenaza 3	Humana
Vulnerabilidad 3	Amenaza 8	Entorno
Vulnerabilidad 4	Amenaza 4	Humana
	Amenaza 5	Natural
Vulnerabilidad 5	Amenaza 8	Humana
	Amenaza 2	Natural
Vulnerabilidad 6	Amenaza 4	Humana

Tabla 3-13Relación de Vulnerabilidades y amenazas

Recordemos que una amenaza representa riesgo solamente cuando existe una vulnerabilidad en el sistema a la que pueda explotar. Como se puede observar, inicialmente se identificaron ocho amenazas potenciales, pero en la tabla anterior podemos ver que las amenazas 6 y 7 no se relacionan con ninguna vulnerabilidad del sistema de información, por lo que no representan riesgos y en adelante no se tendrán en cuenta.

El desarrollo de este paso dejó como aprendizaje que es posible identificar algunas amenazas que por alguna razón se escaparon en el proceso anterior, esto debido a que pueden surgir vulnerabilidades que no se puedan relacionar con ninguna de las amenazas identificadas anteriormente y cabe aclarar que toda vulnerabilidad debe estar relacionada con una amenaza, pues bien se debe entonces buscar esa relación y consignarla en la tabla anterior.

Debido a la gran cantidad de vulnerabilidades técnicas que puede tener un sistema de información, se recomienda en primer lugar cubrirlas a un nivel general y luego en la etapa de mejora del SGSI realimentar la lista de con vulnerabilidades más específicas de cada sistema, para ello se puede acudir a ayudas como National Vulnerabilities Database [30] creada por el NIST que es una herramienta web con una vasta base de datos sobre vulnerabilidades técnicas.

3.10.3 Análisis de Controles

Como se propuso en el capítulo de adaptación, para facilitar la identificación de controles o medidas de seguridad existentes se recomienda usar la tabla 3-3 de la MVR.

Comúnmente las organizaciones que aún no han implantado un SGSI no tienen controles formalmente establecidos, pero tienen medidas de seguridad. Se recomienda comparar dichas medidas con controles del estándar ISO/IEC 27002:2013 para que la organización comprenda cuales de sus medidas actuales son controles o están cerca de serlo y las que definitivamente no se pueden considerar como control. La siguiente tabla muestra cómo se puede consignar los datos de una forma organizada y poder presentarlos en el documento entregable correspondiente.

Área de Seguridad	Control o medida de seguridad	Equivalencia con controles de ISO/IEC 27002:2013
Seguridad Administrativa y gerencial	Control 1	Buscar controles en el estándar ISO/IEC 27002:2013 similares a las medidas de seguridad existentes en la organización.
Seguridad Operacional	Control 2	
Seguridad Técnica	Control 3	
Seguridad Técnica	Control 4	
Seguridad Operacional	Control 5	

Tabla 3-14Controles existentes

3.10.4 Determinación de Probabilidad

Para aplicar el método propuesto en el artículo "Risk Assessment Instructions" de Virginia Information Technologies Agency (VITA), se debe definir los criterios de valoración para la ocurrencia de cada amenaza y la efectividad de controles existentes. Para crearlos se recomienda tener en cuenta la información disponible en la organización como reportes de incidentes o monitoreo para que la valoración sea consecuente en cada caso particular.

En este caso los criterios de probabilidad de ocurrencia se crearon teniendo en cuenta la capacidad de la fuente de amenaza o la ocurrencia de amenazas en los últimos tres años puesto que es la información con la que cuenta la organización. Para valorar la efectividad de los controles o medidas de seguridad se tuvo en cuenta registros acerca de la disminución del impacto de las amenazas desde la implementación del control. Cabe resaltar que estos criterios pueden servir como base para adaptarlos a otra organización. Los criterios son los siguientes:

Ocurrencia de las amenazas		
Bajo	**Medio**	**Alto**
La fuente de amenaza carece de capacidad o No se ha registrado ocurrencia en los últimos tres años	La fuente de amenaza tiene capacidad para vulnerar la seguridad o se ha registrado algunas ocurrencias en los últimos tres años	La fuente de amenaza tiene capacidad considerable para vulnerar la seguridad o se ha registrado varias ocurrencias en los últimos tres años

