ANÁLISIS Y EVALUACIÓN DE RIESGOS, DE LOS ACTIVOS DE INFORMACIÓN DE LA DIRECCIÓN EJECUTIVA SECCIONAL DE ADMINISTRACIÓN JUDICIAL DE TUNJA - DESAJT, ADOPTANDO UNA METODOLOGÍA DE GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN

TERESA HERMINIA JIMÉNEZ FONSECA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍAS (ECBTI)
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CEAD TUNJA
2018

ANÁLISIS Y EVALUACIÓN DE RIESGOS, DE LOS ACTIVOS DE INFORMACIÓN DE LA DIRECCIÓN EJECUTIVA SECCIONAL DE ADMINISTRACIÓN JUDICIAL DE TUNJA - DESAJT, ADOPTANDO UNA METODOLOGÍA DE GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN

TERESA HERMINIA JIMÉNEZ FONSECA

Monografía para optar el título de Especialista en Seguridad Informática

Director
FREDY ALEXANDER CASTELLANOS ÁVILA
Ingeniero Especialista en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍAS (ECBTI)
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CEAD TUNJA
2018

Nota de Aceptación

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Tunja, Noviembre de 2018

DEDICATORIA

Dedico la presente monografía a mi familia por su gran apoyo, el cual se constituyó en el ímpetu para cumplir esta meta profesional y de esta forma, seguir escalando a nivel intelectual y humano.

Y en especial, dedico este logro a mi esposo, por su orientación, solidaridad, comprensión y constante motivación durante el transcurso de mis estudios de la especialización y la culminación de la misma.

AGRADECIMIENTOS

Agradezco a Dios por ser la fuente espiritual en este caminar y el permitirme llegar a obtener este título, como bendición para toda mi familia.

En segundo lugar, agradezco a los tutores y director de proyecto de la Especialización en Seguridad Informática de la Universidad Nacional Abierta y a Distancia UNAD, por su valiosa orientación académica, por los valores y principios humanos que han aportado al aprendizaje y enseñanza en mi calidad de estudiante, de tan prestigiosa Institución de Educación Superior en Colombia.

RESUMEN

La presente monografía aborda el estudio de las metodologías de gestión de riesgos de sistemas de información: MAGERIT versión 3 y NIST SP800-30 revisión 1, que se destacan por proporcionar las actividades que le permiten a una organización conocer los riesgos que pueden generarse con el uso de los sistemas tecnológicos, de comunicaciones y el entorno asociado a su nivel de operación. Con los resultados de este estudio, de forma aplicada se ha tomado una organización con activos y sistemas de información específicos, con el objeto proponer la metodología de gestión de riesgos, que se ajusta a los requerimientos en materia de seguridad de la organización y determinar los riesgos a los que se encuentran sometidos sus activos a través del análisis y evaluación de los riesgos.

Con fundamento en lo anterior, esta monografía desarrolla los siguientes temas: en el primer capítulo se describe la estructura organizacional de la Dirección Ejecutiva Seccional de Administración Judicial de Tunja – DESAJT (organización tomada como caso de estudio), y la estructura de procesos de su Sistema Integrado de Gestión y Control de la Calidad y el Medio Ambiente – SIGCMA, obteniendo a través de sus procesos de apoyo el inventario de los activos de información más relevantes, mediante los cuales se soporta el funcionamiento operativo y la prestación de servicios de la organización.

En el segundo capítulo se estudian los aspectos más importantes de las metodologías de gestión de riesgos para sistemas de la información: MAGERIT versión 3 y NIST SP800-30 revisión 1, donde se exponen las actividades y procedimientos de cada metodología respecto del proceso de análisis y evaluación de riesgos. Como resultado de este estudio, se resaltan los aspectos más importantes de cada metodología en cuanto a objetivos de seguridad contemplados, la aplicación de gestión de riesgos sobre los activos de la organización, las tareas y subtareas de las actividades del análisis y evaluación de riesgos y los criterios de evaluación respecto de las amenazas, vulnerabilidades, la probabilidad, el impacto y el nivel del riesgo. Permitiendo de esta forma, establecer un cuadro comparativo de cada uno de estos aspectos, logrando seleccionar a la metodología MAGERIT versión 3, por su esquema de actividades y gran compatibilidad con el modelo actual de gestión de riesgos de la Dirección Ejecutiva Seccional de Administración Judicial de Tunja – DESAJT.

En el tercer capítulo se presenta la metodología MAGERIT versión 3, como la metodología que puede ser integrada al modelo actual de administración de riesgos de la Dirección Ejecutiva Seccional de Administración Judicial de Tunja – DESAJT. Esta integración puede llevarse a cabo mediante un “Proyecto de análisis de

riesgos” dentro de la organización; por lo cual, en esta sección se propone la guía para llevar a cabo el análisis y evaluación de riesgos, de los activos de información de la Dirección Ejecutiva Seccional de Administración Judicial de Tunja - DESAJT, mediante el desarrollo del “Proyecto de análisis de riesgos”, por lo que se describen cada una de las actividades preliminares que le permiten a la organización emprender el proyecto, realizar el análisis de riesgos y comunicar los resultados del mismo; logrando de esta forma con la ejecución de este proyecto que los objetivos de la presente monografía sean alcanzados y brinden un aporte fundamental para la gestión de riesgos en materia de seguridad de la información a la organización tomada en el presente estudio.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

INTRODUCCIÓN

A través de los años las organizaciones han adquirido tecnologías que le permitan optimizar e innovar sus procesos, con el principal objetivo de mejorar sus procedimientos y brindar una eficiente prestación del servicio a sus clientes y usuarios. No obstante de la mano de esta evolución, es conveniente que las organizaciones adopten estrategias en materia de seguridad de la información, que le permitan preservar la confidencialidad, integridad y disponibilidad, de los sistemas tecnológicos y de comunicaciones, mediante los cuales se almacena y procesa su información e intervienen en la misión y funciones del negocio.

Existen muchas estrategias en materia de Seguridad de la Información, que le permiten a las organizaciones identificar los riesgos a los que se encuentran expuestos sus activos de información y aún más, conocer el nivel de seguridad de cada uno de ellos. Como apoyo a esta gran iniciativa y con el objeto de iniciar este proceso dentro de una organización, se presenta como principal herramienta las metodologías de análisis y evaluación de riesgos para sistemas de información, que permiten llevar a cabo la identificación de riesgos para los activos de información de una entidad; partiendo de esta forma, el camino hacia la adopción y el fortalecimiento de estrategias de seguridad, que le permitirán a la organización prevenir y salvaguardar sus recursos de información.

Bajo este contexto y con el propósito de lograr que dentro de un entorno corporativo, con activos de información específicos, y sobre los cuales se consiga fortalecer los principios de seguridad de la información, es fundamental que la organización conozca e integre a su modelo de gestión, las actividades que le permitan analizar y evaluar los riesgos que puedan presentarse en los distintos niveles de funcionamiento y operación, de tal forma que se contribuya a garantizar la protección de los recursos (equipos, personas, infraestructura, etc.) que le permiten llevar a cabo el cumplimiento de sus objetivos.

De acuerdo con las anteriores consideraciones, en la presente monografía se realiza un reconocimiento de los activos de información de un entorno corporativo específico, como son los administrados por la Dirección Ejecutiva Seccional de Administración Judicial de Tunja – DESAJT, entidad tomada para efectuar el presente estudio–; paso seguido se realiza una revisión bibliográfica de las metodologías de gestión de riesgos para sistemas de información más reconocidas: MAGERIT versión 3 y NIST SP800-30 revisión 1, donde se realiza un estudio comparativo de las actividades de análisis y evaluación de riesgos y las características de cada una de ellas. Como resultado de esta revisión, se determina la metodología de gestión de riesgos para sistemas de información, que se ajusta

más al tipo de activos de información que posee la entidad y además cubra sus requerimientos en materia de seguridad de la información.

Finalmente de acuerdo con las actividades de análisis y evaluación de riesgos de la metodología seleccionada, se presentará una guía para el análisis y evaluación de riesgos que integre los procesos, procedimientos y servicios en los que intervienen los activos de información de la entidad.

1. TÍTULO

Análisis y evaluación de riesgos, de los activos de información de la Dirección Ejecutiva Seccional de Administración Judicial de Tunja - DESAJT, adoptando una metodología de gestión de riesgos de los sistemas de información.

2. DEFINICIÓN DEL PROBLEMA

2.1 ANTECEDENTES DEL PROBLEMA

Actualmente las organizaciones no dimensionan en su totalidad los riesgos a los que se encuentran expuestos sus activos de información, por el uso y funcionamiento de sus recursos tecnológicos y sistemas de información, sólo se es posible indagar al respecto, cuando se suscita un incidente que atenta contra la confidencialidad, integridad y disponibilidad de su información y los recursos y sistemas de información y comunicación que la apoyan.

Infortunadamente, esta concepción reside en la mayoría de organizaciones que le temen a reducir la brecha de desconocimiento frente a los aspectos que brinda la Seguridad de la Información y no consideran oportunamente integrar a su modelo organizacional, una estrategia que se ajuste a los requerimientos de seguridad y le permita identificar los puntos débiles y vulnerables presentes en sus activos de información.

2.2 FORMULACIÓN DEL PROBLEMA

Atendiendo que existen distintas metodologías reconocidas de gestión de riesgos, que permiten llevar a cabo el análisis y evaluación de riesgos para los sistemas de información y de comunicaciones, que contemplan los principios de confidencialidad, integridad y disponibilidad de estos recursos, se planea realizar un estudio que permita seleccionar y determinar ¿Qué metodología de gestión de riesgos de los sistemas de información, es aplicable, para elaborar una guía para el análisis y evaluación de riesgos de los activos de información de la Dirección Ejecutiva Seccional de Administración Judicial de Tunja – DESAJT?.

2.3 DESCRIPCIÓN DEL PROBLEMA

La problemática planteada en la presente monografía, se fundamenta en adoptar una metodología de gestión de riesgos que se ajuste a los activos de información de una organización específica y a las necesidades de seguridad que ésta requiere. Como apoyo de este estudio, se ha tomado la Dirección Ejecutiva Seccional de Administración Judicial de Tunja - DESAJT, entidad de la Rama Judicial, la cual posee un Sistema Integrado de Gestión y Control de Calidad y Medio Ambiente – SIGCMA, implementado bajo la norma ISO 9001:2008, mediante el cual realiza la

administración de riesgos, empleando una versión de la metodología de gestión de riesgos del Departamento Administrativo de la Función Pública (DAFP), que no contempla todos los aspectos que en materia de seguridad informática, requieren los sistemas de información y de comunicaciones de la entidad.

Puntualmente, la administración de riesgos de los activos de información y los recursos tecnológicos y de comunicaciones de la DESAJT, se ha orientado en identificar el riesgo según las no conformidades en cuanto a la calidad de la prestación del servicio, lo cual es válido y muy importante para una organización del estado; no obstante, únicamente se identifican los riesgos frente a la no disponibilidad del servicio; y no se consideran los demás elementos o activos de información, que eventualmente son vulnerables y están expuestos a ataques o incidentes de seguridad que atenten contra la confidencialidad e integridad de la información y los sistemas; de ahí, que se describe como problema, el que la organización no cuente con una guía y/o metodología de gestión de riesgos para los sistemas de información, que le permita identificar y determinar los riesgos que atentan contra todos los principios de la seguridad informática – la confidencialidad, disponibilidad e integridad y además esta metodología integre los procesos y procedimientos en los que intervienen sus activos de información.

3. JUSTIFICACIÓN

Existen distintas metodologías de gestión de riesgos para sistemas de información, que aunque tienen un propósito en común, es significativo para el desarrollo de esta monografía conocer cuáles son sus objetivos, fortalezas, debilidades, el ámbito de aplicación, los aspectos y criterios que abordan para efectuar el análisis y la evaluación de riesgos de los recursos tecnológicos a proteger en una organización.

Dentro de las metodologías de gestión de riesgos para los sistemas de información, que actualmente son las más reconocidas por su campo de aplicación y su amplia documentación están: MAGERIT versión 3 y NIST SP800-30 revisión 1, las cuales contemplan dentro de sus estructura el método formal, para llevar a cabo el proceso de análisis y evaluación de riesgos dentro de una organización que soporta su información en sistemas informáticos y de comunicaciones.

De acuerdo con lo anterior, apoyados en el estudio comparativo de las metodologías enunciadas, se determinará cual se ajusta más a los activos de información específicos de la Dirección Ejecutiva Seccional de Administración Judicial de Tunja – DESAJT–, y cuál puede ser integrada al modelo organizacional de la entidad. Y de esta forma, establecer una guía para el proceso de análisis y evaluación de riesgos de acuerdo con la metodología seleccionada e integrada a los distintos procesos, procedimientos y servicios en los que intervienen los activos de información de la entidad.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Elaborar una guía que permita analizar y evaluar los riesgos, de los activos de información de la Dirección Ejecutiva Seccional de Administración Judicial de Tunja - DESAJT, adoptando una metodología de gestión de riesgos de los Sistemas de Información.

4.2 OBJETIVOS ESPECÍFICOS

- Identificar los activos de información de la entidad, de acuerdo a los servicios que presta a la comunidad judicial y sus usuarios.

- Seleccionar una metodología de gestión de riesgos de los sistemas de información, apropiada para el análisis y evaluación de los riesgos, de los activos de información que administra la Dirección Ejecutiva Seccional de Administración Judicial de Tunja - DESAJT.

- Establecer una guía para el análisis y evaluación de los riesgos para los activos de información de la Dirección Ejecutiva Seccional de Administración Judicial de Tunja – DESAJT, de acuerdo con la metodología de gestión de riesgos seleccionada.

5. MARCO REFERENCIAL

5.1 MARCO TEÓRICO

Como fundamento teórico de la presente monografía, a continuación se presentan los conceptos propios de la Seguridad de la información, la Seguridad informática, los elementos que hacen parte de la gestión de riesgos y las actividades y procedimientos de los procesos de análisis y evaluación de riesgos de las metodologías MAGERIT versión 3 y NIST SP800-30 revisión 1.

5.1.1 Seguridad de la información y la seguridad informática. La Seguridad de la Información[1], contempla las normativas y/o mejores prácticas que le permiten a las organizaciones, elevar los niveles de aseguramiento de sus procesos, recursos tecnológicos, humanos y los procedimientos que en materia de seguridad de la información ha de tener en cuenta el nivel directivo de una organización. Cabe resaltar que los aspectos estratégicos y operativos son propios de la Seguridad Informática, los cuales motivan la realización de implementaciones técnicas orientadas a la protección de la información.

5.1.2 Activos de información de una organización. Los activos de información son aquellos recursos con los que cuenta una entidad para llevar a cabo el cumplimiento de su misión y objetivos institucionales; los cuales se pueden clasificar de la siguiente manera: la información, los equipos que la soportan y procesan, los usuarios que la utilizan, las instalaciones físicas donde se encuentran ubicadas, las redes que las transmiten, entre otros. Dentro de esta clasificación inicial, se expone una forma más detallada de estos tipos de activos, así[2]:

- La información: son todos aquellos datos que se encuentran registrados en medios impresos y/o digitales; dentro de los cuales se encuentran los documentos, reportes, informes, manuales, códigos fuente, libros, etc.

- Los equipos que soportan la información: bajo esta categoría se encuentran los recursos de *hardware* que soportan la infraestructura tecnológica que brinda el

[1] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES MinTIC. "Modelo nacional de gestión de riesgos de seguridad digital". [En línea]. <https://www.mintic.gov.co/portal/604/articles-61854_documento.docx>. [citado el 17 de octubre de 2018].

[2] ISOTools Excellence. "ISO 27001: Los activos de información". [En línea]. <https://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-informacion/>. [citado el 17 de octubre de 2018].

almacenamiento y procesamiento de la información de la entidad. Como equipos de *hardware* tenemos: los computadores, portátiles, servidores, *routers* y *switchs*.

- Los programas o aplicaciones: estos componentes se denominan recursos de *software* que se constituyen en todo programa instalado en los equipos de *hardware,* que permiten el procesamiento de datos y sistematización de los procesos de entidad, dentro de los cuales se pueden enunciar los sistemas operativos, programas corporativos y/o comerciales.

- Los usuarios que utilizan la información: son aquellas personas que de acuerdo a sus funciones utilizan la infraestructura tecnológica y de comunicaciones de la entidad; dentro de las cuales se encuentran los directivos, coordinadores, empleados, operadores, clientes, usuarios externos, etc.

- Las instalaciones físicas: corresponden a las oficinas, archivadores, cuartos de comunicaciones, y salas de trabajo que conforman la infraestructura física de la entidad.

5.1.3 El riesgo en seguridad informática. El riesgo en seguridad informática[3] hace referencia a la posibilidad de que suceda u ocurra un incidente de seguridad, ocasionado por una amenaza, la cual se genera por algún tipo de vulnerabilidad existente en un activo o sistema de información de la organización. Es significativo partir de estos conceptos, ya que al momento de estudiar y analizar la forma de asegurar los activos de información, es importante reconocer, de qué manera se pueden determinar los mecanismos de seguridad que fortalezcan la confidencialidad, integridad y disponibilidad de los elementos y sistemas que integran los activos de información de una entidad. De allí se desprende la importancia, de realizar un análisis y estudio de los factores que ponen en riesgo la seguridad y de esta forma, disminuir su impacto.

5.1.4 Gestión de riesgos. La gestión de riesgos en seguridad informática, se constituye como un proceso formal que le permite a una organización: determinar, analizar, valorar y clasificar los riesgos o incidentes que podrían afectar sus operaciones o servicios, causando pérdidas o daños; de tal modo que conociendo este tipo de circunstancias se pueda llegar a ejercer un tratamiento, encaminado en reducir, transferir, evitar y aceptar los riesgos, definidos así:

[3] ISOTools Excellence."ISO 27001: Plan de tratamiento de riesgos de seguridad de la información". [En línea]. <https://www.pmg-ssi.com/2017/06/iso-27001-plan-tratamiento-riesgos-seguridad-informacion/>. [citado el 17 de octubre de 2018].

- Reducir el riesgo, aplicando los respectivos controles que permitan mitigarlo o eliminarlo.

- Transferir el riesgo, dando la responsabilidad del riesgo a un tercero.

- Evitar el riesgo, suspendiendo la actividad que lo genera.

- Aceptar el riesgo, tomando la determinación de no invertir un costo para protegerse del mismo.

De esta forma, la gestión de riesgos[4] le facilita a la organización, la toma de decisiones entorno a los riesgos identificados, estableciendo qué tratamiento ejercer sobre los mismos, evaluando la relación costo –beneficio, decidiendo si la opción es invertir en medidas de seguridad para reducirlos, transferirlos o por lo contrario evitarlos o aceptar el nivel de riesgo que debe ser conocido y controlado.

5.1.5 Análisis de riesgos. El análisis de riesgos[5] es el proceso mediante el cual una organización consigue identificar, conocer, estudiar que activos de información posee, en que se soportan y valorar cuales son esenciales o no, y estimar los potenciales eventos que puedan afectar a los activos para el cumplimiento de los objetivos de la entidad. Este proceso, puede considerarse como una medida de seguridad que contempla varias actividades, con el propósito de identificar los activos de información a proteger en una entidad, cuáles son sus vulnerabilidades o puntos débiles y las amenazas que pueden tener la probabilidad de materializarse.

Mediante el análisis de riesgos, la organización da un primer paso para reconocer la importancia de la gestión de la seguridad de la información en su marco operativo. Como actividades principales dentro del análisis de riesgos, se pueden enunciar las siguientes:

- Realizar un inventario de los activos de información esenciales de la entidad.

- Identificar las vulnerabilidades inherentes o presentes en los activos de información.

---

[4] UNIVERSIDAD NACIONAL DE LUJÁN. “Riesgo vs. Seguridad de la Información”. [En línea]. <http://www.seguridadinformatica.unlu.edu.ar/sites/www.seguridadinformatica.unlu.edu.ar/files/site/material_taller_gestion_de_riesgo.pdf >. [citado el 17 de octubre de 2018].

[5] BLOG SEGURIDAD INFORMÁTICA. “Análisis de riesgos”. [En línea]. <http://seguridadinformaica.blogspot.com/p/analisis-de-riesgo.html >. [citado el 17 de octubre de 2018].

- Identificar las amenazas que puedan aprovechar las vulnerabilidades o insuficiencias de los activos de información y afectarlos.

- Identificar los riesgos asociados, debido a la posible materialización de una amenaza sobre un activo de información.

Teniendo en cuenta estas actividades, y al realizarlas de forma coherente y acertada, se garantiza que en el análisis de riesgos, se hayan identificado claramente los activos a proteger de la entidad, la manera en que estos se relacionan, las debilidades de cada uno y determinar los riesgos asociados a cada activo de información, dando paso al proceso de evaluación de riesgos.

5.1.6 Evaluación de riesgos. El proceso de evaluación de riesgos busca estimar el riesgo, según la probabilidad de ocurrencia o expectativa de materialización de una amenaza y el impacto ponderado del riesgo (magnitud del daño), sobre un activo de información[6]. De tal forma que el resultado de esta estimación, es obtener el valor del riesgo de los activos de información, lo que le permite a la entidad conocer el grado de aseguramiento de los activos de información y lo que les podría pasar a estos recursos, si no son protegidos adecuadamente o al menos tenerlos a un nivel de riesgo aceptable y controlable.

Finalmente como resultado del análisis y evaluación de riesgos, la entidad conocerá los riesgos a los que se encuentran expuestos sus activos de información y llegar a establecer una administración del riesgo, partiendo del tratamiento de los mismos, mediante controles adecuados. Como resultado de esta valiosa tarea, la organización podrá ejercer un control más eficaz y eficiente sobre sus recursos, y tomar decisiones acertadas, sobre qué medidas y políticas de seguridad deben implantarse al interior de la misma.

5.1.7 Metodologías de gestión de riesgos de los sistemas de información. Las metodologías de gestión de riesgos, hacen parte de las herramientas aplicadas de la Seguridad informática, las cuales fueron diseñadas por un organismo acreditado en aspectos propios de las tecnologías de información y las comunicaciones TICs, regidas por las directrices de un país y certificadas por un organismo de normalización como es la Organización Internacional de Normalización ISO.

[6] SEGU.INFO SEGURIDAD DE LA INFORMACIÓN. “Evaluación de riesgos”. [En línea]. <https://www.segu-info.com.ar/politicas/riesgos.htm>. [citado el 17 de octubre de 2018].