Tabla 3-15Criterios de valoración de efectividad de controles

Efectividad de los Controles		
Bajo	**Medio**	**Alto**
Existen muy pocos registros en la disminución del impacto de las amenazas desde la implementación del control o medida de seguridad	Existen algunos registros de disminución en el impacto de las amenazas desde la implementación del control o medida de seguridad	Existen registros de disminución en el impacto de las amenazas desde la implementación del control o medida de seguridad

Tabla 3-16Criterios de valoración de ocurrencia de amenazas

Generalmente en organizaciones que aún no cuentan con un SGSI puede que no existan registros documentados sino testificaciones por parte de los miembros y aunque son pruebas subjetivas se pueden tener en cuenta después de hacer un análisis de las mismas e indagar al personal en busca de evidencias.

Para obtener la valoración de la Probabilidad de Ocurrencia de amenazas se usa la siguiente tabla tomada de la MVR, teniendo en cuenta las valoraciones de ocurrencia de amenazas y efectividad de controles.

Efectividad de controles existentes	**Probabilidad de ocurrencia de las amenazas**		
	Bajo	**Medio**	**Alto**
Alto	Bajo	Bajo	Medio
Medio	Bajo	Medio	Alto
Bajo	Medio	Alto	Alto

Tabla 3-17Determinación de la probabilidad.

Para documentar los resultados obtenidos en el entregable respectivo se creó la siguiente tabla que relaciona a cada amenaza con su respectiva valoración de ocurrencia de la amenaza y la efectividad de los controles existentes, como se muestra a continuación en la tabla 3-18

Amenaza	Ocurrencia de la Amenaza	Control Relacionado	Efectividad del Control	Probabilidad
Amenaza 1	Alta	Control 2	Media	Alto
Amenaza 2	Media	Control 5	Baja	Alto
Amenaza 3	Media	Control 3	Media	Medio
Amenaza 4	Baja	No existe	Baja	Medio
Amenaza 5	Media	Control 1	Alta	Bajo
Amenaza 8	Baja	Control 4	Alta	Bajo

Tabla 3-18 Probabilidad de Ocurrencia de amenazas

3.10.5 Análisis de impacto

Para realizar este paso se usará los datos de criticidad, obtenidos anteriormente en la MAA de la etapa Análisis de activos, pero como se propuso en la adaptación, se procesara esta información de la siguiente forma.

Se relaciona a cada amenaza con el/los activos a los que puede afectar. Para ello se creó la siguiente tabla. En ella se puede observar que se hizo un promedio de las criticidades de los activos en cada amenaza, esto nos permite seguir trabajando con el mismo número de valoraciones que teníamos en los pasos anteriores, de lo contrario por cada relación amenaza-activo se aumenta en uno el número de valoraciones de impacto debido a que una amenaza afecta a varios activos a la vez si se materializa. De acuerdo a la tabla, la columna Impacto es el promedio de la criticidad de los activos relacionados con una amenaza como se observa a continuación.

Amenaza	Activos Asociados	Criticidad	Impacto
Amenaza 1	Activo 3	2	Alto
	Activo 2	3	
	Activo 1	3	
Amenaza 2	Activo 1	3	Alto
Amenaza 3	Activo 2	2	Medio
Amenaza 4	Activo 2	3	Medio
	Activo 5	1	

Amenaza 5	Activo 6	1	Bajo
Amenaza 8	Activo 4	2	Bajo
	Activo 6	1	

Tabla 3-19 Impacto de las amenazas

La interpretación del nivel de impacto se obtiene con la siguiente tabla tomada del Paso 6 de la MVR.

Nivel de impacto	Definición de impacto
Alto	Genera altos costos y pérdida de activos o recursos. Violaciones que impiden significativamente realizar la misión de la organización o afectan la reputación o intereses de la misma. Incluso puede causar muertes humanas o serias lesiones personales.
Medio	Genera costos y pérdida de activos o recursos moderada. Violaciones que afectan la realización de la misión de la organización o afectan la reputación o intereses de la misma. Podría causar lesiones personales
Bajo	Genera algunos costos por perdida daño de activos o recursos.

Tabla 3-20 Definición de los niveles de impacto

3.10.6 Determinación del riesgo

Siguiendo el modelo propuesto a continuación se aplica el método del Paso 7 de la MVR. Para ello es necesario hacer una multiplicación de la probabilidad de ocurrencia (Paso 5), con el impacto (Paso 6). Para obtener la valoración del nivel de riesgo se usa la siguiente tabla tomada de la MVR.

Probabilidad de ocurrencia de una amenaza	Impacto		
	Bajo (10)	**Medio(50)**	**Alto (100)**
Alta (1.0)	Bajo 10x1.0= 10	Medio 50x1.0= 50	Alto 100x1.0= 100
Media (0.5)	Bajo 10x0.5= 5	Medio 50x0.5= 25	Medio 100x0.5= 50
Baja (0.1)	Bajo 10x0.1= 1	Bajo 50x0.1= 5	Bajo 100x0.1= 10

Tabla 3-21 Calculo del nivel de Riesgos

Dependiendo del valor que resulte al hacer la multiplicación mencionada se determina el nivel de riesgo de acuerdo a la siguiente escala.

Nivel	Valores entre
Alto	1 y 10
Medio	11 y 50
Bajo	51 y 100

Tabla 3-22 Escala del nivel de riesgos.

La interpretación del nivel de riesgo para conocer las medidas a tomar se hace con la siguiente tabla propuesta en la MVR.

Nivel de riesgo	Acciones Necesarias
Alto	Si el riesgo calculado es alto, el sistema puede continuar operando, pero el plan de medidas correctivas debe ser implementado rápidamente.
Medio	Las acciones correctivas son necesarias y el plan debe ser desarrollado e implementado en un periodo de tiempo razonable.
Bajo	Si el nivel de riesgo es bajo, se debe determinar si hay acciones correctivas necesarias o si se acepta el riesgo.

Tabla 3-23 Definición de los niveles de riesgo

Para este caso se creó la siguiente tabla que encapsula los resultados de la determinación de riesgos, la cual puede ser usada para documentar el entregable respectivo.

Amenaza	Probabilidad	Impacto	Nivel de Riesgo
Amenaza 1	Alta (1,0)	Alto (100)	Alto (100)
Amenaza 2	Alta (1,0)	Alto (100)	Alto (100)
Amenaza 3	Media (0,5)	Medio (50)	Medio (25)
Amenaza 4	Media (0,5)	Alto (100)	Medio (50)
Amenaza 5	Baja (0,1)	Medio (50)	Bajo (5)
Amenaza 8	Baja (0,1)	Alto (100)	Bajo (10)

Tabla 3-24 Determinación del riesgo

Con esto se completa la etapa de valoración de riesgos y es necesario realizar el entregable de esta etapa con los resultados obtenidos.

3.11 Selección de objetivos de control y controles.

3.11.1 Plan de tratamiento de riesgos

Siguiendo con la secuencia de la adaptación propuesta se definió el plan de tratamiento de riesgos inicialmente definiendo junto con la dirección el siguiente criterio de aceptación:

“La organización asumirá o aceptará aquellos riesgos que obtuvieron un nivel bajo en la etapa de valoración de riesgos o aquellos a los que se les ha implementado controles efectivos. Se realizaran valoración es de estos riesgos para verificar que su nivel se mantenga bajo”

Cabe resaltar que cada organización puede definir su criterio de aceptación de riesgos, pudiendo usar el mencionado o definirlo de acuerdo a su situación particular.

Por otra parte existen riesgos que para este caso son responsabilidad de otras áreas de la Universidad del Cauca, lo que significa que están tercerizados, para los demás riegos se tomó la opción de mitigarlos, ya que ningún riesgo se puede eliminar debido a que la única forma es eliminando el activo como se explicó antes.

De esta forma se generó la siguiente tabla que se puede usar para mostrar los resultados en el entregable correspondiente.