Las metodologías de gestión especializadas en riesgos de tecnologías de la información y comunicaciones TICs[7], se caracterizan por tener un objetivo principal y un alcance en materia de seguridad para los recursos tecnológicos y sistemas de información (activos de información) de una entidad. Estas metodologías, contemplan un conjunto de procedimientos, que le permitan a la parte u organización interesada, aplicar un esquema definido actividades, para llevar a cabo la gestión de riesgos de sus activos de información, y la cual se ajuste a las necesidades que requiera la entidad.

Teniendo en cuenta que existen distintas metodologías de gestión de riesgos para sistemas de información, que contemplan las tareas de análisis y evaluación de riesgos; a continuación se estudiaran las metodologías MAGERIT versión 3 y NIST SP800-30 revisión 1 y se presentarán los siguientes aspectos de cada una de ellas:

- Nombre de la metodología.
- Organismo que la elaboró y diseñó.
- Procedencia - país.
- Año de publicación.
- Versión.
- Alcance.
- Objetivos.
- Elementos documentales.
- Estructura de actividades - Método.
- Resultados.

[7] ALEMÁN, H. y RODRÍGUEZ, C. “Metodologías para el análisis de riesgos en los SGSI”. [En línea]. <http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874>. [citado el 17 de octubre de 2018].

5.1.7.1 Metodología de análisis y gestión de riesgos de los sistemas de información – MAGERIT versión 3. MAGERIT versión 3 es una metodología abierta, elaborada y diseñada por el Consejo Superior de Administración Electrónica del Ministerio de Hacienda y Administraciones Públicas de España [8]. La primera versión de ésta metodología, data del año 1997 y a partir de allí ha evolucionado considerablemente, a la versión 2 en el año 2005, llegando actualmente a su versión 3 en el año 2012. Transcurridos estos años, se ha consolidado como una de las metodologías de análisis y gestión de riesgos de los sistemas de información, más utilizadas debido a su carácter público y a la gran documentación apoyada en una serie de guías, procedimientos y catálogos, que se acercan cada vez más a la realidad de los recursos tecnológicos y sistemas de información con que cuentan las pequeñas y grandes organizaciones.

- Alcance de MAGERIT versión 3: la metodología MAGERIT versión 3, se especializa en brindar a las pequeñas y grandes organizaciones, un método formal que les permita conocer los aspectos derivados del uso de las tecnologías de la información y las comunicaciones TICs, dentro de los cuales se estiman los riesgos en materia de seguridad de la información. De acuerdo con lo anterior, la metodología proporciona una serie de actividades para llevar a cabo, el análisis y gestión de riesgos, estableciendo de forma concreta un modelo de la organización, a partir del conocimiento de los activos, el valor de cada activo para la organización, las dependencias o relaciones existentes entre ellos, las amenazas que puedan afectarlos y atentar contra la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad; principios considerados por la metodología como dimensiones de seguridad y a través de las cuales, la organización pueda estimar los riesgos a los que se encuentran expuestos sus activos de información y disponer de los controles y /o salvaguardas como medidas de seguridad para tratar los riesgos identificados.

- Objetivos de MAGERIT versión 3: esta metodología ha definido dos tipos de objetivos, los directos y e indirectos, ambos orientados en hacerle ver a la organización y a sus responsables, la importancia de conocer la existencia de los riesgos, y como a través de esta metodología se pueden analizar, evaluar y gestionar oportunamente. Finalmente, destaca que al implementar la metodología, indirectamente la organización está preparada para atender futuros procesos de

[8] PORTAL DE ADMINISTRACIÓN ELECTRÓNICA “MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”. [En línea]. < http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Vr-rq1Lkdpt >. [citado el 8 de Agosto de 2017].

evaluación, auditorias y/o certificaciones. A continuación se enuncian los objetivos directos e indirectos de MAGERIT versión 3[9]:

- Objetivos Directos
    - Sensibilizar a los responsables de la seguridad informática en las organizaciones, de la existencia riesgos y la necesidad de gestionarlos.
    - Ofrecer a la Organización un método sistemático, para analizar los riesgos derivados del uso de tecnologías de información y comunicaciones (TIC).
    - Ayudar a la Organización a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

- Objetivos Indirectos
    - Preparar a la Organización para atender procesos de evaluación, auditoría, certificación o acreditaciones.
    - Estandarizar los informes generados en cada actividad de la metodología.

- Elementos documentales de la metodología MAGERIT versión 3: toda la documentación de MAGERIT versión 3, se soporta en los siguientes libros y guías, los cuales son fundamentales para iniciar un proyecto de análisis de riesgos:
    - Libro I – Método: en este libro se formalizan y detallan cada una de las actividades del proceso de gestión de riesgos de la metodología. Consta de varios capítulos que tratan: a) Los conceptos más relevantes y las actividades del análisis y tratamiento de riesgos, b) Las actividades para llevar a cabo planes de seguridad o planes estratégicos, para ser implementados de acuerdo con las decisiones adoptadas para el tratamiento de riesgos, c) Las actividades del ciclo de desarrollo de *software* y d) Algunos consejos prácticos brindados para ejecutar en un proyecto, cada una de las tareas de análisis y tratamiento de riesgos.

[9] PORTAL DE ADMINISTRACIÓN ELECTRÓNICA “MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”. [En línea]. [En línea]. < http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Vr-rq1Lkdpt >. [citado el 8 de Agosto de 2017].

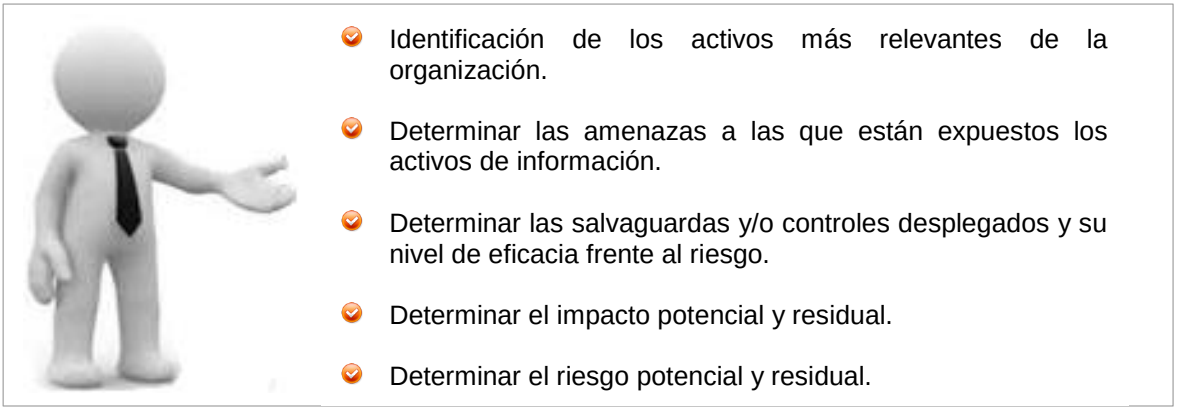
- Libro II – Catalogo de elementos: este libro ofrece un estándar frente a la clasificación de los tipos de activos, dimensiones de seguridad para la valoración de los activos de información, listado estandarizado de amenazas y salvaguardas (controles).

- Guía- Técnicas: en esta guía la metodología presenta las técnicas que se pueden llevar a cabo para emprender proyectos de análisis y gestión de riesgos y las cuales son de utilidad para la aplicación de la metodología.

- Estructura de actividades MAGERIT versión 3: la estructura de la metodología es bastante intuitiva, ya que de acuerdo con la ejecución de una serie de actividades, se obtiene la información sobre el modelo de los recursos tecnológicos, de comunicaciones y sistemas de información, con los que cuenta la organización; los cuales serán la base para dar comienzo a lo que la metodología define como el proceso de gestión de riesgos donde se combinan las actividades de análisis y el tratamiento de riesgos[10].

Partiendo de la primera actividad que consiste en el análisis de riesgos, en la siguiente figura, se muestra cómo la metodología propone los pasos para determinar cuáles son los activos de información con los que cuenta una organización, los elementos fundamentales de este proceso, y como estimar los riesgos a los que se encuentran expuestos dichos activos.

Figura 1. Pasos del análisis de riesgos en MAGERIT versión 3



Fuente: https://administracionelectronica.gob.es/ctt/magerit#.WcMIq8bavIV

[10] PORTAL DE ADMINISTRACIÓN ELECTRÓNICA "MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información". [En línea]. < http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Vr-rq1Lkdpt>. [citado el 8 de Agosto de 2017].

De acuerdo con la metodología, a continuación se describen cada una de las actividades para llevar a cabo el análisis de riesgos:

- Identificación de los activos más relevantes de la organización: esta actividad es considerada como la más importante dentro del proceso de análisis de riesgos en la metodología, ya que a través de ella, se fijan la pautas para que la organización identifique los activos de información esenciales y los demás componentes que integra el sistema, la interrelación o dependencias entre cada uno de ellos, su valor de acuerdo con la articulación y función que cumplen y ejercen sobre el sistema. De acuerdo con lo anterior, las dependencias entre activos le permiten a la organización conocer la medida de afectación de un activo de acuerdo a su nivel, ya sea como activo esencial (nivel superior) o secundario (nivel inferior) dentro del sistema y además le permite, determinar la forma de propagación de un daño sobre los activos en caso de presentarse un incidente de seguridad sobre el sistema. De esta forma, se pueden fijar los requisitos y el nivel de seguridad que requiere la organización. A continuación se exponen los conceptos que tiene en cuenta MAGERIT versión 3, para la identificación de los activos más relevantes dentro de una organización:

  - Definición de un activo de Información: MAGERIT versión 3 al ser una metodología especializada en riesgos para TICs, considera que dentro de en un sistema de información existen dos elementos esenciales, como son la información y los servicios. Partiendo de estos dos elementos, la metodología reconoce la información como toda aquella que se maneja en una organización y los servicios a todos aquellos que presta o brinda la entidad. De igual forma, la metodología establece la importancia de identificar los demás componentes que integran un sistema, los cuales son definidos como activos subordinados a los dos activos esenciales, siendo los siguientes:

    - Los datos, son los documentos en los que se representa la información.
    - Los servicios, son los servicios complementarios requeridos para organizar un sistema.
    - Los programas informáticos, es el *software* que permite tratar los datos.
    - Los equipos informáticos, es el *hardware* que permite almacenar los datos, las aplicaciones (programas informáticos) y servicios.
    - Los dispositivos que soportan la información, son los dispositivos donde se realiza el almacenamiento de los datos.

- El equipamiento auxiliar, son los dispositivos o elementos que complementan el sistema.

- Las redes de comunicaciones, es la infraestructura de transmisión que permite intercambiar datos.

- Las instalaciones físicas, son las ubicaciones físicas u oficinas donde se encuentran instalados los equipos informáticos y de comunicaciones.

- Las personas, son los usuarios que acceden u operan todos los componentes principales y complementarios del sistema.

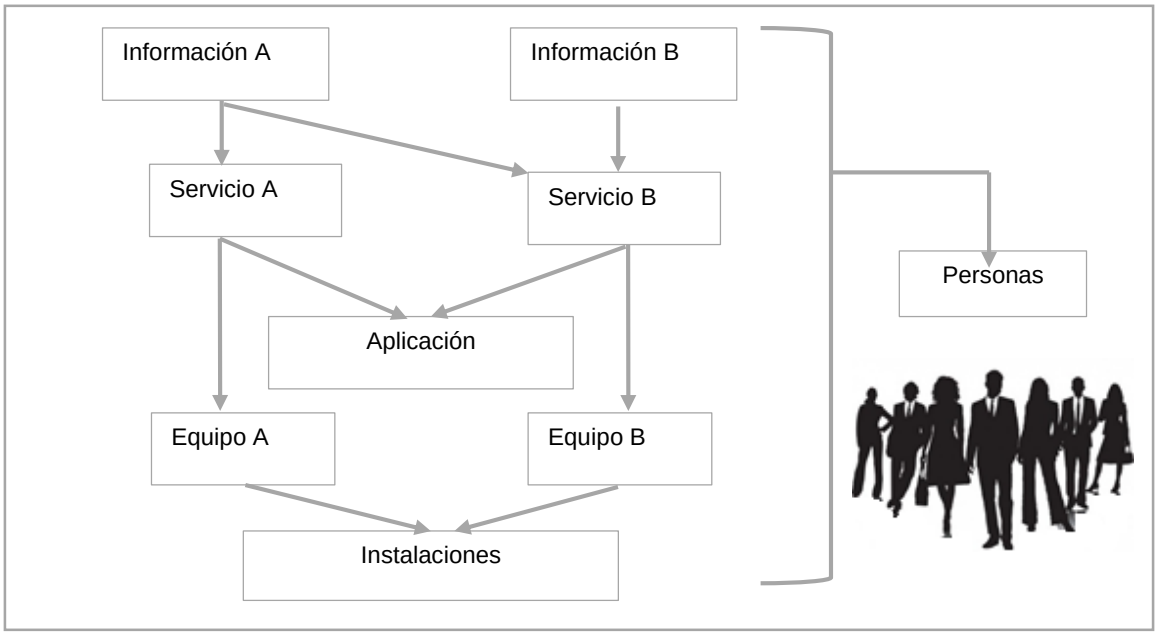
MAGERIT versión 3 establece estos componentes como los tipos de activos presentes en una organización, los cuales estandariza en el libro II[11], que corresponde al catálogo de elementos de la metodología, los cuales más adelante sirven como un criterio para la identificación de amenazas potenciales, para el establecimiento de salvaguardas apropiadas según la naturaleza del activo.

- Conocimiento de las dependencias entre activos: las dependencias entre activos, se definen como aquella relación que poseen los activos esenciales – la información y los servicios - con otros componentes del sistema (otros activos), desde los cuales puede verse comprometida la confidencialidad, integridad y disponibilidad de un sistema; de tal forma, que los activos principales están en un nivel superior y los otros activos catalogados como activos de nivel inferior, son los medios a través de los cuales se transmiten, soportan o almacenan los activos esenciales, dentro de los cuales se encuentran los programas, los equipos, las instalaciones y las personas.

A continuación se presenta una breve ilustración en forma de árbol, donde se ve un esquema de dependencia entre activos, dentro de los cuales fácilmente se puede identificar cuales corresponden al nivel superior y en orden descendente a un nivel inferior dentro de un sistema.

[11] PAE PORTAL ADMINISTRACIÓN ELECTRÓNICA. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. < https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WcgqkMbavIU >. [Citado el 24 de Septiembre de 2017].

Figura 2. Esquema de dependencias entre activos



Fuente: el autor

Cabe resaltar que la metodología formula un esquema de dependencias entre activos, con el objetivo de establecer más adelante el valor de un activo y obtener su valor acumulado, que se calcula de acuerdo a las dependencias que tenga un activo principal o superior y sus activos inferiores, y asimismo el identificar el daño que podría sufrir un activo de nivel superior frente a un incidente de un activo de nivel inferior o viceversa.

- Valor de un activo: la metodología hace especial énfasis en que una organización debe determinar y conocer que activos de información son imprescindibles para el sistema, de tal forma, que al ser muy alto el valor de un activo, su nivel de protección será mayor para cada una de las dimensiones de seguridad. Asimismo, esta valoración se traduce en la asignación de un valor cuantitativo para cada activo, según su propio valor y el valor acumulado. Este valor acumulado puede obtenerse con el esquema derivado de las dependencias entre activos, donde un activo del nivel inferior acumulará el valor de los activos superiores (que se apoyan en ellos) y de esta forma, se pueda conocer la valoración propia de cada activo.

- Dimensiones de seguridad de un activo: la metodología dentro de su estructura ha considerado que de acuerdo a la función o servicio que cumpla un activo, se deben considerar los tres pilares de la seguridad informática:

- La confidencialidad, aspecto inherente y para preservar sobre los datos.

- La integridad, al igual que el anterior, para garantizar el tratamiento de los datos.

- La disponibilidad, especialmente sobre los servicios que presta el sistema.

No obstante, ha tenido en cuenta la autenticidad y la trazabilidad, conceptos que contemplan los datos y los servicios, respecto de preservar quién accede a cada uno de ellos, quién lo hace, en qué momento lo hace y que hace con ellos.

- Determinar las amenazas a las que están expuestos los activos de información: conocidos e identificados los activos de información a proteger y atendiendo el catálogo de elementos dispuesto por la metodología, el segundo paso que establece MAGERIT versión 3 es determinar que amenazas pueden afectar a cada activo, su origen y valorar su influencia sobre cada dimensión de seguridad.

- Identificación y origen de las amenazas: MAGERIT versión 3 ha estandarizado e identificado las amenazas más comunes que pueden consultarse en el catálogo de elementos de la metodología, donde se establecen los siguientes orígenes de las amenazas que podrían afectar los activos información y/o un sistema de información:

- De origen natural: son incidentes que pueden ocurrir sin la intervención de los seres humanos, conocidos también como de origen accidental, dentro de los cuales se enuncian: incendios, inundaciones, terremotos.

- De origen industrial: son situaciones que se generan por la intervención de los seres humanos, dentro de los cuales se enuncian: la contaminación (polvo, suciedad, vibraciones), contaminación química, fallos eléctricos, campos electromagnéticos, condiciones incorrectas de temperatura, fallo de servicios de comunicaciones, deterioro de los soportes de almacenamiento y averías físicas de los equipos, que pueden presentarse por defectos en su diseño, o generados durante la implementación del sistema.

- De origen lógico de las aplicaciones: corresponden a los fallos en los programas, que pueden presentarse por defectos en su diseño, o generados durante su puesta en marcha.

- De origen no intencional causados por las personas: corresponden a los errores no intencionales suscitados por personas con acceso a los sistemas de información.

- De origen intencional causados por las personas: corresponden a las personas que tiene una intención premeditada para afectar los sistemas de información.

- Valor de las amenazas: la valoración consiste determinar cuál va a ser el grado de afectación de una amenaza sobre el activo de información y además el fijar la probabilidad de que ésta pueda materializarse, de ahí que la metodología establece dos parámetros para valorar una amenaza: la primera consiste en definir la probabilidad de ocurrencia o materialización de una amenaza, que puede ser medida bajo criterios de la frecuencia en los casos de que se haya materializado, la cual puede valorarse como muy frecuente (MF), frecuente (F), normal (N), poco frecuente (B), muy poco frecuente (MB). A continuación en la tabla 1, se enuncian los 5 niveles de probabilidad de ocurrencia de la materialización de una amenaza.

Tabla 1. Probabilidad de ocurrencia

Nivel de probabilidad de ocurrencia	Valor
MF	Muy frecuente
F	Frecuente
N	Normal
B	Poco frecuente
MB	Muy poco frecuente
Fuente: el autor	

La segunda valoración se realiza teniendo en cuenta la degradación o el daño causado al activo, mediante el cual se mide el daño causado a un activo por un incidente en el caso de que se materializará o lo afectara una amenaza. La degradación de un activo puede valorarse como muy alta (MA), alta (A), medio (M), baja (B), muy baja (MB). A continuación, en la tabla 2 se enuncian los 5 valores de degradación de valor de un activo.

Tabla 2. Degradación del valor del activo

Nivel de degradación del activo	Valor
MA	Muy Alta
A	Alta
M	Medio
B	Baja
MB	Muy Baja
Fuente: el autor	

Con base en estas dos valoraciones, la metodología indica que es posible determinar el impacto potencial que va de la mano de la degradación de un activo y éste se define como la medida del daño generado sobre un activo que resulta de la materialización de una amenaza. Este impacto es cuantificable y se calcula conociendo el valor de los activos en sus diferentes dimensiones de seguridad y el grado de afectación que causan las amenazas sobre los mismos, de esta forma se obtiene el impacto que las amenazas tendrían sobre el sistema. Aunado a lo anterior, también es posible determinar el riesgo potencial que se calcula teniendo en cuenta el impacto generado de las amenazas sobre los activos y de acuerdo a su probabilidad de ocurrencia. Dichos riesgos se traducen en la medida del daño probable sobre un activo de información.

- Determinar las salvaguardas y/o controles desplegados y su nivel de eficacia frente al riesgo: para esta determinación la metodología ha establecido dentro de su libro II de catálogo de elementos, una serie de salvaguardas que le sirven a la organización como mecanismos o contra medidas para reducir los riesgos. Dichas salvaguardas deberán seleccionarse de acuerdo a:

  - El tipo de activos que son valiosos para la organización y requiere proteger.
  - Las dimensiones de seguridad que demandan más atención y protección.
  - Las amenazas de las que hay que proteger los activos.
  - La posibilidad de que existan salvaguardas o controles alternativos.

Cabe resaltar que las salvaguardas están orientadas en establecer el tipo de protección requerido, el nivel y/o eficacia de la protección y además puede resultar el conocimiento de las vulnerabilidades que puedan tener dichas medidas de protección sobre los activos.

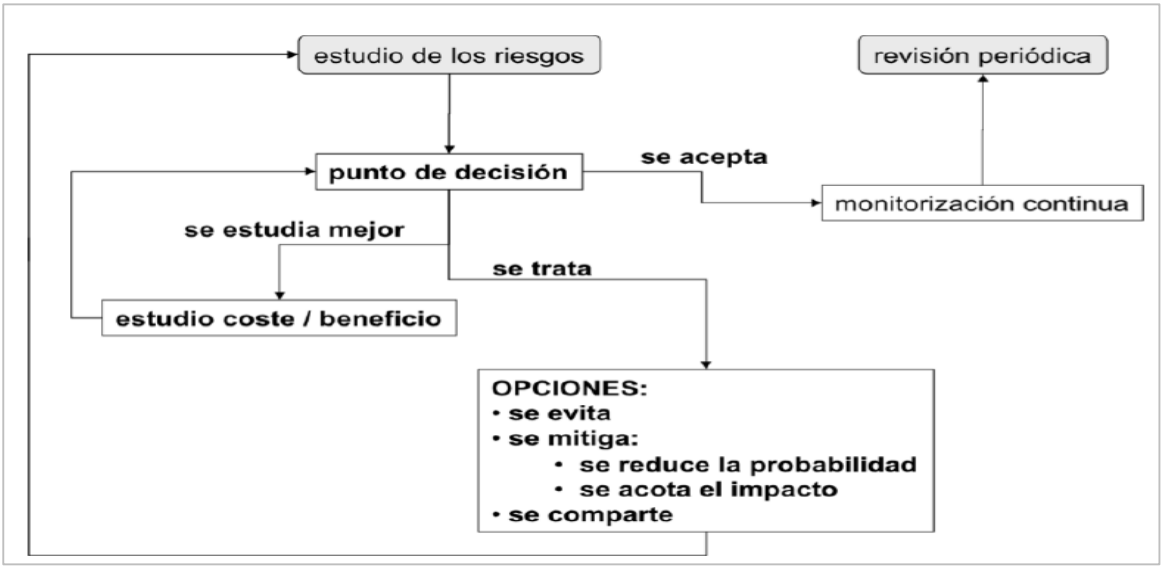
- Determinar el impacto potencial y residual: con el desarrollo de los anteriores aspectos, la metodología define que el impacto es todo aquello que puede ocurrir, de tal forma que el impacto potencial al que está expuesto un activo se estima sin tener en cuenta las salvaguardas implantadas recientemente, y el impacto residual se determina teniendo en cuenta las salvaguardas que se han definido para el sistema. Bajo este contexto, los activos quedan en una situación de posible impacto, donde se puede determinar el impacto potencial sin salvaguardas y modificarlo a un impacto residual con la aplicación de salvaguardas.