Amenaza	Riesgo	Opción de Tratamiento
Amenaza 1	Alto	Mitigar
Amenaza 2	Alto	Transferir
Amenaza 3	Medio	Mitigar
Amenaza 4	Medio	Mitigar
Amenaza 5	Bajo	Asumir
Amenaza 8	Bajo	Asumir

Tabla 3-25Plan de tratamiento de riesgos

3.11.2 Controles y objetivos de control seleccionados

El siguiente paso es determinar los controles más adecuados para aquellos riesgos cuya opción de tratamiento fue mitigar. Para ello nos remitimos al estándar ISO/IEC 27002:2013 en donde es necesario analizar uno a uno los controles con el fin de determinar cuáles son aplicables a la organización, para los que son aplicables se consignan como se muestra en la tabla 3-26 la cual se puede usar para mostrar los resultados en el entregable correspondiente. Para aquellos que no son aplicables se consignan en otra tabla justificando la razón de su exclusión, como por ejemplo que el control ya fue implementado o que no existe ningún riesgo que se pueda mitigar con dicho control, se puede usar el modelo de la tabla 3-27. Si después de hacer este análisis aún existen riesgos que aún no tienen un control relacionado, es labor obligatoria crear él o los controles necesarios.

Objetivo de Control	Control	Amenaza a mitigar
6.2 Dispositivos móviles y teletrabajo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles	6.2.1 Política para dispositivos Móviles: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	Amenaza 3
	6.2.2 Teletrabajo: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	Amenaza 3
8.3 Manejo de medios: Evitar la divulgación, la modificación el retiro o la destrucción no autorizados de información almacenada en los medios	8.3.2 Disposición de los medios: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	Amenaza 1

Tabla 3-26Selección de objetivos de control y controles

Objetivos de Control	Control	Justificación de la exclusión
11.1: Áreas seguras: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.	11.1.1 Perímetro de seguridad Física: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información	El control ya se ha implementado

11.2 Equipos: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización	11.2.6 Seguridad de equipos y activos fuera de las instalaciones: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	La organización no tiene equipos fuera de las instalaciones de la misma

Tabla 3-27Controles no aplicables a la organización

3.11.3 Declaración de aplicabilidad (SOA)

Con la elaboración de las tablas recomendadas en este trabajo es fácil la construcción del SoA, puesto que las tablas ya están creadas, a continuación las recordamos para que sean consignadas en el documento entregable correspondiente.

- Tabla 3-14. Controles Existentes
- Tabla 3-26. Selección de objetivos de control y controles
- Tabla 3-27. Controles no aplicables a la organización

Con esto finalizamos la fase de plan del SGSI ajustando la adaptación propuesta al caso real, Procedimiento Gestión de Servicios y servidores de internet de la Universidad del Cauca. El proceso desarrollado muestra que sí es posible aplicar la adaptación de la metodología de valoración de riesgos NIST SP 800-30 en la fase de plan de un SGSI basado en la norma ISO/IEC 27001:2013 en una organización que trabaja en ambientes TIC, respondiendo a la pregunta planteada inicialmente.

Por último se muestra un resumen de la fase de plan del SGSI desarrollada en la figura 3-6 y un resumen del proceso desarrollado para realizar la valoración de riesgos con la adaptación propuesta en la figura 3-7 y las tablas del ejemplo genérico creado para hacer más fácil la comprensión del proceso.

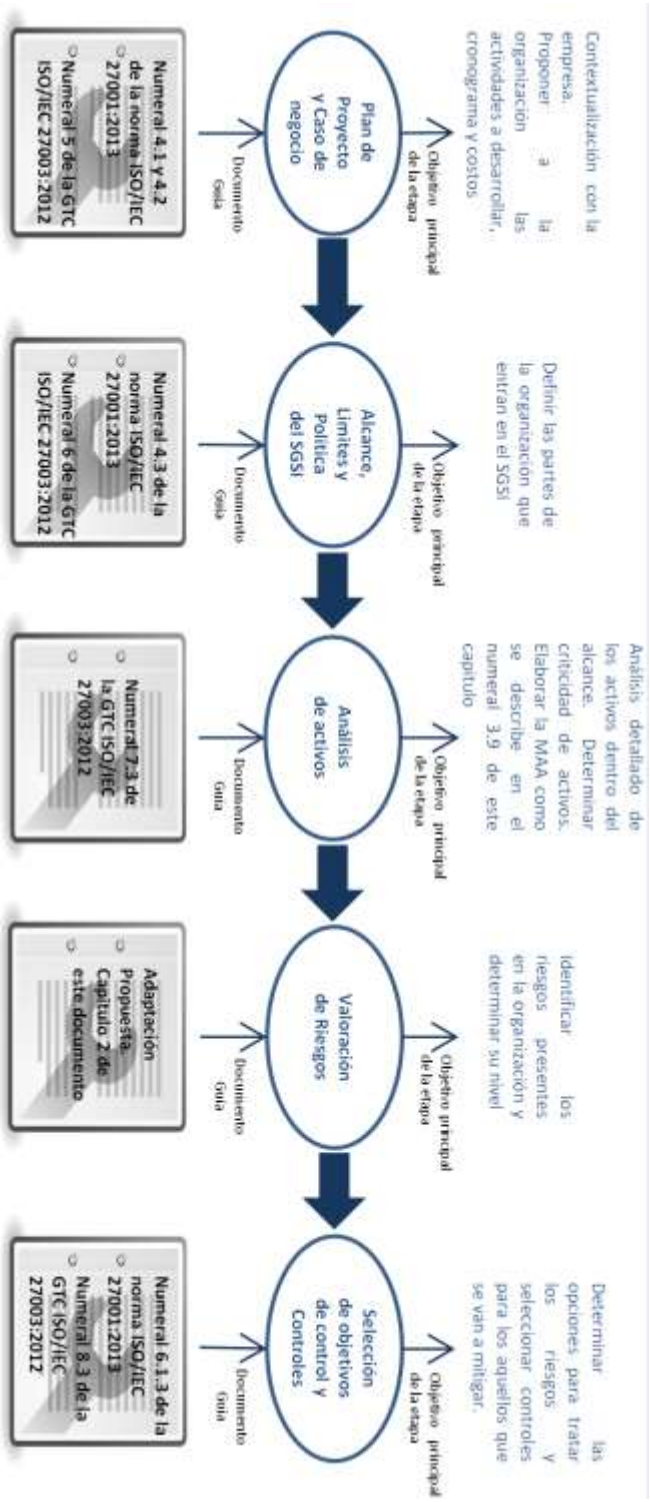

Figura 3-6 Resumen fase plan SGSI

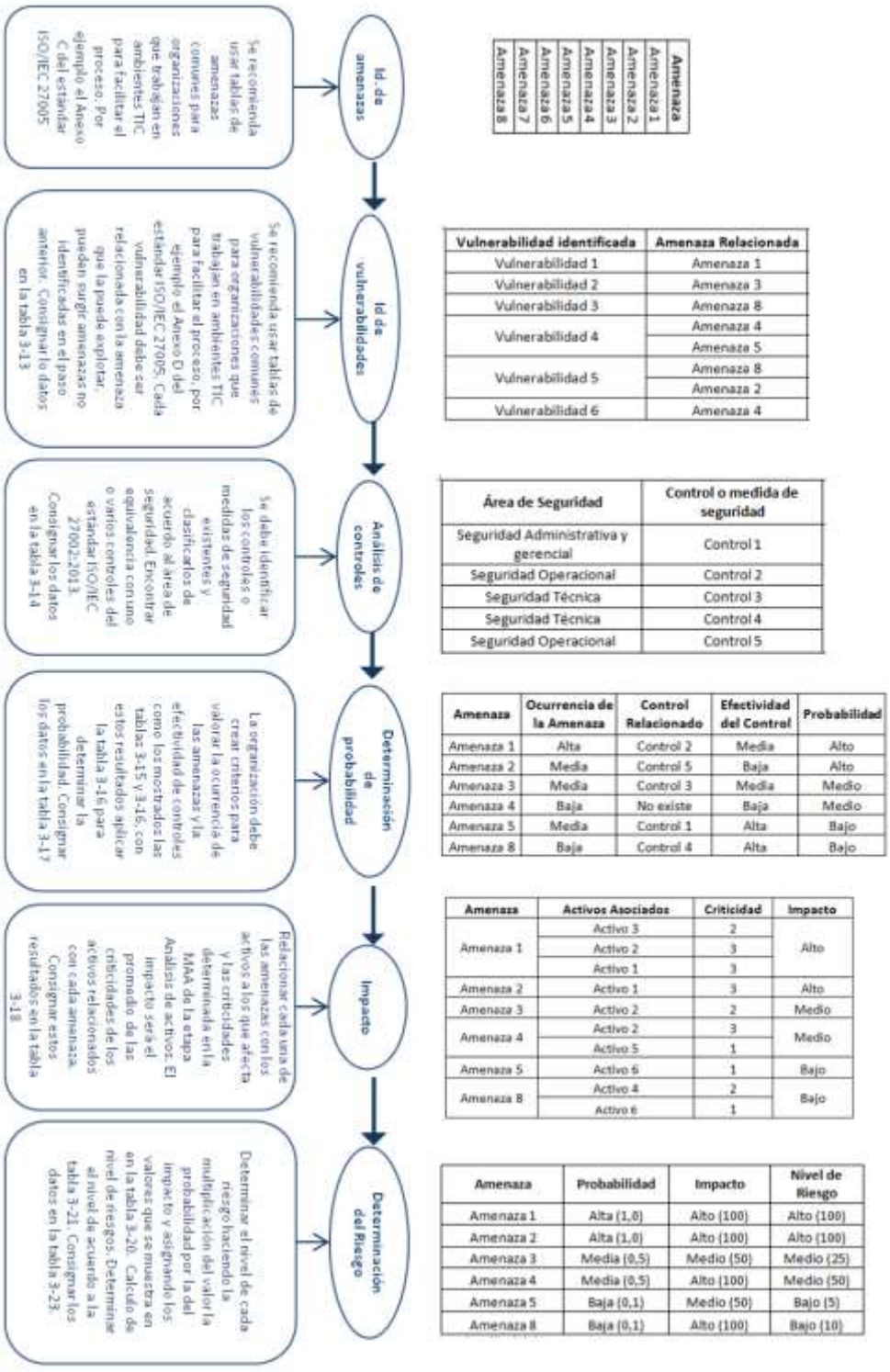

Figura 3-7 Valoración de riesgos con la adaptación propuesta

4. Conclusiones y trabajos futuros

4.1 Conclusiones

- La adaptación propuesta En este trabajo permitió identificar y seleccionar 8 objetivos de control y 17 controles tomados del estándar ISO/IEC 27002:2013. Además se crearon 4 controles adicionales para completar la fase plan del SGSI.

- Los lineamientos planteados en este trabajo sirven de base para la implementación de trabajos futuros, en empresas que trabajan en ambientes TIC

- Los resultados del trabajo permitieron evidenciar que el caso de estudio no está en conformidad totalmente con la Norma ISO/IEC 27001 pero existen las condiciones mínimas y necesarias para iniciar la implementación de un SGSI basado en la norma ISO/IEC 27001.

- De acuerdo a los resultados obtenidos en la fase de valoración de riesgos, se evidencia que es pertinente la implantación de un SGSI para el caso de estudio.

4.2 Trabajos futuros

- Desarrollar las siguientes fases del SGSI, ejecución, revisión y mejora para el caso de estudio, a partir de los resultados obtenidos en este trabajo.

- Verificar que la adaptación propuesta se puede aplicar a una organización de otros sectores como el bancario.