- Determinar el riesgo potencial y residual: para determinar este riesgo, atendiendo que es lo que probablemente ocurra al sistema o a los activos, es importante partir de la estimación del impacto, donde el riesgo potencial es al que están sometidos los activos sin salvaguardas y el riesgo residual, se obtiene después de aplicar el conjunto de salvaguardas y/o controles, donde los activos quedan en una situación de posible riesgo, modificando de esta forma el riesgo desde un valor potencial (sin salvaguardas), a un valor residual (con salvaguardas).

- Tratamiento de riesgos: El tratamiento de riesgos es la segunda actividad del proceso de gestión de riesgos de la metodología MAGERIT versión 3, la cual se vale de los resultados del análisis de riesgos, donde se obtuvieron: a) los activos de información valorados de acuerdo al grado de importancia para la organización y las dependencias con otros activos, b) las amenazas de las cuales deben ser protegidos, c) las salvaguardas implantadas para hacer frente a un incidente, d) y el estado del riesgo que se obtiene con la estimación de los impactos, es decir, identificar lo que puede ocurrir y el daño generado a un activo y de igual forma, el riesgo traducido en la probabilidad de que ocurra un incidente o el daño probable sobre un activo.

Antes de entrar a conocer cada una de las actividades del tratamiento de riesgos, la metodología resume en la siguiente figura, las posibles decisiones que la organización puede tomar después de haber estudiado los riesgos, combinando de esta forma el análisis con la evaluación de riesgos.

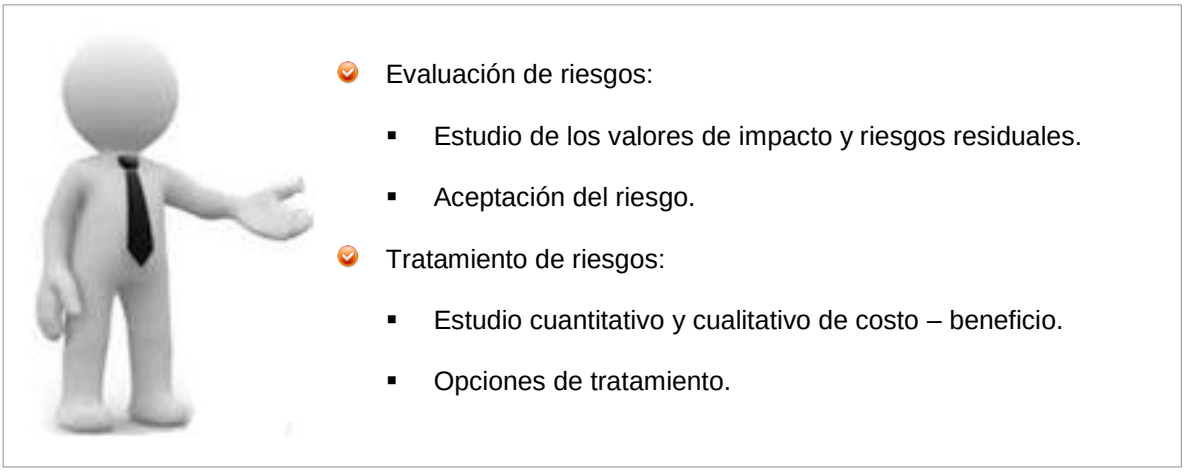
Figura 3. Decisiones de tratamiento de los riesgos



Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Con esta perspectiva, el tratamiento de riesgos se posiciona en cabeza de la organización, y como apoyo a esta labor, la metodología orienta a la organización para que estas decisiones se efectúen, llevando a cabo dos pasos de la gestión de riesgos, que corresponden a la evaluación y tratamiento de riesgos que se muestran en la siguiente figura.

Figura 4. Pasos del tratamiento de riesgos en MAGERIT versión 3



Fuente: https://administracionelectronica.gob.es/ctt/magerit#.WcMIq8bavIV

- Evaluación de riesgos: La evaluación de riesgos consiste en que la organización reconozca el estado presente o actual del nivel de seguridad en el que se encuentran los activos, es por esto, que el nivel directivo de la organización o los responsables de la seguridad, deben tener en cuenta el valor del riesgo residual obtenido para cada activo, y además, el informe de vulnerabilidades o deficiencias arrojadas después de la aplicación de salvaguardas, dentro de cuales hay que prestar especial atención en las salvaguardas que no están y no se han implantado. Además dentro de esta evaluación, es posible considerar qué riesgos son aceptables o no.

    - Estudio de los valores de impacto y riesgos residuales: este estudio consiste en que la organización debe evaluar el contexto de seguridad de los activos respecto de los valores de riesgo, es decir, cuál es el estado del sistema teniendo desplegadas una serie de salvaguardas y la eficacia de las mismas; o si por el contrario, hay que implantar nuevas salvaguardas y fortalecer el esquema actual.

    - Aceptación del riesgo: Es una forma en la que la organización puede considerar el nivel de impacto y riesgo de forma aceptable, donde se hace responsable de tomar esta decisión y la admite formalmente, ya sea por disposición gerencial, legal o por compromisos con terceros. La aceptación del riesgo se puede hacer por activo, por conjunto de activos, por una dimensión de seguridad o por un determinado servicio.

- Tratamiento de riesgos: La metodología define inicialmente que el nivel directivo puede llegar a aceptar el riesgo dentro del sistema de seguridad implantado, considerando:

    - Reducir el riesgo residual: consiste en que la organización acepta un menor riesgo.

    - Ampliar el riesgo residual: consiste en que la organización acepta un mayor riesgo.

Cualquiera de estas dos opciones puede ser asumida, no obstante, debe tenerse en cuenta el contexto de los riesgos soportados por el sistema o los activos teniendo en cuenta todos los escenarios posibles.

- Estudio cuantitativo y cualitativo de costo – beneficio: la metodología define una serie de escenarios donde se reflejan un estudio cuantitativo acerca de los costos de las salvaguardas aplicadas y cuál es el precio de inversión en ellas, en caso de que aún no se hayan implantado. Los escenarios contemplados en caso de que la organización tenga que protegerse de un riesgo significativo, son los siguientes:

    - Escenario 0: no realizar ninguna acción.

    - Escenario 1: el aplicar un cierto conjunto de salvaguardas.

    - Escenario 2: el aplicar otro conjunto de salvaguardas.

Cada escenario indicaría el posible estado del sistema y el coste para cada uno de ellos.

En cuanto al estudio cuantitativo, en estos se consideran los aspectos intangibles como: la imagen de la organización, la capacidad operativa, de producción, el cumplimiento normativo, entre otros. Los cuales estarían expuestos a ciertos riesgos, de ahí que es importante buscar una combinación de medidas asumibles por la organización.

- Opciones de tratamiento del riesgo: de una forma alternativa a la aceptación del impacto y el riesgo, la metodología propone otras opciones para el tratamiento de riesgos que la organización puede llegar a estudiar o adoptar:

    - Eliminar el riesgo: se elimina el origen del riesgo, siendo esta una opción frente a un riesgo que no es aceptable. Dentro de esta alternativa se encuentran: el eliminar algunos activos y emplear otros en su lugar o reordenar la arquitectura y el esquema de dependencias del sistema.

    - Mitigar o reducir el riesgo: la mitigación hace referencia en reducir el riesgo, ya sea respecto de la degradación causada por una amenaza o reducir la probabilidad de materialización de una amenaza. En cualquiera de los dos casos, es importante mejorar las salvaguardas del sistema.

    - Transferir o compartir el riesgo: los riesgos pueden ser transferidos a terceros con el objeto de asegurar económicamente las consecuencias generadas por dichos riesgos y el compartir un riesgo, hace referencia al

hecho de repartir responsabilidades que pueden ser desde el punto legal y otro técnico u operativo.

- Financiar el riesgo: esta opción va de la mano con la aceptación del riesgo, donde la organización decide reservar fondos en caso de que el riesgo sea un hecho y pueda responder y asumir por las consecuencias de este.

Tomada cualquiera de las opciones de eliminar, mitigar, transferir los riesgos, la organización debe realizar un nuevo análisis de riesgos, esto debido a que las condiciones y responsabilidades sobre los activos del sistema han sido modificadas. En cuanto a la opción de tratamiento del riesgo por financiación, esta decisión no altera el contexto del sistema, por lo cual no se requiere realizar un nuevo análisis de riesgos.

- Resultados del análisis y gestión de riesgos con MAGERIT versión 3: como resultado de la realización de cada una de las actividades de análisis y gestión de riesgos, MAGERIT versión 3 contempla los siguientes informes más relevantes de acuerdo a cada tarea ejecutada, así:

- El modelo del sistema, muestra los activos más relevantes para la organización y el valor de cada uno de ellos dentro de su esquema de dependencias con otros activos complementarios.

- El mapa de riesgos, muestra las amenazas identificadas y las que puedan materializarse sobre los activos.

- La declaración de aplicabilidad, muestra el estudio realizado a las salvaguardas, donde se definen cuales aplican o no sobre el sistema.

- El estado del riesgo, muestra la individualización de los activos por su riesgo residual.

- El Informe de insuficiencias, muestra las vulnerabilidades presentes en el sistema de acuerdo a la ausencia o ineficiencia de las salvaguardas desplegadas.

5.1.7.2 Metodología 2: Guía NIST SP800-30 revisión 1 - para realizar evaluaciones de riesgos. La guía de seguridad NIST SP800-30 revisión 1, hace parte de la serie de publicaciones especiales SP 800 orientada a la seguridad de la información. La guía NIST SP800-30 revisión 1, está fundamentada en los aspectos para llevar a cabo la evaluación de riesgos, alineada con los estándares y normativas de la seguridad de información para la gestión de riesgos dentro de una organización, fue diseñada por el Instituto Nacional de Normas y Tecnología de los Estados Unidos –NIST (National Institute of Standards and Technology), organismo que administra la tecnología en el Departamento de Comercio de los Estados Unidos y es el encargado de promover el desarrollo avanzado de normas técnicas, para el uso productivo de las tecnologías de la Información. Esta guía fue publicada en septiembre de 2012[12], sustituyendo la publicación especial NIST SP800-30 "Guía de gestión de riesgo de desarrollo de sistemas informáticos" de julio de 2002, y además se constituye en el complemento del método formal de la gestión de riesgos de la publicación SP800-39.

- Alcance de la metodología NIST SP800-30 revisión 1: la guía establece las actividades encaminadas para llevar a cabo la evaluación de riesgos, como parte fundamental y componente del proceso de gestión de riesgos establecido por el Instituto Nacional de Normas y Tecnología de los Estados Unidos, para las dependencias y sistemas de información federales. No obstante, al incursionar en el contexto de la seguridad de la información, esta guía puede ser aplicada según lo requieran organizaciones de carácter público o privado.

- Objetivos de la metodología NIST SP800-30 revisión 1: Los principales objetivos y propósitos de la guía se fundamentan en:

  - Proporcionar a la organización una guía formal que le permita identificar los riesgos potenciales que surgen del uso y operación de los sistemas de información, así como la información que es procesada, almacenada y transmitida a través de estos.

  - Colaborar a las organizaciones para que a través de la evaluación de riesgos, se determinen los riesgos que puedan afectar la misión de la organización, sus funciones, procesos, infraestructura de servicios y sobre sus sistemas de información.

[12] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guide For Conducting Risk Assessments. [En línea]. < https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final>. [Citado el 17 de agosto de 2017].

- Constituirse en una herramienta que le permita a los directivos de la organización, respaldar la toma decisiones y actividades en los tres niveles de la jerarquía de gestión de riesgos: organización, misión y sistemas de información.

- Elementos documentales de la metodología NIST SP800-30 revisión 1: toda la documentación de la guía de evaluación de riesgo, se encuentra disponible a través de la página principal en internet del Instituto Nacional de Normas y Tecnología de los Estados Unidos –NIST https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final, y en la cual se abordan los siguientes capítulos:

  - Capítulo 1 – presenta una amplia introducción de la guía, donde se contemplan todos los aspectos referidos los objetivos, directrices y referencias relacionadas con otras guías de seguridad de información del NIST.

  - Capítulo 2 – presenta una descripción general y los conceptos clave del proceso de gestión de riesgos, la evaluación de riesgos y su aplicación.

  - Capítulo 3 – presenta los pasos de la guía para realizar la evaluación de riesgos en una organización.

Además la guía NIST SP800-30 revisión 1, se apoya en las siguientes publicaciones especiales[13] :

- SP 800-39: definición del proceso de gestión de riesgos de la seguridad de la información: organización, misión y sistemas de información. Fecha de publicación 03 de enero de 2011.

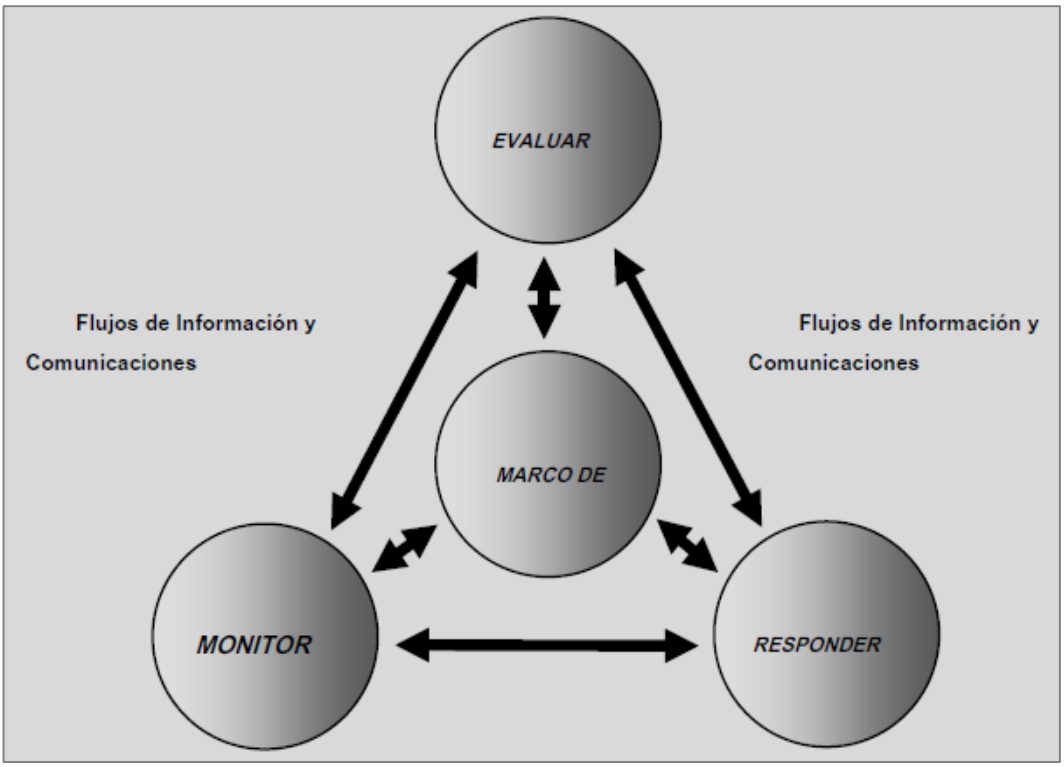
- SP 800-37: guía para la aplicación del marco de gestión de riesgos a los sistemas de información federales. Fecha de publicación 06 de octubre de 2014.

- SP 800-53: controles de seguridad y privacidad para sistemas de información y organizaciones. Fecha de publicación 22 de enero de 2015.

[13] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Computer Security Resource Center. [En línea].< https://csrc.nist.gov/publications/sp> .[Citado el 16 de agosto de 2017].

- Estructura de la metodología NIST SP800-30 revisión 1: la guía NIST SP 800-30 revisión 1, proporciona el método que le permite a una organización conocer los riesgos y el impacto negativo respecto de la seguridad de la información sobre: las operaciones enfocadas en la misión de la entidad, las funciones, la imagen y reputación, así como los activos de información, el personal y su interacción con otras organizaciones. El proceso de gestión de riesgos definido por la guía, está fundamentado en cuatro componentes denominados: marco del riesgo, evaluación del riesgo, respuesta a los riesgos y monitoreo de los riesgos; los cuales interactúan entre sí, de acuerdo a los flujos de información y comunicaciones. En la siguiente figura se ilustra el esquema del proceso de gestión del riesgo[14].

Figura 5. Esquema del proceso de gestión del riesgo NIST SP800-30 revisión 1



Fuente: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Cada uno de los componentes, orienta a la organización hacia como llevar a cabo el proceso de gestión de riesgos y además, establece un propósito para cada uno de ellos; en estricto orden se encuentra el primer componente denominado marco

[14] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. "NIST Special Publication 800-30 Revision 1". [En línea]. <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf >.[Citado el 20 de octubre de 2018].

del riesgo, en él se describe el contexto en el que una organización toma las decisiones fundamentas sobre los riesgos, teniendo como principal propósito en que la organización pueda generar una estrategia de gestión de riesgos, donde se pretenda evaluar, responder y monitorear los riesgos, delimitando el alcance de cada decisión al respecto.

El segundo componente es la evaluación de riesgos, que consiste particularmente en conocer cómo la organización evalúa los riesgos en el contexto del marco del riesgo definido inicialmente. Su principal propósito consiste en identificar las amenazas que pueden presentarse dentro de la organización especialmente sobre sus activos, el personal, sus operaciones y otras organizaciones; las vulnerabilidades internas y externas de la organización, el impacto (daño) que puede ocurrir frente a riesgos potenciales por la explotación de vulnerabilidades, y finalmente, el riesgo o la probabilidad de que se produzca el daño, de acuerdo con la determinación del riesgo.

El tercer componente se fundamenta en la forma del responder de la organización después de determinado el riesgo, es decir, esta acción se realiza al conocer los resultados de la evaluación del riesgo. Su principal propósito consiste en proporcionar una respuesta coherente frente a la evaluación de riesgos, además de conocer el estado del nivel de riesgo de cada uno de los activos de la organización.

El cuarto componente corresponde al monitoreo de los riesgos, su principal propósito es determinar la efectividad de las respuestas dadas a los riesgos, identificar los posibles cambios de riesgos que pueden afectar a los sistemas de información y su entorno, verificar que las respuestas a los riesgos se han implementado y que se satisfagan los requisitos de seguridad de la información de los distintos niveles de la organización o políticas y normatividad que exijan un seguimiento.

Conocidos los componentes del esquema del proceso de gestión del riesgo definido por NIST SP800-30 revisión 1, la guía se centra en llevar a cabo la evaluación de riesgos en tres niveles de la organización denominados “Jerarquía de gestión de riesgos” definida ampliamente en la publicación especial SP800-39 de NIST. De acuerdo con esta jerarquización, es posible reconocer distintas perspectivas de aplicación de la evaluación del riesgo, definidas bajo los niveles de la Organización – nivel 1, la misión y las funciones del negocio – nivel 2 y los sistemas de información – nivel 3; dejando ver este esquema desde un nivel estratégico a un nivel táctico.

En la siguiente figura se muestran cada uno de los niveles de jerarquización del riesgo dentro de una organización.

Figura 6. Jerarquía de gestión de riesgos definida en NIST SP 800-39

Fuente: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Teniendo en cuenta que la evaluación de riesgos, se puede aplicar en cada uno de los niveles de la jerarquía de la gestión de riesgos, es importante resaltar cuales son los aspectos que se fortalecen y se estudian en cada uno de los niveles, y además que se constituyan en las principales fuentes para la toma de decisiones respecto

de los riesgos. A continuación se describe el propósito de la evaluación de riesgos en cada nivel:

- Nivel 1 - Organización: la evaluación de riesgos que se realiza en este nivel, se centra en las operaciones, los activos y los individuos con la evaluación integral a través de la misión y funciones de la organización.

- Nivel 2 - Misión / funciones del negocio: la evaluación de riesgos que se realiza en este nivel, está orientado en la arquitectura de la organización fundamentada en la misión y funciones de la misma, donde se evalúan el nivel de seguridad y los requisitos frente a los procesos del negocio y su capacidad de recuperación con el desarrollo de planes de continuidad.

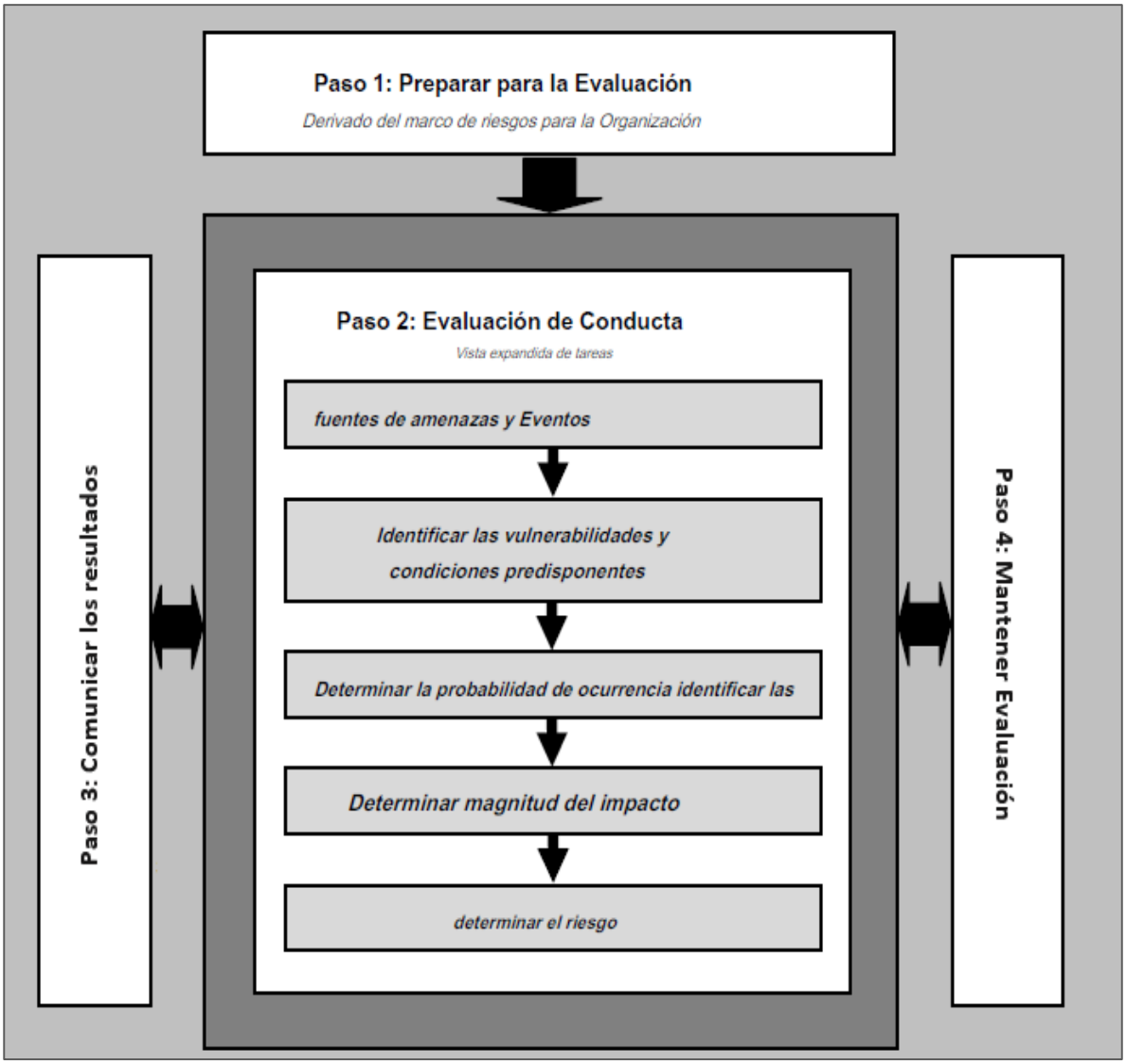
- Nivel 3 - Sistemas de información: la evaluación de riesgos que se realiza en este nivel, se centra en evaluar de forma inicial o posterior, las vulnerabilidades y condiciones predisponentes que afectan a la confidencialidad, integridad y disponibilidad de los sistemas de información en el contexto de posibles entornos que faciliten la explotación de vulnerabilidades sobre los mismos. Permitiendo de esta forma, tomar las decisiones acerca de los controles de seguridad necesarios basados en el entorno de trabajo.

Identificados cada uno de los aspectos y fundamentos establecidos por la guía NIST SP800-30 revisión 1, a continuación se describen las etapas y actividades del proceso de evaluación de riesgos.

- Proceso de evaluación de riesgos: en el componente de evaluación de riesgos, se concentran cada uno de los elementos esenciales que le permiten a una organización llevar a cabo una efectiva evaluación de riesgos, logrando de esta forma, determinar los riesgos a los que se encuentran sometidos sus activos de información, el entorno en el que actúan, las operaciones, los individuos de la organización y su relación con otras organizaciones.

En la siguiente figura se enuncian las cuatro etapas del proceso de evaluación de riesgos.

Figura 7. Etapas del proceso de evaluación de riesgos con NIST SP800-30 revisión 1



Fuente: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Dentro de cada etapa del proceso de evaluación de riesgos, se desprenden una serie de tareas, donde sus resultados son el insumo para iniciar una nueva actividad, destacando que la organización puede de manera iterativa llevar a cabo este proceso de evaluación en el evento que lo requiera. De igual manera, la guía proporciona a modo de ejemplo, una serie de tablas y escalas de evaluación, como apoyo a la organización, para conocer en detalle cómo abordar y desarrollar cada etapa y las tareas de este proceso. A continuación se describen cada uno de los

pasos y las tareas específicas propuestas en la evaluación de riesgos dentro de los tres niveles de jerarquización de riesgos, definidos para una organización[15]:

- Paso 1 - Preparación para la evaluación de riesgos: para llevar a cabo la evaluación de riesgos, inicialmente se deben conocer las políticas y los requisitos definidos por la organización dentro de su marco de gestión, es decir, delimitar el alcance de la evaluación, establecer las estrategias y metodologías para abordar el análisis, los procedimientos de los factores de riesgo a tener en cuenta y los requisitos para determinar el riesgo dentro de la organización. Con el objeto de llevar a cabo este primer paso, la guía establece las siguientes actividades de preparación para una evaluación de riesgos:

    - Identificar el propósito de la evaluación de riesgos: consiste en identificar los aspectos o la información que se desea obtener con la aplicación de la evaluación de riesgos, es decir, reconocer cual es el objetivo de la evaluación e identificar qué áreas de la organización se deben apoyar.

    - Identificar el alcance de la evaluación de riesgos: consiste en establecer el alcance sobre la aplicabilidad de la evaluación del riesgo, teniendo en cuenta qué partes de la organización se van a evaluar y se verán afectadas, así como los aspectos técnicos, de duración y las decisiones resultantes de la evaluación.

    - Identificar los supuestos y las limitaciones asociadas a la evaluación de riesgos: corresponde a supuestos que la organización puede llegar a tener respecto de fuentes de amenaza, vulnerabilidades, impactos potenciales, enfoques de análisis y evaluación; además de identificar las restricciones de recursos disponibles, habilidades, conocimientos y consideraciones operativas para la evaluación de riesgos.

    - Identificar las fuentes de información que se utilizarán como insumos para la evaluación de riesgos: consiste en identificar las fuentes detalladas que contengan la información de las amenazas, vulnerabilidades e impactos a tener en cuenta en la evaluación de riesgos; de tal forma que la organización pueda determinar la importancia de la información de amenazas y vulnerabilidades.

[15] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. “NIST Special Publication 800-30 Revision 1”. [En línea]. <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf >. [Citado el 20 de octubre de 2018].

- Identificar el modelo de riesgo y los enfoques analíticos para ser empleados durante la evaluación de riesgos: en ésta identificación la organización debe emplear uno o varios modelos de riesgo para llevar a cabo la evaluación de riesgo, el cual se puede fundamentar en los factores de riesgo que pueden estar presentes en la organización como: las amenazas, vulnerabilidades, el impacto, la probabilidad y/o una condición predisponente. Así mismo, la organización debe definir el enfoque de análisis específico que se utilizará para la evaluación de riesgos, donde se incluye el enfoque de evaluación: cuantitativo, cualitativo y semi-cuantitativo, y el enfoque de análisis que puede estar orientado a las amenazas, orientado a los activos / impacto y orientado a las vulnerabilidades.

- Paso 2 - Realización de la evaluación de riesgos: en esta segunda etapa del proceso, es fundamental la información recopilada en el paso de preparación de la evaluación del riesgo, donde la organización ha establecido el propósito, el alcance, los supuestos y limitaciones para iniciar la evaluación de riesgos. Definidos los anteriores aspectos, se podrá iniciar el proceso de evaluación de riesgos, donde se analizarán las amenazas, vulnerabilidades, impactos y probabilidades de los riesgos que se puedan producir y de esta forma, puedan ser identificados y priorizados de acuerdo con cada nivel de jerarquización de riesgos definidos por la guía.

Como apoyo a las tareas de evaluación de riesgos, la guía contiene una serie de plantillas que proporcionan a la organización la información útil y precisa en la evaluación de riesgos. Estas plantillas están definidas en los apéndices D al I de la documentación de la guía. A continuación se presentan las tareas para llevar a cabo la evaluación de riesgos dentro de una organización:

- Identificar las fuentes de amenaza más importantes para la organización: ésta tarea consiste en identificar plenamente y caracterizar las fuentes de amenaza más relevantes para la organización, además de determinar la capacidad, la intención y orientación de las amenazas. La organización puede apoyarse en el apéndice D de la guía donde se proporciona de manera puntual como identificar, caracterizar y evaluar todos los aspectos de las amenazas.

- Identificar los eventos de amenazas que se puedan producir por las fuentes: a partir de las fuentes de amenaza identificadas, la organización determinará los eventos o escenarios altamente potenciales que puedan ser producto de

las fuentes de una amenaza, en cualquiera de los niveles de jerarquización de riesgos. El apéndice E de la guía, proporciona el conjunto de tablas mediante las cuales se pueden identificar los eventos de amenaza que pueden presentarse dentro de la organización.

- Identificar las vulnerabilidades que podrían ser explotadas por las fuentes y eventos de amenazas, además de las condiciones predisponentes donde se podría materializar la amenaza: la organización a través de diferentes estudios de vulnerabilidad, podrá identificar la naturaleza y el grado en que los procesos de su misión y los sistemas de información son vulnerables a las fuentes de amenazas identificadas en la tarea 1 y a los eventos de amenazas identificadas en la tarea 2. Además debe reconocer que aspectos o entornos de operación y físicos se constituyen en vulnerabilidades generadas de condiciones predisponentes, tales como la ubicación de oficinas o la arquitectura de un sistema de información, que por sus mismas condiciones aumentan o disminuyen la probabilidad de ocurrencia de un evento de amenaza, que generalmente tiene impactos adversos para la organización. El apéndice F de la guía, proporciona el conjunto de tablas mediante las cuales se pueden identificar las vulnerabilidades y las condiciones predisponentes presentes dentro de una organización.

- Determinar la probabilidad de ocurrencia de las amenazas: en esta actividad se determina la probabilidad de que una amenaza se presente, teniendo en cuenta las fuentes de amenazas que podrían iniciar un evento o incidente. Las vulnerabilidades y condiciones predisponentes identificadas, y la susceptibilidad del conjunto de salvaguardas y medidas previstas por la organización para detener las amenazas, información que ha sido recopilada con el desarrollo de las tareas previas a esta actividad.

Sumado a lo anterior, para llevar a cabo la determinación de la probabilidad de ocurrencia de las amenazas, la guía propone emplear un proceso de tres pasos considerando tres escenarios: i) evaluar la probabilidad de iniciación de un evento de amenaza, teniendo en cuenta las características de las fuentes de amenaza. ii) evaluar la probabilidad cuando los eventos de amenazas se han producido y hayan generado impactos adversos sobre los activos, el funcionamiento de la organización, los individuos y otras organizaciones, teniendo en cuenta las vulnerabilidades y condiciones predisponentes identificadas. iii) evaluar la probabilidad general como la combinación de la probabilidad de inicio / ocurrencia y la probabilidad de tener un impacto adverso.

El apéndice G de la guía, proporciona el conjunto de tablas mediante las cuales se pueden identificar los aspectos a tener en cuenta dentro de una organización para determinar y evaluar la probabilidad de iniciación / ocurrencia de amenazas.

- Determinar la magnitud de los impactos adversos originados por eventos de amenazas: en esta actividad se definen los posibles tipos de impactos que pueden ser causados sobre los activos, funcionamiento y personas de los tres niveles de la jerarquía de riesgos. De igual forma, se evalúa el impacto generado por los eventos de amenazas y sus efectos adversos sobre la organización.

  El apéndice H de la guía, proporciona el conjunto de tablas mediante las cuales se pueden encontrar ejemplos como llevar a cabo la determinación del impacto, los tipos de impactos y la evaluación de estos.

- Determinar los riesgos de seguridad de información: ésta tarea consiste en identificar los riesgos para la organización, tomando el impacto generado por los eventos de amenaza por su probabilidad de ocurrencia. El resultado de esta evaluación define el nivel del riesgo para la organización asociado con los eventos de amenazas identificados; determinando así, el grado en que las organizaciones están amenazadas por este tipo de eventos. El apéndice I de la guía, proporciona el conjunto de tablas mediante las cuales se pueden encontrar como determinar el nivel del riesgo, además de presentar un modelo de riesgos basado en las fuentes de amenaza.

- Paso 3 - Comunicar los resultados de la evaluación de riesgos: en esta tercera etapa del proceso, le corresponde a la organización fijar los mecanismos adecuados para socializar y compartir a las partes interesadas e integrantes de la organización los resultados obtenidos en la evaluación de riesgos, lo cuales pueden ser presentados mediante informes, reuniones, comunicaciones formales e informales.

La guía proporciona en el apéndice K, la información esencial que la organización puede utilizar para comunicar los resultados obtenidos en la evaluación de riesgos, socializando de esta forma a toda la organización de los riesgos que se derivan de la operación, el uso de los sistemas de información de la organización y los entornos en los que operan estos sistemas.

- Paso 4 - Mantener la evaluación de riesgos: finalmente en esta cuarta y última etapa del proceso, se establecen las directrices para que la organización tenga actualizado el conocimiento específico de los riesgos a los que se encuentran expuestos e incorporar los cambios o modificaciones detectadas a través del componente de monitoreo del proceso de gestión de riesgos a través de:

- Seguimiento contínuo de factores de riesgo: de manera frecuente se debe llevar a cabo un monitoreo contínuo de los factores de riesgo que favorecen a los cambios en el riesgo, sobre los activos, operaciones, individuos de la organización, u otras organizaciones o la Nación.

- Actualización de la evaluación de riesgos: como mecanismo de mejora del proceso de gestión de riesgos, es importante actualizar la evaluación de riesgos realizada, utilizando los resultados del monitoreo contínuo de los factores de riesgo identificados.

5.2 MARCO CONCEPTUAL

Durante el desarrollo de la presente monografía, se abordaron los siguientes términos y definiciones:

- Activo de información. Son aquellos recursos físicos, tecnológicos, de comunicaciones y de información (*hardware* y *software*), con los que cuenta una organización, mediante los cuales se genera, procesa y almacena la información que requiere para su operación y el cumplimiento de sus objetivos.

- Adversario. La guía NIST SP800-30 revisión 1, la define como la entidad, individuo y/o grupo que tiene la intención de efectuar actividades dañinas para la organización.

- Amenaza. Es un agente o evento interno o externo, que aprovechando las vulnerabilidades presentes en los activos de información, es la principal causa que genera un incidente de seguridad, produciendo pérdidas y/o daños a los mismos, afectando de esta forma a la organización. Una amenaza puede ser causada por: los usuarios, programas maliciosos, intrusos, el personal interno de sistemas, los operadores o un siniestro (incendio, inundación, robo, entre otros).

- Análisis. Es el proceso de estudio de un elemento o sujeto de forma detallada, con el fin de conocer sus componentes y las relaciones entre ellos.

- Autenticidad. Considerada por algunas metodologías de gestión de riesgos TIC, como una dimensión de seguridad que se caracteriza por identificar que el sujeto o entidad es quien dice ser, o se conoce la fuente de la cual procede la información.

- *Bring Your Own Device (BYOD*). "Es una tendencia cada vez más generalizada en la que las empresas permiten a los trabajadores llevar sus dispositivos portátiles personales para llevar a cabo tareas del trabajo y conectarse a la red y recursos corporativos."[16]

- Confidencialidad. Pilar de la seguridad de la información, que consiste en garantizar que sólo las personas autorizadas, pueden acceder a la información requerida.

- Condición predisponente. Corresponde a una situación, que por su diseño, ubicación, arquitectura u origen puede constituirse en una debilidad o vulnerabilidad para la organización.

- Control. Es un mecanismo de seguridad preventivo y/o correctivo, utilizado para manejar el riesgo.

- Disponibilidad. Pilar de la seguridad de la información, que consiste en garantizar el acceso y consulta de los sistemas y la información dispuestos de acuerdo al rol y servicio que prestan estos recursos en la organización.

- Frecuencia. Es la medida que indica el número de veces que se presenta un evento positivo o negativo por unidad de tiempo.

[16] COMPUTER HOY. ¿Qué es BYOD?, ventajas e inconvenientes. [en línea]. < http://computerhoy.com/noticias/moviles/que-es-byod-ventajas-e-inconvenientes-7250> [citado 05 de septiembre de 2017]

- Integridad. Pilar de la seguridad de la información, que consiste en garantizar el aseguramiento y preservación de los datos y la información.

- Impacto. Es la consecuencia de que una o varias amenazas ocurran o se materialicen sobre un activo de información, provocándole una determinada degradación o pérdida de su valor.

- Incidente de seguridad. Es cualquier suceso que daña o representa una amenaza importante para la información y los sistemas informáticos y de comunicaciones que hacen parte de una organización.

- Organización. Es una entidad integrada por un conjunto de personas, recursos e instalaciones, las cuales dentro de su estructura organizacional ejercen unas responsabilidades y funciones para el desempeño de su trabajo.

- Probabilidad. Es la medida cualitativa y/o cuantitativa de posibilidad que determina si una vulnerabilidad puede ser explotada por una amenaza.

- Seguridad de la Información. Es la ciencia mediante la cual se definen varios modelos y estándares diseñados para la preservación y aplicación de los principios de confidencialidad, integridad y disponibilidad de la información.

- Seguridad Informática. Es la parte táctica y operacional, de la Seguridad de la Información. Su principal objetivo consiste en asegurar que la información, los recursos y los sistemas de información (*hardware* y *software*) de una organización. Generalmente, la seguridad informática es administrada por el equipo de seguridad de la organización.

- Servidor Judicial. Son las personas que ocupan cargos en las sedes judiciales y en las entidades administrativas de la Rama Judicial.

- Riesgo. Es la posibilidad de que un evento pueda afectar positiva o negativamente a un activo de información de la organización[17], e indica de

[17] ECURED. Seguridad Informática. [en línea]. < https://www.ecured.cu/Seguridad_Inform%C3%A1tica> .[citado 27 de marzo de 2017].

acuerdo a su estimación lo que le podría suceder a los activos en caso de que se presente.

- Sumas de verificación. “Es una función hash que tiene como propósito detectar cambios accidentales en una secuencia de datos para proteger la integridad de estos, verificando que no haya discrepancias entre los valores obtenidos al hacer una comprobación inicial y otra final tras la transmisión.”[18]

- Trazabilidad. Considerada por algunas metodologías de gestión de riesgos TIC, como una dimensión de seguridad mediante la cual se garantiza el saber que sujeto y/o entidad realiza un procedimiento y en qué periodo de tiempo.

- Vulnerabilidad. Son condiciones débiles de los activos de información, que pueden ser explotadas y de esta forma, facilitar la materialización de las amenazas.

5.3 ESTADO DEL ARTE

A través de los años y en la actualidad debido al auge de las tecnologías de la información, las instituciones encargadas de normalizar y estandarizar los temas referentes a la seguridad de la información, han logrado que a través de sus amplios y específicos contenidos, exista un gran interés por parte de las organizaciones públicas o privadas de acoger y adoptar modelos de gestión de riesgos que le permitan conocer de cerca y evaluar el nivel de seguridad de sus activos y sistemas de información.

Llevando de esta forma a las metodologías de gestión de riesgos de sistemas de información, a tomar un papel fundamental como herramienta táctica y operacional, a través de la cual se puedan acometer las actividades para identificar amenazas, vulnerabilidades o deficiencias del sistema, probabilidades e impactos para la determinación de riesgos, la fijación de controles de seguridad y el fortalecimiento de los existentes, prestando especial atención en la evaluación de riesgos para su posterior tratamiento.

[18] WIKIPEDIA. Suma de Verificación. [en línea]. < https://es.wikipedia.org/wiki/Suma_de_verificaci%C3%B3n> .[citado 27 de marzo de 2017].

Bajo este contexto es importante resaltar que el Gobierno de Colombia mediante el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), ha emprendido la labor para que a través de sus distintos programas y proyectos, las organizaciones del estado, se concienticen de la importancia de gestionar los riesgos e incluyan en sus planes estratégicos, la adopción de modelos de seguridad orientados en fortalecer la seguridad de sus recursos tecnológicos y por ende, de todos los activos que la componen. Siguiendo esta misma línea, las organizaciones estatales por norma han implementado al interior de sus organizaciones la metodología establecida por el Departamento Administrativo de la Función Pública (DAFP), mecanismo mediante el cual identifican, valoran y minimizan los riesgos a los que están expuestos, fortaleciendo de manera conjunta el Sistema de Control Interno de la organización, que integra el cumplimiento de los objetivos misionales y los fines esenciales del Estado Colombiano.

No obstante, a las normativas establecidas en el ámbito nacional, es válido proponer la integración de metodologías de gestión de riesgos en materia de seguridad de la información, que le permitan a las organizaciones estar a la vanguardia con la adopción de modelos basados en buenas prácticas internacionales, que le permitan llevar a cabo la gestión de riesgos. Dando paso a esta gran posibilidad, se han generado una serie de estudios sobre las metodologías más reconocidas de análisis de riesgos y se han adoptado bajo el cumplimiento de argumentos sólidos que permitan ajustarse dentro de las organizaciones tomadas como campo de aplicación de estos estudios. Como referencia de estas importantes iniciativas y proyectos se pueden enunciar los siguientes:

- El modelo nacional de gestión de riesgos de seguridad digital del Gobierno de Colombia (MGRSD): este modelo está diseñado por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, fundamentado principalmente en el uso de buenas prácticas nacionales e internacionales para la gestión de riesgos, teniendo como fin contribuir a la prosperidad económica y social del país, por medio de acciones que conlleven al aprovechamiento de un entorno digital seguro[19].

- Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios: este es un proyecto de investigación emprendido por miembros del grupo de investigación de la Universidad Distrital Francisco José de Caldas (Bogotá – Colombia), en el cual presentan una metodología para

[19] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES MinTIC. "Modelo nacional de gestión de riesgos de seguridad digital". [En línea]. <https://www.mintic.gov.co/portal/604/articles-61854_documento.docx>. [citado el 19 de octubre de 2018].

gestionar los riesgos tecnológicos siguiendo los estándares internacionales ISO 31000 e ISO 27005 e integrar estas metodologías a la gestión de continuidad de negocios, analizando su impacto y el desarrollo de estrategias de sus procesos tecnológicos[20].

- Estudio análisis de riesgos en seguridad de la información: estudio realizado por el grupo de investigación MUISCA, de la Facultad de Ingeniería de la Fundación Universitaria Juan de Castellanos (Tunja – Colombia), mediante el cual se exponen y analizan cada uno de los aspectos de las metodologías de análisis de riesgos como: OCTAVE, MEHARI, MAGERIT, CRAMM, EBIOS Y NIST SP 800-30, obteniendo como resultado final el determinar de acuerdo con la estructura de un negocio que metodología es más efectiva y completa para su aplicación[21].

Finalmente, es posible evidenciar que de acuerdo a cada ámbito ya sea estudiantil, corporativo y/o gubernamental, se desprende la iniciativa de trabajar y fortalecer en todos sus aspectos la seguridad de la información, y que mejor forma, el estudiar y aplicar las distintas herramientas y metodologías que ayudan a gestionar y reconocer los riesgos derivados por el uso de los sistemas de información.