- Elaborar un plan de continuidad del negocio a partir de los resultados obtenidos.

Bibliografía

[1] ISO, ISO/IEC 27000:2014 Information technology — Security techniques — Information security management systems - Overview and vocabulary, 2014.

[2] A. G. Alexander, Diseño de un sistema de gestion de seguridad de informacion, Bogotá, Colombia: Alfa Omega Colombiana S.A., 2007.

[3] ISO, Norma técnica Colombiana NTC - ISO/IEC 27001:2013 TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. REQUISITOS, Bogotá DC: icontec, 2013.

[4] ISOTools Excellence, «pmg-ssi,» 2015. [En línea]. Available: http://www.pmg-ssi.com/2015/01/la-serie-iso-27000/. [Último acceso: 15 09 2015].

[5] advisera, «27001Academy,» 2015. [En línea]. Available: http://advisera.com/27001academy/es/que-es-iso-27001/. [Último acceso: 16 09 2015].

[6] «iso27000.es,» [En línea]. Available: http://www.iso27000.es/sgsi.html.

[7] DivTIC - Universidad del Cauca, «www.unicauca.edu.co,» 04 09 2015. [En línea]. Available: http://ublogs.unicauca.edu.co/. [Último acceso: 15 11 2015].

[8] ISO, GUÍA TÉCNICA COLOMBIANA GTC - ISO/IEC 27003, TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. GUÍA DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, Bogotá DC: Icontec, 2012.

[9] INTECO, «incibe.es,» 16 08 2012. [En línea]. Available: http://es.slideshare.net/kramerg/guia-apoyo-sgsi. [Último acceso: 16 09 2015].