[20] RAMÍREZ CASTRO, SANDRA. ORTÍZ BAYONA, Zulima. "Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios". [En línea]. <https://dialnet.unirioja.es/descarga/articulo/4797252.pdf>. [citado el 19 de octubre de 2018].

[21] ABRIL, Ana. Pulido, Jarol. A. Bohada, Jhon. "Análisis de Riesgos en Seguridad de la Información". [En línea]. <http://www.revistasjdc.com/main/index.php/rciyt/article/download/292/283> [citado el 19 de octubre de 2018].

6. ESQUEMA TEMÁTICO

Para el desarrollo de la presente monografía, se ha tomado como objeto de estudio un organismo administrativo de la Rama Judicial, que cuenta con unos activos de información específicos, con un modelo organizacional y operativo que se soporta en los sistemas de información y comunicaciones.

6.1 ORGANIZACIÓN CASO DE ESTUDIO

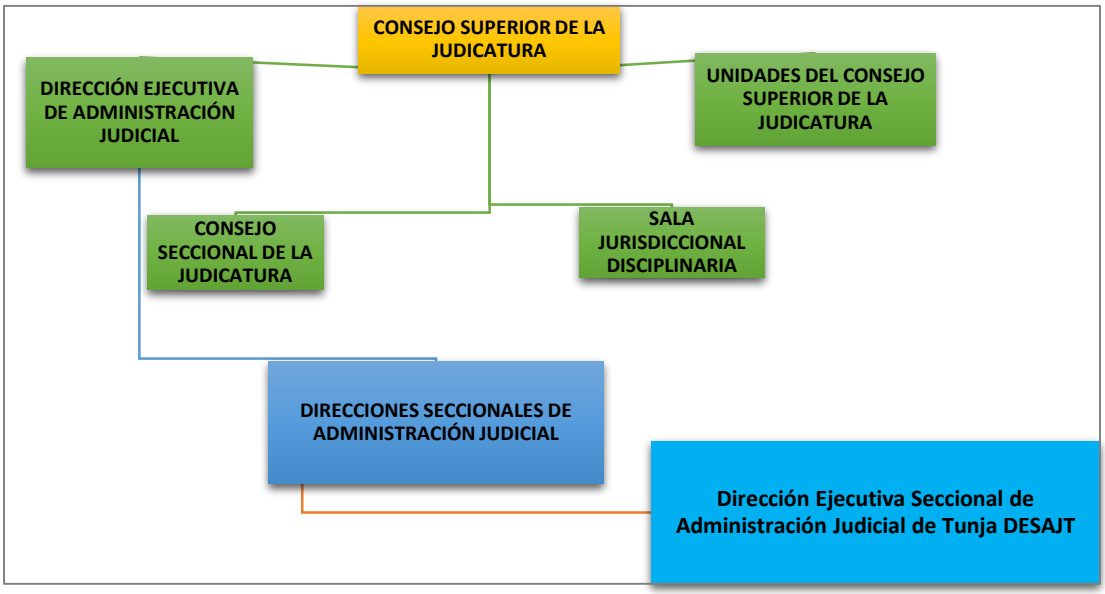
Ésta organización hace parte de una de las seccionales de la Dirección Ejecutiva de Administración Judicial - órgano administrativo y técnico de la Rama Judicial-, la cual realiza sus funciones conforme a la normativa y lineamientos establecidos por el Director Ejecutivo Nacional de la Administración Judicial. Cabe resaltar que dentro de su estructura organizacional, la Dirección Ejecutiva Seccional de Administración Judicial de Tunja - DESAJT, puntualmente apoya la administración de sus recursos tecnológicos y de comunicaciones, en el área de Soporte Tecnológico que se encarga de: i) coordinar proyectos relacionados con tecnologías de la información, ii) administrar y soportar la infraestructura tecnológica y de comunicaciones, bases de datos, sistemas operativos y sistemas de información; funciones donde se origina y gestiona la información de recursos humanos, financiera, administrativa, judicial y tecnológica de las distintas dependencias de la entidad.

A continuación se presenta y describe brevemente el organigrama, misión, visión y estructura de dependencias de la Dirección Ejecutiva Seccional de Administración Judicial de Tunja - DESAJT:

6.1.2 Organigrama de la DESAJT. La Dirección Ejecutiva Seccional de Administración Judicial de Tunja – DESAJT, es uno de los órganos descentralizados que hace parte de Dirección Ejecutiva de Administración Judicial y en estricto orden ascenderte hace parte del Consejo Superior de la Judicatura, el cual se encarga de administrar y planear los recursos de la Rama Judicial de Colombia, y la cual cambia su estructura y renueva su imagen institucional en el mes de agosto del año 2016.

A continuación, se ilustra en orden jerárquico el organigrama del Consejo Superior de la Judicatura de la Rama Judicial de Colombia, encontrando en el recuadro inferior derecho la Dirección Ejecutiva Seccional de Administración Judicial de Tunja – DESAJT (fondo azul).

Figura 8. Organigrama Consejo Superior de la Judicatura



Fuente: el autor

6.1.3 Misión de la DESAJT. "El Consejo Superior de la Judicatura, es el órgano constitucional de administración y control del poder judicial en Colombia, responsable de su administración autónoma para lograr la plena realización del derecho de acceso a la justicia de todos los colombianos propendiendo por la independencia judicial, la calidad, la eficiencia, la eficacia y la transparencia en la gestión pública en orden a propiciar la paz y la convivencia social."[22]

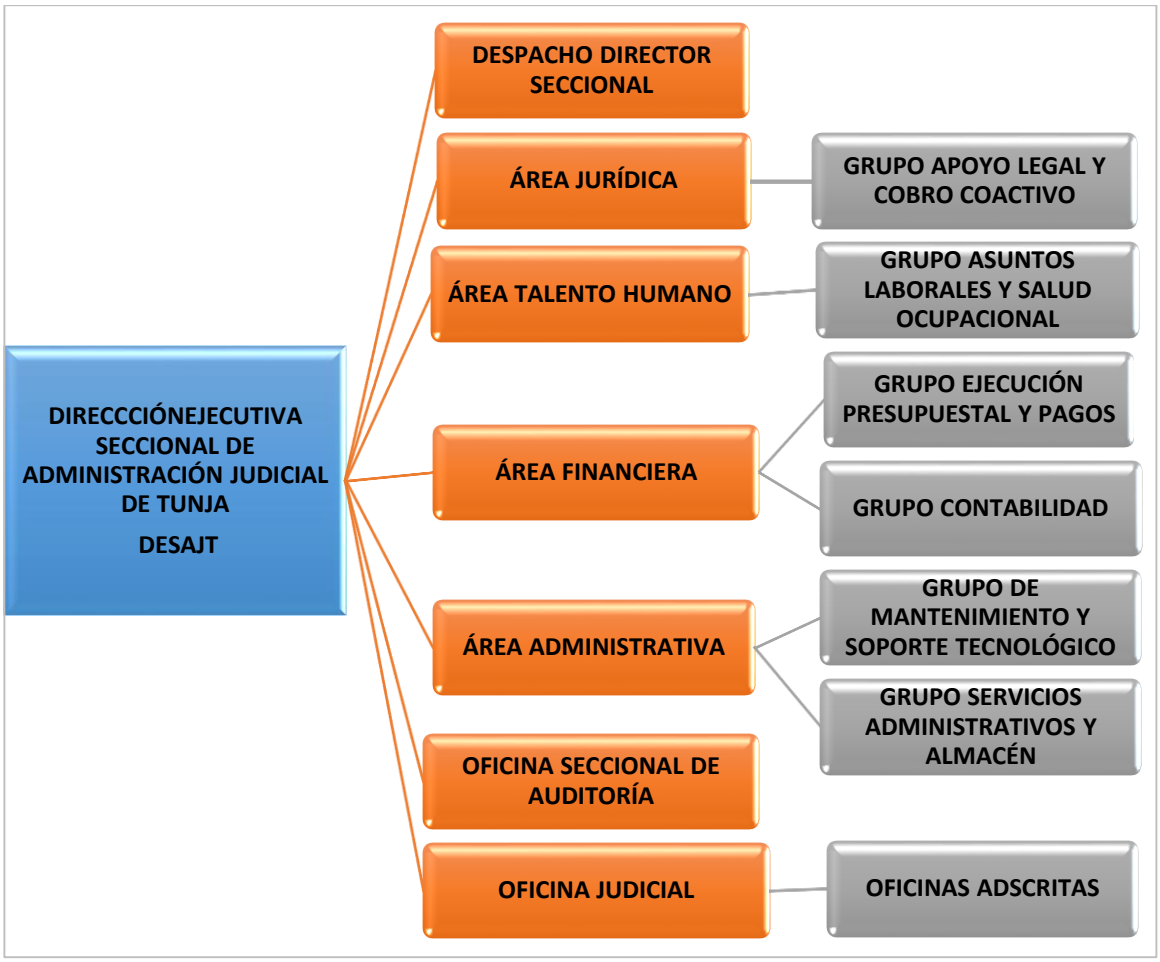
6.1.4 Visión de la DESAJT. "…Seremos la entidad que en consideración a sus características internas y reconocimiento externo, asegurará la efectiva prestación de un servicio de administración de la justicia, esto es, con eficiencia y calidad, en el que la adecuada utilización de todos los recursos, el compromiso de su gente y la confiabilidad de sus procesos la harán modelo de gestión del estado Colombiano."[23]

[22]ESCUELA JUDICIAL RODRIGO LARA BONILLA. La Sala Administrativa del Consejo Superior de la Judicatura y sus Seccionales como parte del Modelo de Gobierno Judicial. [en línea]. <http://w1.cejamericas.org/index.php/biblioteca/biblioteca-virtual/doc_download/6932-la-sala-administrativa-del-consejo-superior-de-la-judicatura.html>[citado el 8 de Agosto de 2017].

[23]ESCUELA JUDICIAL RODRIGO LARA BONILLA. La Sala Administrativa del Consejo Superior de la Judicatura y sus Seccionales como parte del Modelo de Gobierno Judicial. [en línea]. <http://w1.cejamericas.org/index.php/biblioteca/biblioteca-virtual/doc_download/6932-la-sala-administrativa-del-consejo-superior-de-la-judicatura.html>[citado el 8 de Agosto de 2017].

6.1.5 Estructura de dependencias de la DESAJT. La Dirección Ejecutiva Seccional de Administración Judicial de Tunja - DESAJT, dentro de su estructura seccional, tiene a cargo las siguientes dependencias:

Figura 9. Estructura organizacional seccional DESAJT



Fuente: el autor

La Dirección Ejecutiva Seccional de Administración Judicial de Tunja – DESAJT, atendiendo la directriz institucional de la entidad, a partir del año 2007 cuenta con el Sistema Integrado de Gestión y Control de la Calidad y el Medio Ambiente - SIGCMA, fundamentado en las Normas NTCGP1000:2009 – Norma Técnica de Calidad en la Gestión Pública, ISO 9001 - Norma Internacional y el Modelo Estándar de Control Interno –MECI.

Sistema Integrado de Gestión de Calidad que se encuentra implementado en su totalidad en el nivel central y en las seccionales, y está orientado en alcanzar los principios de calidad, control y medio ambiente, tendientes a garantizar la "satisfacción de los usuarios, la preservación del medio ambiente y la generación de controles efectivos, que le permitan el cumplimiento de su misión institucional"[24] y elementos esenciales de su modelo de gestión. Bajo este contexto, la entidad lleva a cabo sus actividades de planeación, gestión y control a través de un esquema basado en los siguientes procesos[25]:

- Procesos estratégicos: son aquellos que le permiten a la entidad, definir los mecanismos y herramientas que le permiten fortalecer todos los planes, proyectos de la organización, teniendo en cuenta los lineamientos y objetivos institucionales; además le permiten garantizar el cumplimiento y seguimiento de su quehacer, orientada en generar una retroalimentación y mejoramiento de su SIGCMA. El principal propósito de estos procesos, es el de generar las condiciones adecuadas para la administración de los recursos de la Rama Judicial. A continuación se indican los procesos estratégicos del Sistema Integrado de Gestión y Control de Calidad y Medio Ambiente – SIGCMA de la Calidad de la entidad:

    - Planeación estratégica.
    - Gestión para la integración de listas de Altas Cortes.
    - Comunicación institucional.
    - Mejoramiento del Sistema Integrado de Gestión y Control de la Calidad.

- Procesos misionales: son aquellos procesos en los que se centran la mayoría de los servicios que la entidad presta a la comunidad judicial y sus usuarios. En estos procesos se fundamenta la misión de la entidad, involucrando la gestión de las actividades administrativas y judiciales, fortaleciendo las condiciones necesarias en la prestación del servicio en sus diferentes áreas.

---

[24] CONSEJO SUPERIOR DE LA JUDICATURA. Políticas del SIGCMA. [en línea]. <http://sistemagestioncalidad.ramajudicial.gov.co/ModeloCSJ/portal/index.php?idcategoria=184>. [citado el 21 de Septiembre de 2017].

[25] CONSEJO SUPERIOR DE LA JUDICATURA. Manual calidad 2013. [en línea]. < http://sistemagestioncalidad.ramajudicial.gov.co/ModeloCSJ/portal/index.php?idcategoria=195>. [citado el 24 de Noviembre de 2013].

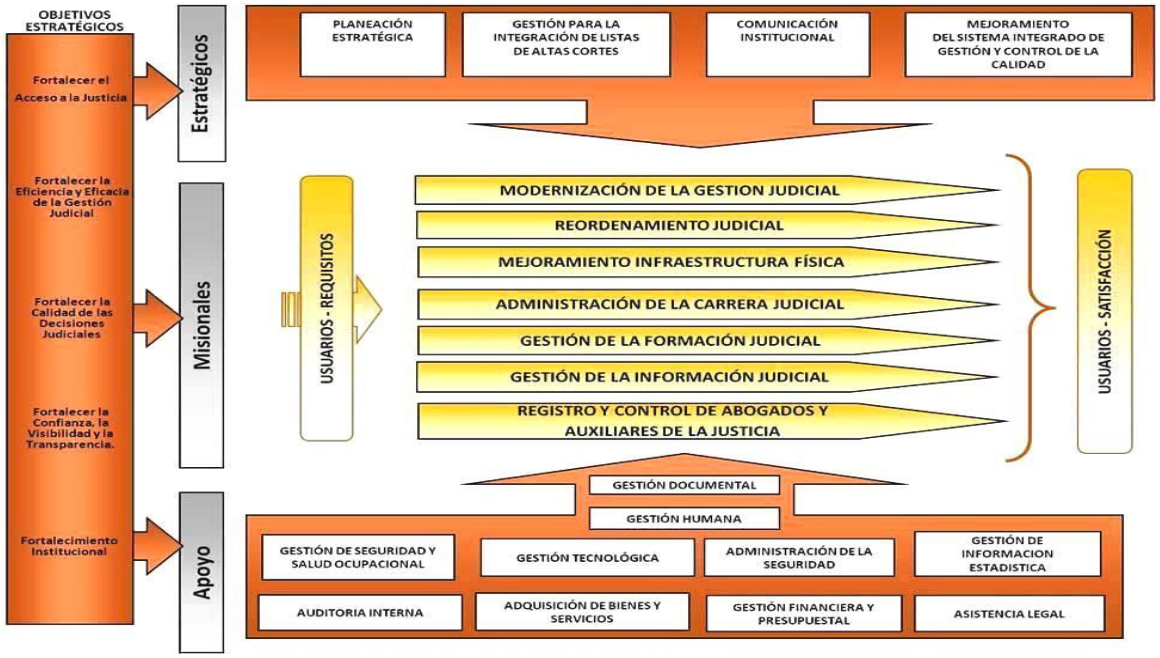
- Modernización de la gestión judicial.
- Reordenamiento judicial.
- Mejoramiento infraestructura física.
- Administración de la carrera judicial.
- Gestión de la formación judicial.
- Gestión de la información judicial.
- Registro y Control de abogados y auxiliares de justicia.

- Procesos de apoyo: son aquellos procesos en los que la entidad a través de sus recursos: humano, presupuestal, judicial, tecnológico, físico (infraestructura) y de información; se promueven el desarrollo de los procesos institucionales, generando al interior de la entidad: seguridad y bienestar ocupacional, la administración, manejo adecuado y mantenimiento de sus recursos, la verificación, consolidación y evaluación de su información en lo que respecta a trámites y servicios realizados por las dependencias administrativas de la entidad.

  - Gestión humana.
  - Gestión tecnológica.
  - Auditoria interna.
  - Administración de la seguridad.
  - Gestión de información estadística
  - Adquisición de bienes y servicios.
  - Gestión financiera y presupuestal.
  - Asistencia legal.
  - Gestión documental.
  - Gestión de seguridad y salud ocupacional.

De acuerdo con la anterior estructura, estos procesos se relacionan entre sí y originan el mapa de procesos del Sistema Integrado de Gestión y Control de Calidad y Medio Ambiente – SIGCMA de la entidad, que se ilustra en la siguiente figura.

Figura 10. Mapa de procesos del SIGCMA



Fuente: http://sistemagestioncalidad.ramajudicial.gov.co/ModeloCSJ/imagenes/Mapa_procesos_CSJ.jpg

Mediante este mapa de procesos, se indican los objetivos estratégicos de la entidad (parte izquierda), que aportan valor a cada uno de los procesos principales – Estratégicos, Misionales y de Apoyo-, constituyéndose como elementos de entrada al SIGCMA, de acuerdo con las distintas gestiones que se generan en pro de la consecución de dichos objetivos.

Cada Proceso principal contempla un conjunto de actividades de los cuales una dependencia de la entidad es proveedora del servicio y/o responsable, además se encuentran los distintos procedimientos que intervienen para llevar a cabo el proceso, generando los resultados que se constituyen en las salidas del sistema, las cuales van dirigidas a un cliente o usuario de la organización. Con el objetivo de identificar los activos de Información específicos administrados por la Dirección Ejecutiva Seccional de Administración Judicial de Tunja – DESAJT, se ha tenido en cuenta la estructura de procesos del Sistema Integrado de Gestión y Control de la Calidad y el Medio Ambiente – SIGCMA de la entidad, donde se identifican los

recursos de cada proceso de acuerdo con la estructura de dependencias de la organización y los servicios que prestan dentro de la misma.

6.2 IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN DE LA ORGANIZACIÓN.

La identificación de los activos de información de la entidad, se realizó teniendo en cuenta cada uno de los procesos de apoyo del SIGCMA, en los cuales intervienen cada una de las dependencias administrativas de la Dirección Ejecutiva Seccional de Administración Judicial de Tunja – DESAJT, y el Consejo Seccional de la Judicatura, tal como se muestra en la siguiente figura.

Figura 11. Procesos de apoyo del SIGMA vs. Estructura organizacional de la entidad

Fuente: el autor

Después de conocer la forma en la que cada dependencia administrativa de la entidad y el Consejo Seccional de la Judicatura, hace parte de los procesos de apoyo del Sistema Integrado de Gestión y Control de Calidad y Medio Ambiente – SIGCMA, a continuación se indican de manera general los criterios a tener en cuenta en Seguridad Informática, para identificar los activos de información fundamentales con los que puede contar una organización:

- La información y/o los datos que se manejan en cada una de las dependencias de la organización.

- Los servicios que se prestan dentro y fuera de la organización.

- La infraestructura tecnológica y de comunicaciones (*hardware*, *software* y redes) mediante los cuales se gestiona, transmite y accede a la información o a un sistema informático dentro de la organización.

- Las instalaciones físicas en las cuales se encuentran ubicadas las oficinas y los recursos tecnológicos y de comunicaciones, de la organización.

- El personal de cada una de las dependencias de la organización, los usuarios y clientes externos de la organización.

Atendiendo los criterios anteriormente citados, en la tabla 7 se lista el inventario de activos de información administrados, gestionados, controlados y utilizados por la Dirección Ejecutiva Seccional de Administración Judicial de Tunja – DESAJT, los cuales se han de tener en cuenta para la seleccionar la metodología de gestión de riesgos en materia de la seguridad de la información.

Tabla 3. Inventario de activos de información de la DESAJT

Tipo de Activo	Dependencia responsable	Activo	Descripción del activo
Información: Documentación física o impresa de la entidad.	Despacho de la Dirección	Oficios, Resoluciones.	Documentos emitidos por el Despacho de la Dirección Seccional.
		Manuales de Procedimientos.	Documentación de los procedimientos que realiza cada dependencia administrativa de la entidad.
		Archivos de gestión del despacho de la Dirección Seccional.	Documentos físicos que hacen parte del archivo de gestión (solicitudes y respuestas) del despacho de la Dirección Seccional.
	Oficina de Auditoria	Planes de auditoria.	Documentación de los planes y programas de auditoria, aplicados a las dependencias administrativas y

Tabla 3. (Continuación)

Tipo de Activo	Dependencia responsable	Activo	Descripción del activo
			despachos judiciales de la seccional.
		Archivos de gestión de la oficina de auditoría.	Documentos físicos que hacen parte del archivo de gestión (solicitudes, informes y respuestas) de la oficina de auditoria.
	Área Jurídica	Procesos jurídicos.	Expedientes físicos del área jurídica y cobro coactivo de la entidad.
		Archivos de gestión del área jurídica.	Documentos físicos que hacen parte del archivo de gestión (solicitudes y respuestas) del área jurídica y cobro coactivo de la entidad.
	Área Talento Humano	Hojas de Vida y novedades de los empleados y servidores judiciales.	Documentación de la hoja de vida y novedades de cada servidor judicial.
		Documentos de nómina y cesantías de los empleados y servidores judiciales.	Documentación de la nómina y cesantías de cada servidor judicial.
		Documentos de salud ocupacional.	Documentación de casos de salud ocupacional de los servidores judiciales.
		Archivos de gestión del área de talento humano.	Documentos físicos que hacen parte del archivo de gestión (solicitudes y respuestas) del área de talento humano de la entidad.
	Área Financiera	Documentación Financiera.	Documentación correspondiente a: libranzas, Registros Presupuestales, Certificados de disponibilidad, entre otros, soportes de la entidad.
		Archivos de gestión del área financiera.	Documentos físicos que hacen parte del archivo de gestión (solicitudes y respuestas) del área financiera de la entidad.

Tabla 3. (Continuación)

Tipo de Activo	Dependencia responsable	Activo	Descripción del activo
	Área Administrativa	Contratos.	Documentos de los procesos de contratación celebrados por la entidad con terceros.
		Inventarios.	Documentos de ingresos, movimientos y egresos de la sección de almacén.
		Archivos de gestión del área administrativa.	Documentos físicos que hacen parte del archivo de gestión (solicitudes y respuestas) del área administrativa de la entidad.
		Correspondencia Interna.	Son los documentos generados internamente por las dependencias administrativas de la entidad.
		Correspondencia Externa.	Son las solicitudes radicadas por usuarios, entidades externas y despachos judiciales, en la oficina de correspondencia de la entidad.
	Grupo de Mantenimiento y Soporte Tecnológico	Manuales de Sistemas de Información.	Documentación sobre los manuales de administración y de usuario, de los sistemas de información de la entidad.
		Manuales de *hardware*.	Documentación relacionada a los equipos informáticos y de comunicaciones adquiridos por la entidad.
		Archivos de gestión del área de mantenimiento y soporte tecnológico.	Documentos físicos que hacen parte del archivo de gestión (solicitudes y respuestas) del área de mantenimiento y soporte tecnológico de la entidad.
	Oficina Judicial y Oficinas Adscritas	Procesos Judiciales.	Expedientes físicos recibidos en las Oficinas adscritas a la entidad

Tabla 3. (Continuación)

Tipo de Activo	Dependencia responsable	Activo	Descripción del activo
		Depósitos judiciales.	Documentos físicos de los depósitos judiciales constituidos para los despachos judiciales y las oficinas adscritas de la entidad.
		Archivos de gestión de la oficina judicial, de servicios y de apoyo de la seccional.	Documentos físicos que hacen parte del archivo de gestión (solicitudes y respuestas) de las oficinas adscritas de la seccional.
	Despachos Judiciales y Consejo Seccional de la Judicatura	Procesos Judiciales.	Demandas judiciales en físico.
		Archivos de gestión de los despachos judiciales de la seccional.	Documentos físicos que hacen parte del archivo de gestión (solicitudes y respuestas) de los despachos judiciales.
Datos informatizados: Es la información que se encuentra almacenada en un archivo digital, sistema o medio informático.	Grupo de Mantenimiento y Soporte Tecnológico	Bases de Datos.	Corresponde al conjunto de datos ingresados y procesados por los Sistemas de Información de la entidad y se encuentran almacenados de forma organizada en una Base de datos.
	Todas las dependencias administrativas, despachos judiciales y Consejo Seccional de la Judicatura	Copias de seguridad.	Corresponde a los archivos de *backups* o copias de seguridad de la información de las dependencias administrativas y despachos judiciales almacenados en equipos y/o soportes de información.
		Archivos digitales.	Corresponde al conjunto de datos y ficheros en formato digital: documentos de ofimática, grabaciones de audio, grabaciones de audio y video.
		Archivos de gestión interna.	Son los archivos y ficheros digitales generados por labor de las dependencias administrativas y despachos judiciales de la entidad.

Tabla 3. (Continuación)

Tipo de Activo	Dependencia responsable	Activo	Descripción del activo
Servicios: Son las funciones que prestan los sistemas informáticos y de comunicaciones de la entidad, mediante las cuales se satisfacen las necesidad de los servidores judiciales y usuarios externos (usuarios del servicio).	Grupo de Mantenimiento y Soporte Tecnológico	Servicio de DNS.	Aplicación que realiza la resolución de nombres de dominio para equipos de los servidores judiciales se conectan a la red de la entidad.
		Servicio de DHCP.	Protocolo de red que realiza la asignación de direcciones ip a los equipos de los servidores judiciales conectados a la red de la entidad.
		Servicio de Directorio Activo.	Aplicación que soporta la autenticación de los usuarios (asignados a los servidores judiciales) para el acceso, a los sistemas operativos de las estaciones de trabajo y equipos servidores de la entidad.
		Servidor de actualizaciones WSUS.	Aplicación que proporciona los servicios de actualización de los sistemas operativos de las estaciones de trabajo y equipos servidores de la entidad.
	Todas las dependencias administrativas y despachos judiciales	*World Wide Web.*	Servicio al cual pueden acceder los servidores judiciales de la entidad.
		Correo electrónico institucional	Servicio de correo y *ondrive* al cual pueden acceder los servidores judiciales de la entidad.
	Despachos judiciales y público en general.	Consulta en línea del estado de los procesos judiciales y sus actuaciones a cargo de los despachos judiciales.	Servicio al que pueden acceder los empleados y clientes de la entidad.

Tabla 3. (Continuación)

Tipo de Activo	Dependencia responsable	Activo	Descripción del activo
Software: Es el conjunto de aplicaciones o programas instalados en un sistema informático, que reciben y gestionan los datos.	Grupo de Mantenimiento y Soporte Tecnológico	Sistemas de Gestión de Bases de Datos.	Administra las bases de datos de los sistemas de información de la entidad.
		Sistemas Operativos equipos servidores.	Sistema operativo de los servidores de la entidad.
		Sistema administrador de copias de seguridad.	Aplicación que permite realizar de forma programada copias de seguridad de las bases de datos del sistema.
	Todas las dependencias administrativas, despachos judiciales y Consejo Seccional de la Judicatura	Sistemas Operativos equipos de cómputo y portátiles.	Sistema operativo de los equipos de cómputo y portátiles de trabajo de la entidad.
		Antivirus.	Aplicación mediante la cual se protege el sistema detectando y eliminando amenazas o virus informáticos, protegiendo de esta forma los equipos servidores y estaciones de trabajo de la entidad.
		Herramientas de ofimática y utilitarios.	Aplicaciones que permiten crear archivos digitales que le permitan, manejar, transmitir y almacenar la información necesaria de las dependencias administrativas y despachos judiciales de la entidad.
	Despachos judiciales	Sistema de Información Justicia XXI.	Aplicación Cliente / Servidor mediante la cual se registra y consultan los procesos judiciales y sus actuaciones.
		Sistema de videoconferencia.	Aplicación que permite la conexión a videoconferencias y/o audiencias judiciales de forma virtual.
	Todas las dependencias administrativas y Consejo	Sistema de gestión de correspondencia.	Sistema a través del cual se administran las comunicaciones oficiales de la entidad.

Tabla 3. (Continuación)

Tipo de Activo	Dependencia responsable	Activo	Descripción del activo
	Seccional de la Judicatura		
Hardware: Son los equipos informáticos y de comunicaciones donde se almacenan y transmiten los datos y mediante los cuales se soportan los servicios que presta la entidad.	Grupo de Mantenimiento y Soporte Tecnológico	Equipos Servidores.	Equipo con características robustas, donde se gestiona toda la información de las bases de datos corporativas, se realizan las configuraciones para el acceso y la prestación de servicios al personal de la entidad y se alojan las aplicaciones.
		Equipo de almacenamiento copias de seguridad.	Equipo donde se almacenan las copias de seguridad de las Bases de datos, archivos planos y archivos digitales de trabajo de los servidores judiciales de la entidad.
		Equipos de respaldo.	Son los equipos y dispositivos preparados para ser un respaldo en caso de daño o falla en los equipos y dispositivos de producción de la entidad.
		Router.	Dispositivo que permite la interconexión de redes LAN y se utilizan básicamente para los servicios de Internet.
		Switchs.	Dispositivo analógico que permite la interconexión de equipos tecnológicos en red.
		PBX.	Equipos del conmutador telefónico de la entidad.
	Todas las dependencias administrativas, despachos judiciales y Consejo Seccional de la Judicatura	Equipos de cómputo.	Equipos asignados a los servidores judiciales de la entidad.
		Computadoras Portátiles.	Equipos portátiles asignados a los servidores judiciales de la entidad.

Tabla 3. (Continuación)

Tipo de Activo	Dependencia responsable	Activo	Descripción del activo
		Medios de impresión.	Impresoras de la entidad.
		Escáneres.	Escáneres de la entidad.
		Fotocopiadoras.	Fotocopiadoras contratadas por la entidad con terceros.
Redes de Comunicaciones: son las interconexiones o instalaciones dedicadas al transporte que llevan datos de un lugar a otro dentro y fuera de la entidad.	Área administrativa y grupo de mantenimiento y soporte tecnológico.	Red de área local	Conformada por la interconexión alámbrica de equipos y dispositivos tecnológicos, que conforman la red local de la entidad.
		Red Telefónica	Conformada por la interconexión alámbrica de dispositivos telefónicos, que conforman la red telefónica de la entidad.
	Proveedor de servicio de internet (tercero)	Red de internet	Es la infraestructura de telecomunicación conformada por la interconexión de fibra óptica de dispositivos de la red de datos y el proveedor de internet.
Soportes de Información: Son los dispositivos o medios físicos que permiten almacenar la información por un tempo corto o permanente.	Todas las dependencias administrativas, despachos judiciales y Consejo Seccional de la Judicatura	Discos duros extraíbles portables.	Sistema de almacenamiento de datos, donde se guardan las copias de seguridad de las bases de datos de los sistemas de información de la entidad, archivos de trabajo y audiencias de los despachos judiciales.
		Discos CD y DVD.	Discos ópticos que permiten almacenar información de manera permanente, como informes, audiencias, archivos de trabajo de las dependencias y despachos judiciales de la entidad.
		Memorias USB.	Dispositivos usb donde se almacenan de forma temporal información de archivos digitales de las dependencias y despachos judiciales de la entidad.
Equipamiento auxiliar: Son los equipos en los cuales se soportan o	Área administrativa y grupo de mantenimiento	Sistemas de alimentación Ininterrumpida - UPS.	Dispositivo que suministra energía eléctrica por un lapso de tiempo determinado, a todos los dispositivos que tenga conectados,

Tabla 3. (Continuación)

Tipo de Activo	Dependencia responsable	Activo	Descripción del activo
apoyan los sistemas informáticos y de comunicaciones de la entidad.	y soporte tecnológico.		durante una interrupción del servicio eléctrico o de energía.
		Equipos de climatización.	Sistemas y equipamiento utilizados para ejercer el adecuado control de los niveles de temperatura, humedad y otras condiciones ambientales dentro de las oficinas y cuartos de comunicaciones de la entidad.
		Equipos de extinción de incendios.	Componentes que en conjunto permiten la extinción de incendios.
		Cableado sistema eléctrico.	Conjunto de cables que forman parte de un aparato o sistema eléctrico.
		Cableado de red.	Conjunto de cables que forman parte de la LAN (Red de área local) de la entidad.
		Fibra óptica.	Sistema de cableado de fibra óptica que permite conectar la red de área local de la entidad.
Instalaciones: Son los lugares que albergan los activos de información de la entidad.	Grupo de Mantenimiento y Soporte Tecnológico	Cuarto de comunicaciones.	Sitio donde se concentran los equipos de comunicaciones: racks, *routers*, *switchs* y Pbx, que permiten la transmisión de voz y datos, en la red de telefonía, red local (LAN) e internet.
		Cuarto de servidores.	Sitio donde se concentran los equipos servidores de la entidad.
	Todas las dependencias administrativas, despachos judiciales y Consejo	Oficinas.	Lugares de trabajo de los servidores judiciales dispuestos en la entidad.

Tabla 3. (Continuación)

Tipo de Activo	Dependencia responsable	Activo	Descripción del activo
	Seccional de la Judicatura		
Personal: Son las personas que interactúan con los activos de información de la entidad.	Grupo de mantenimiento y soporte tecnológico.	Administradores del sistema.	Ingenieros de sistemas de la entidad, con el rol de administrador del sistema.
	Área administrativa y grupo de mantenimiento y soporte tecnológico.	Contratistas y Terceros	Personal que prestan sus servicios a la entidad.
	Todas las dependencias administrativas, despachos judiciales y Consejo Seccional de la Judicatura	Servidores Judiciales	Magistrados, Funcionarios, empleados administrativos y de los despachos judiciales de la seccional.
	Todas las dependencias administrativas, despachos judiciales y Consejo Seccional de la Judicatura	Público en general	Usuarios externos de la entidad.
Fuente: el autor			

Con este inventario de activos de la entidad, se pretende analizar cuál de las dos metodologías estudiadas: MAGERIT versión 3 y NIST SP800-30 revisión 1, se ajusta más a los activos de información y a los requisitos de seguridad de información que requiere la entidad.

6.3 SELECCIÓN DE LA METODOLOGÍA DE GESTIÓN DE RIESGOS PARA LOS SISTEMAS DE INFORMACIÓN

Con el propósito de seleccionar la metodología de gestión de riesgos para sistemas de información, según el tema de estudio y atendiendo los objetivos propuestos en la presente monografía, a continuación se enuncian los temas desarrollados en esta sección:

- Analizar cada uno de los aspectos que contemplan las metodologías de gestión de riesgos MAGERIT versión 3 y NIST SP800-30 revisión 1, con el objetivo de comparar cada una de las actividades de análisis y evaluación de riesgos y obtener las fortalezas y bondades que ofrece cada una de ellas.

- Tomar la matriz de riesgos del SIGCMA de la organización y determinar los aspectos del análisis y evaluación de riesgos que le aportan mayor valor a las necesidades de seguridad, seleccionando la metodología que la organización puede adoptar.

6.3.1 Análisis de las metodologías de gestión de riesgos MAGERIT versión 3 y NIST SP800-30 revisión 1.

De acuerdo con la documentación de cada metodología, en esta sección se presentan las actividades principales, etapas, pasos, tareas y subtareas definidas en el proceso de gestión de riesgos para los sistemas y tecnologías de información, definidos en la metodología MAGERIT versión 3 y la guía NIST SP800-30 revisión 1. Lo anterior, con el objeto de conocer de cerca y profundizar los aspectos más relevantes y apremiantes que hace parte de este estudio de las dos metodologías de gestión de riesgos para sistemas de información. A continuación se presentan los resultados de este estudio.

6.3.1.1 MAGERIT versión 3:

La metodología MAGERIT versión 3 propone dos actividades para llevar a cabo la gestión de riesgos, de forma estructurada se inicia con la actividad de análisis de riesgos y con los resultados obtenidos de esta actividad, se emprende la evaluación y el tratamiento de riesgos, que de manera conjunta hacen parte de la segunda actividad correspondiente al tratamiento de riesgos. Estas dos tareas le permiten a la organización determinar el estado de seguridad de sus activos, cuan apropiados y seguros son sus mecanismos de protección o qué medidas de seguridad se deben implementar para llevar a cabo el control de riesgos.

Figura 12. Proceso de gestión de riesgos con MAGERIT versión 3

Fuente: el autor

La primera tarea es el análisis de riesgos y de ella ese desprenden una serie de pasos que le permiten a la organización iniciar este proceso de gestión de riesgos:

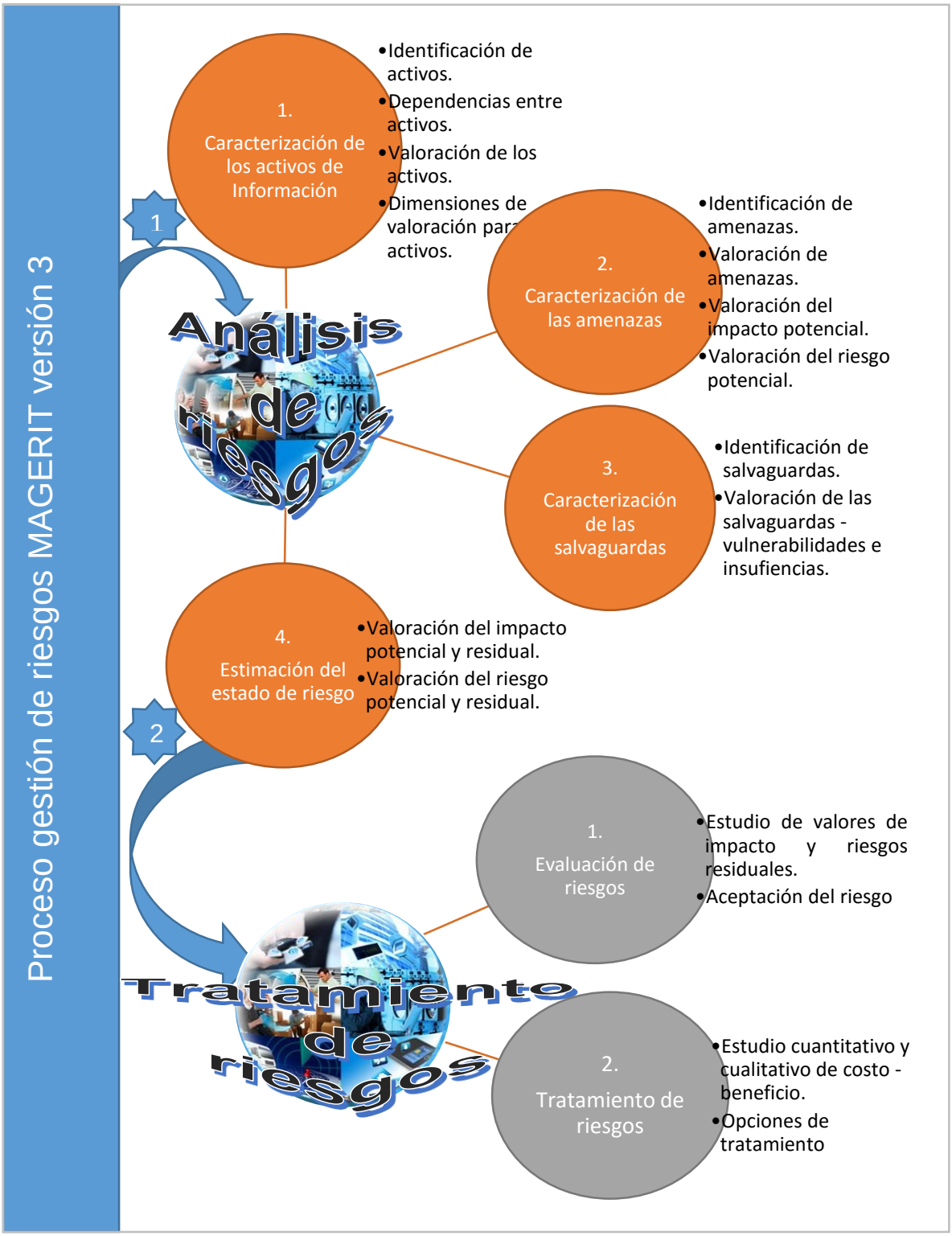
a) Paso 1: Identificación de activos, b) Paso 2: Identificación de amenazas, c) Paso 3: Identificación de salvaguardas, d) Paso 4: Estimación del impacto residual y e) Paso 5: Estimación del riesgo residual.

La segunda tarea es el tratamiento de riesgos, que incluye esencialmente una evaluación de riesgos que permite conocer cómo la organización debe responder ante los riesgos:

a) Actividad 1: Evaluación de riesgos, b) Actividad 2: Aceptación del riesgo, c) Actividad 3: Tratamiento de riesgos, d) Actividad 4: Estudios cuantitativos, cualitativos y mixtos de coste / beneficio y e) Actividad 5: Opciones de tratamiento de riesgos.

A continuación se ilustran de manera conjunta las actividades y tareas del proceso de gestión de riesgos de MAGERIT versión 3.

Figura 13. Actividades de análisis y tratamiento de riesgos con MAGERIT versión 3



Fuente: el autor

De acuerdo con la anterior ilustración, fácilmente se identifica el esquema de actividades y tareas del proceso de gestión de riesgos de MAGERIT versión 3; no obstante, es clave detallar cada una de las sub-tareas del análisis de riesgos, es por esto que en la siguiente tabla se describen qué herramientas brinda la metodología, cual es el trabajo que debe realizar la organización respecto de cada sub-tarea y los resultados e informes que se obtienen al finalizar cada paso del análisis de riesgos.

Tabla 4. Descripción del método de análisis de riesgos – MAGERIT versión 3

Pasos del método / Actividad	Sub-tareas	Elementos de apoyo de la metodología	A cargo de la Organización	Resultados / Informes
1. Caracterización de los activos de Información.	Identificación de los activos.	Catálogo de tipos de activos.	Tomar como referencia el catálogo de tipos de activos.	Identificación de activos de información que componen el sistema.
	Dependencias entre activos.	Consejos prácticos para descubrir y modelar las dependencias entre activos.	Identificar las relaciones entre los diferentes activos.	Obtener el árbol de dependencias entre activos.
	Valoración de los activos.	Criterios de valoración.	Determinar el valor de un activo, de acuerdo con la importancia para la organización.	Obtener el valor propio de un activo o acumulado de acuerdo a los activos que se apoyan en ellos.
	Dimensiones de valoración para los activos.	Dimensiones de valoración.	Tomar como referencia las dimensiones de seguridad de la metodología.	Reconocer en qué dimensión de seguridad es importante cada activo y valorar su importancia para la organización.
	Informe de esta actividad: se obtiene el modelo valor, donde se identifica el valor y las dependencias que representan los activos para la organización.			
2. Caracterización de las amenazas	Identificación de las amenazas.	Catálogo de amenazas posibles sobre un activo.	Tomar como referencia el catálogo amenazas.	Identificación de amenazas relevantes sobre cada activo de información dentro del entorno del sistema.
	Valoración de las amenazas.	Criterios cuantitativos y cualitativos y escalas	Estimar la frecuencia de ocurrencia y el grado de	Estimación de la frecuencia y degradación y afectación de los

Tabla 4. (Continuación)

Pasos del método / Actividad	Sub-tareas	Elementos de apoyo de la metodología	A cargo de la Organización	Resultados / Informes
		para la valoración de amenazas.	afectación que causaría una amenaza en cada dimensión de los activos.	activos con la materialización de una amenaza.
	Informe de esta actividad: se obtiene el mapa de riesgos donde se muestran las posibles amenazas, representadas por su frecuencia de ocurrencia y la degradación que causarían a los activos de información.			
3. Caracterización de las salvaguardas	Identificación de las salvaguardas pertinentes.	Catálogo de salvaguardas.	Tomar como referencia el catálogo de salvaguardas.	Identificación de las salvaguardas que permiten hacer frente a las amenazas reconocidas.
	Valoración de las salvaguardas.	Tipos de protección prestados por las salvaguardas.	Estimar la eficacia de las salvaguardas identificadas.	Estimación de las salvaguardas implantadas, de acuerdo a su efectividad.
	Informe de esta actividad: se obtienen dos informes la relación de las salvaguardas necesarias denominada “Declaración de Aplicabilidad” y se obtiene un informe de insuficiencias donde se relacionan las vulnerabilidades existentes en las salvaguardas desplegadas o la falta de salvaguardas según el caso.			
4. Estimación del estado del riesgo	Estimación del impacto potencial.	Criterios para la estimación del impacto potencial.	Tomar los informes de caracterización de activos, amenazas y salvaguardas.	Estimación del impacto potencial (o lo que puede ocurrir) al que están expuestos los activos, sin tener en cuenta las salvaguardas implantadas.
	Estimación del impacto residual.	Criterios para la estimación del impacto residual.		Estimación del impacto residual al que están expuestos los activos, temiendo en cuenta la eficacia de las salvaguardas implantadas.
	Estimación del riesgo potencial.	Criterios para la estimación del riesgo potencial.	Tomar los informes de caracterización de activos, amenazas, salvaguardas y estimaciones del impacto	Estimación del riesgo potencial (lo que probablemente ocurra) al que están sometidos los activos, sin tener en cuenta las salvaguardas implantadas.