[10] Fondo de Tecnologías de la información y las Comunicaciones, «Metodología de gestión del riesgo modelo de seguridad de la información para la estrategia de gobierno en línea,» Bogota, D.C., 2010.

[11] National institute of standards and technology, NIST Special Publication 800 - 30, 2002.

[12] National institute of standards and technology, NIST Special Publication 800-30, 2002.

[13] Fondo de Tecnologías de la información y las Comunicaciones, «Metodología de gestiuón del riesgo modelo de seguridad de la información para la estrategia de gobierno en línea,» Bogota, D.C., 2010.

[14] INTECO Instituto nacional de tecnologías de la comunicación, «www.incibe.es,» 2010. [En línea]. Available: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf. [Último acceso: 15 diciembre 2015].

[15] F. G. F. J. P. M. P. M. T. B. Cesar Pardo, «Método de integracion para soportar la armonización de múltiple modelos y estándares,» de *XVI jornadas de ingenieria del software y bases de datos SISTEDES 2011*, A Coruña, España, 2011.

[16] G. Toth, implementacion de la guia NIST SP 800-30 mediante la utilizacion de OSSTMM, Neuquen, Argentina: Universidad Nacional de Comahue, 2014.

[17] S. I. G. Sanchez, Propuesta de aplicación de una metodología para la seguridad informática en la división de ciencias básicas, Mexico DF: Universidad nacional autónoma de méxico, 2009.

[18] M. E. V. S. M. I. Vasco Aguas, Plan de gestóin de seguridad de la información basada en TICS para la facultad de ingeniería de sistemas de la escuela politécnica nacional, Quito, Ecuador: Escuela Politécnica nacional, 2009.

[19] P. H. Ohtoshi, analise comparativa de metodologias de gestao e d analise de riscos soba ótica da norma NBR-ISO/IEC 27005, Brasilia, Brasil: Universidad de brasilia, 2008.

[20] V. N. A. Serrano, Desarrollo de una aplicacion para la gestión de riesgops en los sistemas de información utilizando la guía metodológica NIST SP 800-30 caso práctico: "Liceo del Valle", Sangolqui, Ecuador : Escuela Politécnica del ejército, 2007.

[21] Z. O. B. A. Ramirez Castro, Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios, Bogotá, Colombia: Universidad distrital Francisco José de Caldas , 2011.

[22] A. Abril, Análisis de riesgos en seguridad de la información, tunja, Colombia: Universidad Juan de Castellanos, 2013.

[23] D. F. E. T. J. P. Martinez Pulido, Gestión del riesgo en la seguridad de la información con base en la norma ISO/IEC 27005:2011, proponiedo una adaptación de la metodología OCTAVE S, Popayán, Colombia: Universidad del Cauca, 2014.

[24] R. E. Stake, The art of case study research, Thousand Oaks, CA: Sage, 1995.

[25] *Ley 872 de 2003 Nivel Nacional,* Bogotá: Diario Oficial 45418 de enero 2 de 2004, 30 de diciembre 2003.

[26] Universidad del Cauca, *Manual de procesos y procedimientos,* Popayán, Abril 01 de 2011.

[27] División de tecnologías de la información y comunicación - Universidad del Cauca, 2015. [En línea]. Available: http://ublogs.unicauca.edu.co/sgc-tics/. [Último acceso: 15 octubre 2015].

[28] Fondo de tecnologías de la información y las comunicaciones, *Anexo 5: formato política SGSI modelo de seguridad de la información para la estrategia de gobierno en líneas,* Bogotá D.C., 2011.

[29] A. G. Alexander, Diseño de un sistema de gestion de seguridad de informacion, Bogotá, Colombia: Alfa Omega Colombiana S.A., 2007.

[30] NIST, «National vulnerabilities database,» [En línea]. Available: https://nvd.nist.gov/. [Último acceso: 2 noviembre 2015].

[31] ISO, ISO/IEC 27000:2014 Information technology — Security techniques — Information security management systems - Overview and vocabulary, 2014.

[32] G. A. Toth, Implementación de la guía NIST SP 800-30 mediante la utilización de OSSTMM, Neuquén, Argentina: Universidad Nacional de Comahue, 2014.