Tabla 4. (Continuación)

Pasos del método / Actividad	Sub-tareas	Elementos de apoyo de la metodología	A cargo de la Organización	Resultados / Informes
	Estimación del riesgo residual.	Criterios para la estimación del riesgo residual.	potencial y residual.	Estimación del riesgo residual al que están sometidos los activos, temiendo en cuenta la eficacia de las salvaguardas implantadas.
	Informe de esta actividad: se obtienen informes sobre el impacto y el riesgo, potenciales y residuales por activo frente a cada amenaza; de igual forma, se obtiene un informe de vulnerabilidades en el sistema de salvaguardas.			
Fuente: autora				

Con los resultados derivados del análisis de riesgos, donde se obtiene la caracterización de activos, amenazas, salvaguardas, la estimación del impacto y riesgo residual, y que dentro del esquema de actividades del procesos de gestión de riesgos, estos resultados se constituyen en las entradas para el tratamiento de riesgos. A continuación en la siguiente tabla, se describen cada una de las sub-tareas de la evaluación y tratamiento de riesgos, donde se muestran qué herramientas brinda la metodología, cual es el trabajo que debe realizar la organización respecto de cada sub-tarea y los resultados e informes que se obtienen al finalizar cada paso de esta actividad.

Tabla 5. Descripción del método de evaluación y tratamiento de riesgos – MAGERIT versión 3

Pasos del método / Actividad	Sub-tareas	Elemento de la metodología	A cargo de la Organización	Resultados / Informes
1. Evaluación de riesgos.	Interpretación de valores de impacto.		Evaluar el contexto de seguridad de los activos respecto de los valores de impacto obtenidos con la estimación del estado del riesgo.	La organización toma decisiones para iniciar el tratamiento de riesgos.
	Interpretación de valores de riesgo.		Evaluar el contexto de	La organización toma decisiones para

Tabla 5. (Continuación)

Pasos del método / Actividad	Sub-tareas	Elemento de la metodología	A cargo de la Organización	Resultados / Informes
			seguridad de los activos respecto de los valores de riesgo obtenidos con la estimación del estado del riesgo.	iniciar el tratamiento de riesgos.
	Aceptación del riesgo.		Determinar el nivel del impacto y riesgo aceptable.	La organización acepta bajo qué circunstancias o de acuerdo al contexto del sistema un impacto y riesgo es aceptable.
2. Tratamiento de riesgos.	Tratamiento	Escenarios posibles respecto de reducir o ampliar el riesgo residual.	La organización evalúa los escenarios sugeridos por la metodología y determinar cuál es asumible.	La organización toma decisiones para iniciar el tratamiento de riesgos.
	Estudio cuantitativo y cualitativo de costo – beneficio.	Escenarios donde se reflejan costos de las salvaguardas aplicadas o no y los aspectos intangibles respecto de cada escenario.	La organización evalúa los escenarios sugeridos por la metodología y determinar cuál es asumible.	La organización toma decisiones para iniciar el tratamiento de riesgos.
	Opciones de tratamiento	Establece cuatro opciones para el tratamiento de riesgos.	La organización evalúa las opciones de tratamiento sugeridos por la metodología.	La organización determina que opción de riesgos adopta como propuesta de tratamiento.
Fuente: autora				

Es fundamental que después de desarrolladas cada una de las actividades y subtareas correspondientes al proceso de gestión de riesgos, la organización se apoye en los indicadores y listas de control establecidas al finalizar para cada de las

actividades del análisis y tratamiento de riesgos, esto con el objeto de verificar si se ha identificado, estimado y valorado cada aspecto del contexto del estado de seguridad del sistema y su opción de tratamiento, para cada uno de los activos, de acuerdo con las amenazas, impactos, riesgos, salvaguardas, valoración de riesgos y la selección de una opción de tratamiento de riesgos, donde se culmina el proceso de gestión de riesgos según la metodología.

- Herramientas de la metodología: la metodología brinda como apoyo una herramienta sistematizada que le permite a una organización llevar a cabo el proceso de riesgos y hacer un tratamiento cuantitativo o cualitativo de la información requerida; además de permitir exportar e importar los datos que se manejan en cada una de ellas en formato XML (*Extended Markup Languaje*) y CSV (*Comma Separated Values*). Estas herramientas están fundamentadas en la estructura de la metodología manejando:

  - El catálogo de los tipos de activos.
  - El catálogo de las dimensiones de valoración para los activos.
  - La valoración de activos de acuerdo a unos criterios.
  - El catálogo de amenazas.
  - El catálogo de salvaguardas.
  - Evaluar (calcular) el impacto y riesgos residuales.

La herramienta PILAR – Procedimiento Informático–Lógico para el análisis de riesgos, es aquella herramienta que le permite a una organización realizar el análisis de riesgos, soportando todas las actividades del análisis e incorporando los catálogos dispuestos por la metodología. De igual forma, mediante esta herramienta se puede evaluar el impacto y riesgos: acumulado, repercutido, potencial y residual, permitiendo conocer y analizar el por qué se presenta un impacto o riesgo.

- Guía de técnicas de la metodología: la metodología pone a disposición de las organizaciones una serie de técnicas generales y específicas, las cuales podrán ser aplicadas según sea el contexto en el cual se va a realizar el análisis y la gestión de riesgos. Dentro de las técnicas generales encontramos:

- Técnicas gráficas fundamentadas en diagramas de tarta, de Pareto e histogramas.

- Técnicas en sesiones de trabajo fundamentadas en presentaciones, reuniones, entrevistas.

- Técnica de valoración Delphi, donde se agrupan un conjunto de técnicas de acuerdo al contexto y los objetivos que se pretenden desarrollar.

Las técnicas específicas se aplican en las actividades definidas dentro de la metodología para llevar a cabo el análisis y gestión de riesgos, de tal forma que estas técnicas no se utilizan en otros escenarios de trabajo. Dentro de las técnicas específicas encontramos:

- Análisis mediante tablas - estimación de impacto y riesgo.

- Análisis algorítmico cualitativo y cuantitativo.

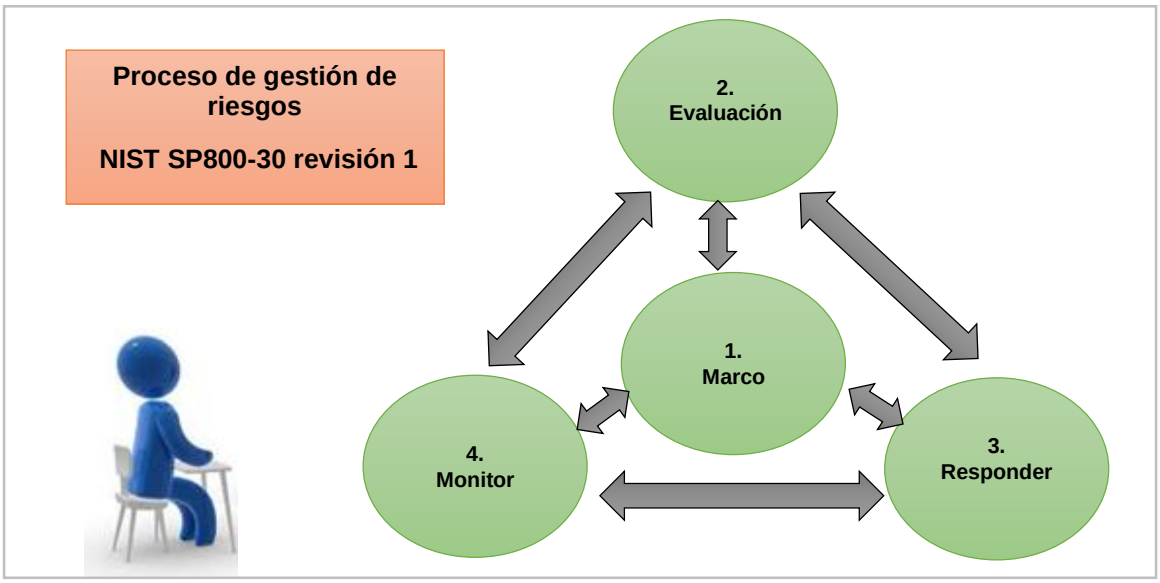
- Árboles de ataque.

Finalmente, los anteriores aspectos se desarrollaron como el estudio realizado a cada una de las actividades principales y subtareas definidas en el proceso de gestión de riesgos de la metodología MAGERIT versión 3.

6.3.1.2 NIST SP800-30 revisión 1: la guía NIST SP800-30 revisión 1, define el proceso que le permite a una organización identificar, evaluar y priorizar los riesgos en cuanto a la seguridad de la información y lo hace a través de cuatro componentes definidos como el proceso de gestión de riesgos, los cuales son: marco, evaluación, responder y monitor del riesgo.

La guía se centra en el componente de evaluación de riesgos de seguridad en el cual define el método para realizarlo en cada uno de los niveles de jerarquía de riesgos definidos como el Nivel 1 – La Organización, Nivel 2 – La misión y funciones del negocio y Nivel 3 - Los sistemas de información. Los componentes del proceso de gestión de riesgos, se caracterizan por estar definidos bajo un esquema de mejora continua, permitiendo de esta forma iniciar el proceso de evaluación de riesgos ante cualquier cambio o actualización presentado dentro de la organización. A continuación se muestra en la figura los componentes del proceso de gestión de riesgos de NIST SP800-30 revisión 1.

Figura 14. Proceso de gestión de riesgos con NIST SP800-30 revisión 1



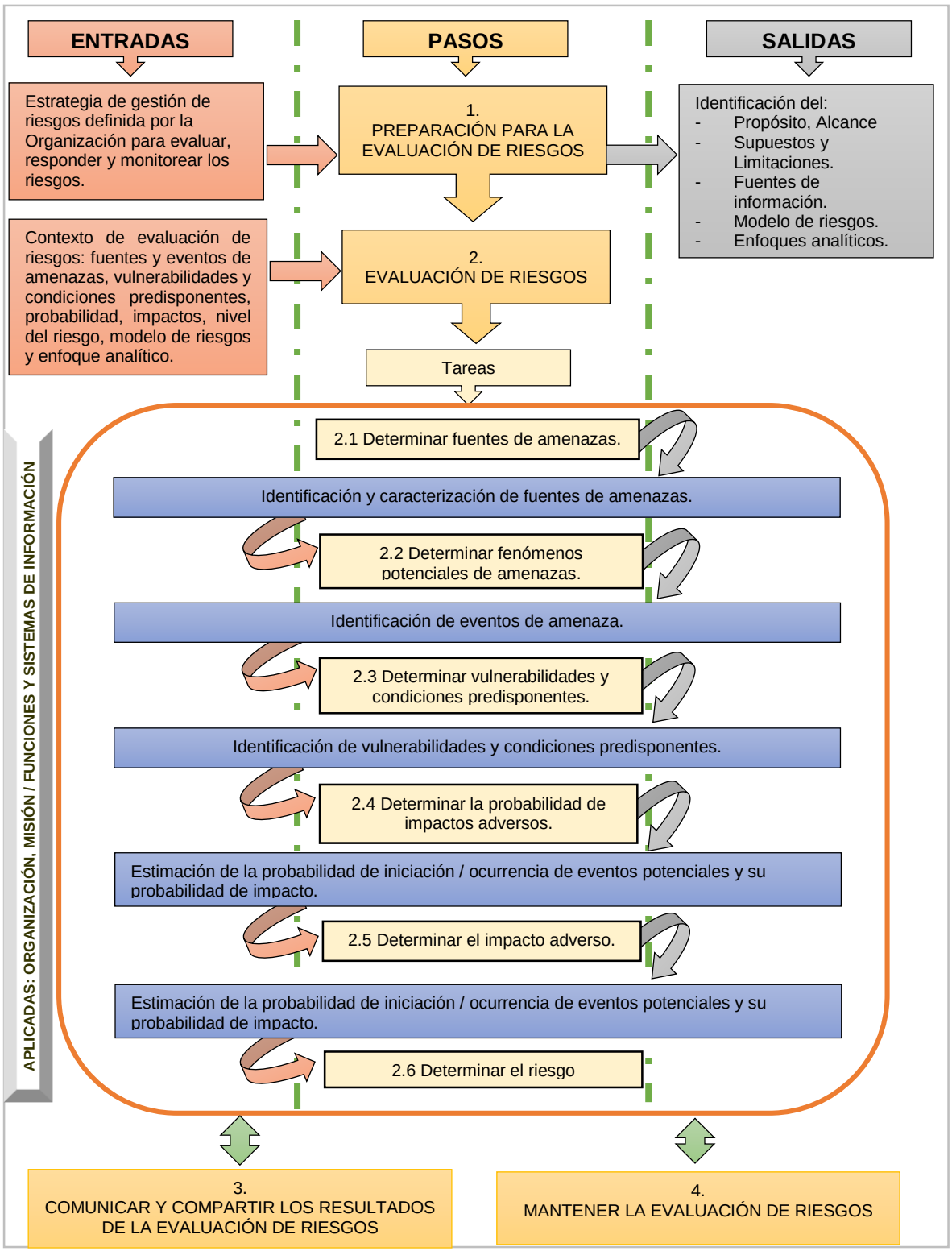
Fuente: el autor

Dentro de la anterior estructura, encontramos el componente de evaluación de riesgos, y es precisamente sobre éste componente que se desarrollan cada uno de los pasos que le permiten a una organización identificar los riesgos y gestionarlos a través de sus diferentes niveles: organización, misión / funciones y sistemas de información.

- Paso 1: Preparación para la evaluación de riesgos.
- Paso 2: Realización de la evaluación de riesgos.
- Paso 3: Comunicación de los resultados de la evaluación de riesgos.
- Paso 4: Mantener la evaluación de riesgos.

A continuación se ilustran los pasos y tareas definidas por la guía para llevar a cabo la evaluación de riesgos.

Figura 15. Pasos de la evaluación de riesgos con NIST SP800-30 revisión 1



Fuente: el autor

De acuerdo con la anterior ilustración, se identifica el esquema de actividades y tareas establecidas por la guía NIST SP800-30 revisión 1, las cuales serán descritas en la siguiente tabla; además de identificar qué elementos brinda la guía, cual es el trabajo que debe realizar la organización respecto de cada tarea y los resultados e informes que se obtienen al finalizar cada paso.

Tabla 6. Descripción de los pasos y tareas de la evaluación de riesgos – NIST SP800-30 revisión 1

Pasos de la guía	Tareas	Elementos de apoyo de la guía	A cargo de la Organización	Resultados / Informes
1. Preparación para la evaluación.	Identificar el propósito de la evaluación.	Orientación respecto de cómo obtener información a través de la evaluación del riesgo.	Reconocer el estado actual de seguridad en los distintos niveles de jerarquía de riesgos.	Obtener un marco estratégico compuesto de la información obtenida de cada una de las tareas de la preparación de la evaluación y de esta forma continuar con el paso 2 de la guía.
	Identificar el alcance de la evaluación.	Orientación respecto de los parámetros e tener en cuenta para la aplicabilidad de la evaluación de riesgos.	Reconocer las consideraciones a tener en cuenta para llevar a cabo la evaluación de riesgos.	
	Identificar los supuestos y limitaciones asociadas a la evaluación.	Orientación respecto de posibles supuestos respecto de fuentes y eventos de amenazas, vulnerabilidades, condiciones predisponentes, probabilidad, impactos, enfoques analíticos, entre otros.	Definir qué aspectos son tenidos en cuenta como supuestos o limitaciones dentro de la evaluación de riesgos.	
	Identificar las fuentes de información que se utilizarán para la evaluación.	Proporciona un listado de fuentes de amenazas, eventos de amenazas, impactos y determinación del riesgo en los apéndices D, E, H e I.	Reconocer las fuentes primarias de información respecto de amenazas, vulnerabilidades e impacto para llevar a cabo la evaluación de riesgos.	
	Identificar el modelo de riesgos	Orientación respecto de varios	Seleccionar el o los modelos de	

Tabla 6. (Continuación)

Pasos de la guía	Tareas	Elementos de apoyo de la guía	A cargo de la Organización	Resultados / Informes
		modelos de riesgos para su utilización para llevar a cabo la evaluación de riesgos.	riesgos a utilizar en la evaluación de riesgos.	
	Identificar los enfoques analíticos.	Orientación respecto de los distintos enfoques analíticos riesgos para llevar a cabo la evaluación de riesgos	Identificar cada enfoque analítico para llevar a cabo la determinación del riesgo.	
	La organización establece un marco donde contempla el propósito, el alcance, las fuentes de información y reconoce las limitaciones y el modelo de riesgos que permita llevar a cabo la evaluación de riesgos.			
2. Realizar la evaluación del riesgo	Identificar y caracterizar las fuentes de amenaza.	Apéndice D de la guía.	Estudiar las posibles fuentes de amenaza presentes en el nivel sujeto de evaluación.	Documentación de la identificación de las fuentes de amenaza.
	Identificar eventos de amenaza.	Apéndice E de la guía.	Estudiar los posibles eventos potenciales de amenaza.	Documentación de la identificación de los eventos de amenaza.
	Identificar vulnerabilidades y condiciones predisponentes.	Apéndice F de la guía.	Estudiar las vulnerabilidades y condiciones predisponentes presentes en el nivel sujeto de evaluación.	Documentación de la identificación de vulnerabilidades y condiciones predisponentes.
	Determinar la probabilidad de iniciación / ocurrencia de amenazas y la probabilidad de impacto adverso.	Apéndice F de la guía.	Analizar la probabilidad de iniciación / ocurrencia de amenazas y la probabilidad de impacto adversos sobre los activos de la organización.	Documentación de la determinación de la probabilidad de amenazas, con la evaluación de la iniciación de ocurrencia y la probabilidad de eventos de amenazas.
	Determinar el impacto.	Apéndice H de la guía.	Estimar el daño o impactos	Documentación de la

Tabla 6. (Continuación)

Pasos de la guía	Tareas	Elementos de apoyo de la guía	A cargo de la Organización	Resultados / Informes
			adversos para la organización.	determinación y evaluación de los impactos adversos para la organización.
	Determinar el riesgo.	Apéndice I de la guía.	Estimar los niveles de riesgos sobre los activos, funciones, individuos y otras organizaciones.	Documentación de la determinación de los riesgos sobre los activos, funciones, individuos y otras organizaciones.
	Como resultado de la evaluación de riesgos se obtiene un listado de los riesgos de seguridad, que son priorizados por el nivel de riesgo de acuerdo a su probabilidad e impacto; y que se tienen en cuenta para establecer las decisiones de respuesta a estos riesgos.			
3. Comunicar los resultados	Comunicar los resultados de la evaluación de riesgos.	Apéndice K de la guía.	Establecer los mecanismos para comunicar y compartir los resultados de la evaluación de riesgos.	Conocimiento a las partes interesadas de la organización y sus empleados de los resultados de la evaluación de riesgos.
	Compartir la información relacionada con los riesgos identificados.			
	La organización en general ha comunicado y compartido a los líderes y partes interesadas la información de los resultados obtenidos en la evaluación de riesgos.			
4. Mantener la evaluación	Seguimiento contínuo de factores de riesgo.	Orientación respecto de los criterios a tener en cuenta para realizar un seguimiento contínuo a los factores de riesgo.	Identificar los posibles cambios o modificación que se presenten sobre los activos, funciones, individuos y otras organizaciones.	Conocimiento de la situación actual de los cambios o modificaciones que afectan las actividades, la misión, sistemas de información, y entornos de operación, que se consideren

Tabla 6. (Continuación)

Pasos de la guía	Tareas	Elementos de apoyo de la guía	A cargo de la Organización	Resultados / Informes
				como factores de riesgo.
	Actualización de la evaluación de riesgos.	Orientación respecto los criterios a tener en cuenta para actualizar la evaluación de riesgos existente.	Tomar la información derivada del seguimiento contínuo de los factores de riesgo identificados, para realizar una actualización de la evaluación de riesgos realizada.	Definición de que aspectos se van a revisar en una nueva evaluación de riesgos o simplemente evaluar cómo los factores de riesgo han cambiado.
	La organización realiza un seguimiento continuo a nuevos factores de riesgos, determinan su nivel de cambio y estiman lo pertinente para actualizar la evaluación de riesgos existente.			
Fuente: autora				

Es fundamental que la organización tenga en cuenta la orientación y documentación que establece la guía, como apoyo para llevar a cabo las tareas de la evaluación de riesgos; las cuales están definidas en los apéndices y plantillas que le proporcionan a la organización la información útil y precisa en la evaluación de riesgos.

Con los resultados derivados del proceso de evaluación de riesgos, la organización ha obtenido una determinación del riesgo para cada uno de los niveles de la jerarquización de riesgos, los cuales son el fundamento para la toma de decisiones encaminadas siempre para dar respuesta a los riesgos identificados.

6.3.2 Comparativo entre la metodología de gestión de riesgos MAGERIT versión 3 y la guía NIST SP800-30 revisión 1. Cada una de las metodologías MAGERIT versión 3 y la guía NIST SP800-30 revisión 1, contemplan dentro de su estructura de gestión de riesgos para sistemas de información, una serie de aspectos que dejan ver las fortalezas y bondades que ofrece cada una de ellas, además de conocer cuáles son sus diferencias.

6.3.2.1 Objetivos de seguridad contemplados en cada metodología: en seguridad informática los tres pilares u objetivos principales son la confidencialidad, integridad y disponibilidad, no obstante a través del estudio realizado a las metodologías, se puede advertir que MAGERIT versión 3 contempla dentro de su estructura estos tres objetivos como las dimensiones de seguridad en las cuales puede verse afectado un activo de información, y además considera dos dimensiones más, las cuales son la trazabilidad y la autenticidad, que son aspectos de seguridad derivados específicamente del uso de los sistemas de información.

Por su parte la guía NIST SP800-30 revisión 1, contempla los tres objetivos principales en los cuales se ven comprometidos los sistemas de información y/ o la información, teniendo en cuenta los impactos adversos sobre las operaciones de la organización y de sus activos, individuos, otras organizaciones y la Nación.