[33] S. I. Gaínza Sánchez , Propuesta De Aplicación De Una Metodología Para La Seguridad Informática En La División De Ciencias Básicas, México, D.F.: Universidad Nacional Autónoma de México, 2009.

[34] M. I. Vasco Aguas y M. E. Verdezoto Saltos, Plan De Gestión De Seguridad De La Información Basada En Tics Para La Facultad De

Ingeniería De Sistemas De La Escuela Politécnica Nacional, Quito, Ecuador: Escuela Politécnica Nacional, 2009.

[35] P. Hideo Ohtoshi, Análise Comparativa de Metodologias de Gestão e de Análise de Riscos sob a Ótica da Norma NBR-ISO/IEC 27005, Brasilia, Brasil: Universidad de Brasilia, 2008.

[36] V. N. Avalos Serrano, Desarrollo de una aplicación para la gestión de riesgos en los sistemas de información utilizando la guía metodológica NIST SP 800-30 caso práctico: “Liceo Del Valle“, Sangolquí, Ecuador: Escuela Politécnica del Ejército, 2007.

[37] A. Ramírez Castro y Z. Ortiz Bayoma, Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios, Bogotá, Colombia: Universidad Distrital Francisco Jose de Caldas, 2011.

[38] A. Abril, Análisis De Riesgos En Seguridad De La Información, Tunja, Colombia: Universidad Juan de Castellanos, 2013.

[39] J. P. Martínez Pulido y D. F. Espinoza Tafur, Gestión del riesgo en la seguridad de la información con base en la norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la metodología OCTAVE-S. Caso de estudio: Proceso de inscripciones y admisiones en (DARCA) de la universidad del Cauca, Popayán, Colombia: Universidad del Cauca, 2014.

[40] ICONTEC, "Estándar Internacional GTC-ISO/IEC 27003:2012 Information Technology -- security techniques -- Information Security Management System Implementation Guidance", 2013.

[41] NIST, "NIST special publication 800-30: Risk Management Guide for Information Technology Systems", 2002.

[42] ICONTEC, Estándar Internacional NTC ISO/IEC 27005:2011 Information technology — Security techniques — information security risk management (second edition), ed, 2011.

[43] ICONTEC, "Estándar Internacional ISO/IEC 27002:2013 Information Technology -- security techniques -- Code of Practice for Information Security Controls", 2013.

[44] ISO, ISO 31000:2009, Risk management – Principles and guidelines, 2009.

[45] Computer Emergency Response Team, Operationally Critical Threat, Asset and Vulnerability Evaluation, 2001.

[46] Computer Emergency Response Team, MEHARI, 2010.

[47] Consejo Superior de Administración Electrónica, MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, 2012.

[48] Central Computer and Telecommunications Agency, CRAMM (CCTA Risk Analysis and Management Method), 2002.

[49] Direction Centrale de la Sécurité des Systèmes d'Information, EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), 2000.

[50] «business901,» [En línea]. Available: http://business901.com/blog1/gemba-coach-talks-pdca/.

[51] ISO, "Estándar Internacional ISO/IEC 27004:2009 Information technology -- Security techniques -- Information security management -- Measurement, 2009.

[52] Universidad del Cauca, «www.unicauca.edu.co,» 19 diciembre 2014.

[En línea]. Available: http://www.unicauca.edu.co/prlvmen/subprocesos/mapa-de-procesos. [Último acceso: 20 09 2015].

[53] NIST, «national vulnerability database,» [En línea]. Available: nvd.nist.gov.

[54] ICONTEC, "Estándar Internacional ISO/IEC 27001:2013 Information Technology -- security techniques -- Specification for an information Security Management System, 2013.

[55] Virginia Information Technologies Agency (VITA), "Appendix D - Risk Assessment Instructions," in *Information Technology Risk Management guideline*, 2006.

[56] Servicio geológico Colombiano, «http://seisan.sgc.gov.co,» [En línea]. Available: http://seisan.sgc.gov.co/RSNC/index.php?option=com_content&view=article&id=50&Itemid=62. [Último acceso: 02 03 2016].

[57] Servicio Geológico Colombiano, «http://www2.sgc.gov.co,» [En línea]. Available: http://www2.sgc.gov.co/Popayan/Volcanes/Volcan-Purace/Mapa-de-amenaza.aspx.