Tabla 7. Cuadro comparativo objetivos de seguridad metodologías de gestión de riesgos

METODOLOGÍA	OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN				
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TRAZABILIDAD	AUTENTICIDAD
MAGERIT versión 3	X	X	X	X	X
NIST SP800-30 revisión 1	X	X	X	-	-
Fuente: el autor					

Es importante resaltar que aunque ambas metodologías están orientadas en determinar los riesgos asociados al uso de los sistemas de información, cada una de ellas fija sus esfuerzos en distintos principios de seguridad; particularidad en las que establecen su proceso de gestión de riesgos.

6.3.2.2 Aplicación de la gestión de riesgos en la organización: la aplicación de la gestión de riesgos, permite conocer cuáles son los niveles o partes de la organización que tiene en cuenta cada la metodología, para llevar a cabo la el análisis y evaluación de riesgos; de tal forma que fácilmente se pueda determinar el estado de seguridad en cada una de estas áreas y determinar los posibles riesgos.

Tabla 8. Cuadro comparativo aplicación de la gestión de riesgos

METODOLOGÍA	APLICACIÓN DE LA GESTIÓN DE RIESGOS										
	PROYECTO	PROCESO	MISIÓN	FUNCIONES	INFORMACIÓN	SISTEMAS DE INFORMACIÓN	INFRAESTRUCTURA FÍSICA	PERSONAL / INDIVIDUOS	SERVICIOS	IMAGEN / REPUTACIÓN	OTRAS ORGANIZACIONES
MAGERIT versión 3	X	X	X	X	X	X	X	X	X	X	-
NIST SP800-30 revisión 1	-	X	X	X	X	X	X	X	X	X	X
Fuente: el autor											

Cada una de las metodologías se enmarca en una categoría en la cual desarrolla la gestión de riesgos, y permite identificar de qué manera se realiza esta labor; por su lado, MAGERIT versión 3 aborda el proceso de gestión de riesgos a través de un proyecto mediante el cual se planifican todas las actividades preliminares del análisis de riesgos y en las cuales se tendrán en cuenta los procesos, misión, funciones, activos, sistemas de información y servicios de la organización, pero sin proyectarse hacia una gestión de riesgos sobre otras organizaciones.

Por otro lado la guía NIST SP800-30 revisión 1, realiza las evaluaciones de riesgo a través de un proceso global, que se subdivide en los tres niveles de la jerarquía de gestión de riesgos, y de forma particular determina los riesgos sobre la información, los sistemas, los individuos, servicios y su vínculo con otras organizaciones y la nación, ya que hace parte de una de las publicaciones en materia de seguridad del Departamento de Comercio de los Estados Unidos.

6.3.2.3 Actividades de análisis y evaluación de riesgos de las metodologías: las actividades de análisis y evaluación de riesgos de cada una de las metodologías, permiten conocer de cerca el modelo del proceso de gestión de riesgos mediante el cual una organización puede llegar a comprender y a identificarse respecto de las necesidades de seguridad que esta requiere. Permite visualizar que aspectos le hace falta entrar a estudiar o adoptar respecto del contexto de la determinación de riesgos. A continuación se presenta un comparativo de las tareas y subtareas contempladas en las actividades de análisis y evaluación de riesgos de las metodologías.

Tabla 9. Actividades del análisis y evaluación de riesgos de las metodologías

TAREAS / SUBTAREAS	**METODOLOGÍAS**	
	MAGERIT versión 3	NIST SP800-30 revisión 1
Definición del alcance	X	X
Definición de un modelo de riesgos	X	X
Identificación de activos	X	X
Valoración del activo	X	-
Dependencias entre activos	X	-
Identificación de amenazas	X	X
Valoración de las amenazas	X	-
Fuentes / origen de amenazas	X	X
Eventos potenciales de amenazas	-	X
Identificación de vulnerabilidades / insuficiencias	X	X

Tabla 9. (Continuación)

TAREAS / SUBTAREAS	METODOLOGÍAS	
	MAGERIT versión 3	NIST SP800-30 revisión 1
Identificación de condiciones predisponentes	-	X
Identificación de controles / salvaguardas	X	-
Valoración de controles / salvaguardas	X	-
Determinar la probabilidad	X	X
Determinar el impacto	X	X
Tratamiento de riesgos	X	-
Fuente: el autor		

Fundamentalmente, el conocimiento de cada una de las actividades que ofrece cada metodología o de las que carece, constituye uno de los puntos de partida sobre el tipo de metodología a adoptar.

6.3.2.4 Criterios de análisis y evaluación de riesgos de las metodologías: los criterios de análisis y evaluación de riesgos de cada una de las metodologías, obedecen a la forma en la cual se evalúan las amenazas, las vulnerabilidades, la probabilidad, el impacto, el nivel del riesgo y se presentan en términos cuantitativos donde se emplean escalas numéricas, en términos cualitativos donde se emplean categorías no numéricas (ej: bajo, medio, alto), de forma semi-cuantitativa donde se combinan las formas cuantitativa y cualitativa. A continuación se muestran los tipos de criterios para la estimación de los aspectos del análisis y evaluación de riesgos contempladas en cada una de las metodologías.

Tabla 10. Criterios de análisis y evaluación de riesgos

METODOLOGÍA	TIPOS DE CRITERIOS PARA EL ANÁLISIS Y LA EVALUACIÓN DE RIESGOS		
	CUALITATIVA	CUANTITATIVA	SEMI-CUANTITATIVA
MAGERIT versión 3	X	X	-
NIST SP800-30 revisión 1	X	X	X

Fuente: el autor

Estos criterios de evaluación le permiten a la organización determinar el grado de afectación positivo o negativo sobre cada uno de los aspectos desarrollados en las tareas del análisis y evaluación de riesgos, constituyéndose en la parte fundamental para lograr estimar y determinar las decisiones a adoptar para el tratamiento de los riesgos.

6.3.3 Determinar los aspectos del análisis y evaluación de riesgos que le aportan mayor valor a las necesidades de seguridad, seleccionando la metodología que la organización puede adoptar. Con el objeto de determinar los requerimientos de seguridad de la organización de este caso de estudio, es importante conocer los aspectos contemplados en esta materia, por lo cual se ha tomado como marco de referencia la ficha técnica de riesgos del proceso de gestión tecnológica, dependencia que se encarga de gestionar, administrar, soportar los activos de información, infraestructura tecnológica y de comunicaciones, sistemas de información y servicios tecnológicos en los cuales se soportan los procesos y procedimientos de la entidad. A continuación se muestra la ficha técnica de la matriz de riesgos del proceso de gestión tecnológica de la la Dirección Ejecutiva Seccional de Administración Judicial de Tunja – DESAJT.

Tabla 11. Matriz de riesgos del proceso de gestión tecnológica de la DESAJT

RESPONSABLE	RIESGO	DESCRIPCIÓN / CAUSAS /EFECTOS	CALIFICACIÓN PRELIMINAR	EVALUACIÓN PRELIMINAR DEL RIESGO	CONTROLES EXISTENTES	DISMINUYE NIVEL DEL RIESGO	VALORACIÓN	VALORACIÓN DEL RIESGO	OPCIONES DE MANEJO	CONTROLES POSTERIORES
			PROBABILIDAD Alto Medio Bajo	Importante Moderado Aceptable Inaceptable		Si	**PROBABILIDAD** Alto Medio Bajo	Tolerable Moderado Aceptable	Asumir / Reducir Compartir /Transferir	
			IMPACTO Leve Moderado Catastrófico			No	**IMPACTO** Leve Moderado Catastrófico			
Fuente: http://sistemagestioncalidad.ramajudicial.gov.co/ModeloCSJ/index.php										

De acuerdo con la ficha técnica de la matriz de riesgos definida en el Sistema Integrado de Gestión y Control de Calidad y Medio Ambiente – SIGCMA de la entidad, se logran evidenciar las variables y parámetros de medida frente a la administración de riesgos, las cuales se encuentran diseñadas de acuerdo con las normas NTCGP1000, ISO9001 y el modelo estándar de control interno (MECI).

Abordando de una manera más práctica la ficha técnica de la matriz de riesgos definida en el Sistema Integrado de Gestión y Control de Calidad y Medio Ambiente – SIGCMA de la entidad, en la siguiente figura se muestra cómo la organización dentro del proceso de gestión tecnológica, ha determinado el riesgo por incumplimiento que se presenta respecto de los servicios y requerimientos de soporte tecnológico. El propósito del presente ejemplo ilustrativo, tiene por objeto reconocer que bajo la actual administración de riesgos, el análisis se realiza a través de la identificación del riesgo, con sus posibles causas y efectos, llegando a obtener una valoración preliminar de la probabilidad y el impacto del riesgo con la ausencia de controles para tratar el riesgo. Paso seguido, con la aplicación de los controles existentes, se evalúa el nivel de disminución de riesgo, aspecto que modifica la valoración de la probabilidad e impacto con controles y como resultado la organización define las opciones de manejo de riesgo y determina la aplicación o no de controles posteriores.

Figura 16. Ejemplo riesgo por incumplimiento proceso de gestión tecnológica de la DESAJT

RIESGO	DESCRIPCIÓN	CAUSAS	EFECTOS	CALIFICACIÓN PRELIMINAR	EVALUACIÓN PRELIMINAR DEL RIESGO	CONTROLES EXISTENTES	DISMINUYE NIVEL DEL RIESGO	VALORACIÓN	VALORACIÓN DEL RIESGO	OPCIONES DE MANEJO	CONTROLES POSTERIORES
Incumplimiento	Incumplimiento en los Acuerdos de Niveles de servicio medidos en los tiempos de respuesta a los usuarios.	Fallas en la coordinación y atención de los requerimientos.	Inconformidad de los usuarios.	**Probabilidad** Medio **Impacto** Catastrófico	Importante	Supervisión, actas de seguimiento	**Probabilidad** Si **Impacto** Si	**Probabilidad** Baja **Impacto** Catastrófico	Moderado	Reducir, transferir el riesgo.	Generar Acción Preventiva

Fuente: http://sistemagestioncalidad.ramajudicial.gov.co/ModeloCSJ/index.php

El anterior esquema de valoración del riesgo, se asemeja a las actividades de estimación del estado del riesgo definidas por la metodología de análisis de riesgos de MAGERIT versión 3. Tal similitud se ve reflejada a partir de la calificación preliminar del riesgo, donde se valoran el impacto y el riesgo potencial que obedece al estado del riesgo sin controles aplicados y luego con la aplicación de los controles existentes se llega a realizar una valoración del impacto y el riesgo residuales, pasando a la evaluación de riesgos donde se estudian los valores de impacto y riesgos, con el propósito de que la organización pueda decidir las opciones de tratamiento de riesgos, de acuerdo con los resultados obtenidos en la evaluación de los mismos.

En virtud de lo anterior, es preciso resaltar que de acuerdo con la actual administración de riesgos de la organización y encontrando una importante similitud con una de las metodologías estudiadas, es posible integrar al proceso de gestión de riesgos de la entidad, el método análisis y evaluación de riesgos que ofrece la metodología MAGERIT versión 3, donde a partir de un “Proyecto de análisis de riesgos” la organización pueda fortalecer la gestión de riesgos frente a:

- Integrar a su actual administración de riesgos, una metodología orientada específicamente al análisis y evaluación de riesgos de los sistemas de información y a los activos que intervienen en el uso de esos sistemas.

- Fortalecer los objetivos de seguridad de la actual administración de riesgos, frente a la determinación de los riesgos presentes en las dimensiones de seguridad: autenticidad y trazabilidad.

- Apoyarse con los catálogos que ofrece la metodología MAGERIT versión 3, donde se identifican las distintas amenazas, su origen, las dimensiones de seguridad afectadas, las vulnerabilidades o insuficiencias de los controles existentes, y los tipos de activos de información que pueden ser afectados o se encuentran sometidos a los riesgos en materia de seguridad de información.

- Determinar el impacto y riesgo potencial, cuando no se han aplicado controles de seguridad sobre los activos de información y su entorno operativo.

- Determinar el impacto y riesgo residual, cuando se han aplicado controles (controles existentes / nuevos controles) de seguridad sobre los activos de información y su entorno operativo.

Finalmente, estas actividades del proyecto de análisis de riesgos, pueden ser promovidas por integrantes del nivel directivo de la organización, donde a través de la adopción de la metodología MAGERIT versión 3, podrán emprender el proyecto de seguridad que se ajusta al ciclo PHVA (planear, Hacer, Verificar y Actuar) del Sistema Integrado de Gestión y Control de Calidad y Medio Ambiente – SIGCMA de la entidad.

6.4 ESTABLECER UNA GUÍA PARA EL ANÁLISIS Y EVALUACIÓN DE LOS RIESGOS PARA LOS ACTIVOS DE INFORMACIÓN DE LA DIRECCIÓN EJECUTIVA SECCIONAL DE ADMINISTRACIÓN JUDICIAL DE TUNJA – DESAJT, DE ACUERDO CON LA METODOLOGÍA DE GESTIÓN DE RIESGOS SELECCIONADA.

Con los resultados del estudio comparativo de las metodologías MAGERIT versión 3 y la guía de seguridad NIST SP800-30 revisión 1, en el capítulo anterior se han indicado los aspectos en cuanto a seguridad que ofrece la metodología de gestión de riesgos MAGERIT versión 3, donde a través de sus actividades se ha encontrado una gran similitud con la actual administración de riesgos de la organización, lo que

satisfactoriamente permite proponer una integración de las tareas de análisis y evaluación de riesgos de esta metodología, al proceso de gestión de riesgos de la Dirección Ejecutiva Seccional de Administración Judicial de Tunja – DESAJT.

Por lo anteriormente expuesto, a continuación se presenta una propuesta para que de la Dirección Ejecutiva Seccional de Administración Judicial de Tunja – DESAJT, pueda integrar las actividades del análisis y evaluación de los riesgos para sus activos de información a través de un “Proyecto de análisis de riesgos “, donde se contemplan los tres principales objetivos de seguridad incluyendo dos objetivos más como son la autenticidad y trazabilidad, que fortalecerán la seguridad y protección de los activos de información, sistemas tecnológicos y de comunicación de la organización.

6.4.1 Guía para el análisis y evaluación de los riesgos para los activos de información de la Dirección Ejecutiva Seccional de Administración Judicial de Tunja – DESAJT. Esta guía se fundamenta principalmente en brindarle a la Dirección Ejecutiva Seccional de Administración Judicial de Tunja – DESAJT, las actividades a través de las cuales pueda emprender un análisis y evaluación de riesgos de sus activos de información, aplicando una metodología de gestión de riesgos en seguridad informática especializada para los sistemas de información. Dicho análisis y evaluación de riesgos, podrá ser acometido mediante un proyecto de análisis de riesgos definido específicamente por la metodología seleccionada y mediante el cual la organización podrá adoptar una metodología de gestión de riesgos en materia de seguridad de la información, que le permita determinar los riesgos a los que se encuentran sometidos sus activos de información y determinar el nivel de aseguramiento de los mismos.

El desarrollo de esta guía para el análisis y evaluación de los riesgos de los activos de información de la Dirección Ejecutiva Seccional de Administración Judicial de Tunja – DESAJT, (en adelante se denominará la organización) está fundamentada en seguir la estructura del proyecto de análisis de riesgos de MAGERIT versión 3 (en adelante se denominará la metodología), mediante la cual la organización podrá conocer las actividades principales para acometer este tipo de proyectos de una forma adecuada y satisfactoria. A continuación, se definen los aspectos más importantes para acometer el proyecto de análisis de riesgos en la organización:

6.4.1.1 Definición de comités, roles y funciones del proyecto de análisis de riesgos. Para ejecutar el proyecto de análisis de riesgos, se requiere de la conformación de unos comités, con roles y funciones específicas dentro de la organización, los cuales a su vez, contarán con una serie de responsabilidades de acuerdo al contexto en el que se desempeñarán. Estos comités serán definidos a lo largo de las tareas del proyecto de análisis de riesgos, por lo cual, a continuación serán descritos ya que serán los encargados de liderar y asegurar que el proyecto de análisis de riesgos sea una realidad y se lleve a feliz término dentro de la organización:

- Comité de seguridad de la información en la organización: está integrado por el nivel directivo y el responsable de seguridad de la organización. En este comité se encabeza la toma de decisiones definitivas y apremiantes, generadas por el proyecto de análisis de riesgos.

- Comité de seguimiento del proyecto: es nombrado por el comité de seguridad de la información, al cual debe reportar el avance de las actividades del proyecto. El comité de seguimiento está integrado por los coordinadores responsables de las dependencias de la organización donde se aplicará el proyecto de análisis de riesgos y de manera primordial el coordinador de soporte tecnológico responsable de los sistemas de información y de comunicaciones. El comité de seguimiento será responsable de[26]:

  - Resolver las incidencias durante el desarrollo del proyecto.
  - Asegurar la disponibilidad de los recursos humanos con los perfiles adecuados y su participación en las actividades donde es necesaria su colaboración.
  - Aprobar los informes intermedios y finales de cada proceso.
  - Elaborar los informes finales para el comité de seguridad de la información.

En el comité de seguimiento debe existir el rol de enlace operacional, el cual corresponde a la persona de la organización con gran conocimiento de los usuarios y dependencias, que ejercerá su labor especial en relacionar al equipo del proyecto

[26] PAE PORTAL ADMINISTRACIÓN ELECTRÓNICA. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. <https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WcgqkMbavIU>. [Citado el 24 de Septiembre de 2017].

con los usuarios, convirtiéndose en un interlocutor visible de éste comité con el grupo de usuarios.

- Equipo del proyecto: tendrá un director y está integrado por el personal especializado y experto en los sistemas de información y telecomunicaciones de la organización, así como el personal técnico con conocimiento en gestión de seguridad de la información y en particular de la metodología de análisis y evaluación de riesgos. Cabe resaltar que este equipo puede estar integrado por consultores por contratación externa, en el caso de que la organización requiera el fortalecimiento de los aspectos técnicos que se requieran. El equipo del proyecto será responsable de[27]:

  - Llevar a cabo las tareas del proyecto.
  - Recopilar, procesar y consolidar datos.
  - Elaborar los informes.

Finalmente, es importante resaltar que el director del equipo del proyecto debe pertenecer al nivel directivo de la organización, con responsabilidades en seguridad de los sistemas de información o coordinador de esta materia en específico; el cual se encargará de reportar las actividades y avances del equipo del proyecto al comité de seguimiento.

- Grupo de usuarios interlocutores de la organización: está integrado por usuarios de las dependencias de la organización donde se llevará a cabo el proyecto y se caracterizan por ser:

  - Los responsables de los servicios de la organización, conocedores de la misión y sus distintas estrategias a través del tiempo (mediano y largo plazo).
  - Los responsables de prestar los servicios internos de la organización.
  - El personal propio de explotación y operación de los servicios de los sistemas de información, conocedores de los medios desplegados en cuanto a

[27] PAE PORTAL ADMINISTRACIÓN ELECTRÓNICA. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. <https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WcgqkMbavIU>. [Citado el 24 de Septiembre de 2017]

aplicaciones de producción y salvaguardas, así como los habituales incidentes de seguridad presentados en la organización.

Después de identificados los distintos comités que serán el pilar para emprender las actividades del proyecto de análisis de riesgos, a continuación se presentan los roles específicos que harán parte de dichos comités:

- Promotor del proyecto: es la persona dentro de la organización que se encargará de liderar las primeras actividades del proyecto, orientando principalmente la oportunidad y el alcance del mismo, y de esta forma lograr el lanzamiento del proyecto de análisis de riesgos dentro de la organización.

- Director del Proyecto: es la cabeza principal del equipo del proyecto y actúa como interlocutor ante el comité de seguridad de la información en la organización o su responsable.

- Enlace operacional del proyecto: es la persona que conecta o enlaza al equipo del proyecto con los usuarios, ejerciendo un contacto interdisciplinario relevante en este tipo de proyectos; su principal función está definida dentro del comité de seguimiento del proyecto.

6.4.1.2 Inicio del proyecto de análisis de riesgos: con el objeto de que la organización pueda orientarse en el desarrollo del proyecto de análisis de riesgos, en la presente guía se han tomado las respectivas fichas técnicas de cada actividad, contempladas en la metodología; mediante las cuales se indican los objetivos, entradas y salidas de cada tarea, técnicas y prácticas que pueden aplicarse y los participantes y comités que son responsables.

- Principales actividades y tareas del proyecto de análisis de riesgos: el proyecto de análisis de riesgos contempla tres actividades principales, con una serie de tareas específicas, que serán llevadas a cabo por los comités del proyecto y mediante las cuales se gestionará y recopilará la información requerida para establecer el esquema del proyecto de análisis de riesgos dentro de la organización. A continuación se indican las tres actividades principales mediante las cuales la organización conseguirá emprender el proyecto de análisis de riesgos:

- Actividades preliminares: las actividades preliminares constituyen la base para estructurar el lanzamiento o implementación del proyecto de análisis de riesgos

dentro de la organización, y para hacer esto posible, se deben realizar las siguientes tareas:

- Tarea 1: realizar un estudio de oportunidad del proyecto, en esta tarea se estima la integración del desarrollo del proyecto bajo el marco de actividades a desarrollar dentro de la organización y para realizarlo, el nivel directivo a través de un promotor del proyecto (puede ser un experto en seguridad de la información interno o externo a la organización), que conocerá los problemas relacionados con la seguridad de los activos y sistemas de información de la organización, a través de:

    - Antecedentes de incidentes de seguridad presentados en la organización.

    - Actualizaciones o modificaciones de las tecnologías y comunicaciones utilizadas por la organización.

    - Desarrollo o adquisición de nuevos sistemas de información.

Será la persona encargada de concientizar a los responsables de las dependencias de la organización, de la importancia de iniciar el proyecto. Para el desarrollo de esta tarea de sensibilización, el promotor podrá valerse de un cuestionario aplicado a los coordinadores de las dependencias de la organización, en el cual abordará aspectos relacionados con la seguridad de los activos y sistemas de información de la organización, provocando una reflexión importante para implementar el proyecto de análisis de riesgos. El promotor podrá apoyarse en la siguiente ficha ofrecida por la metodología para desarrollar el estudio de oportunidad del proyecto.

Figura 17. Ficha técnica estudio de oportunidad del proyecto análisis de riesgos

PAR: Proyecto de análisis de riesgos ***PAR.1: Actividades preliminares*** ***PAR.11: Determinar la oportunidad***
Objetivos • Identificar o suscitar el interés de la Dirección de la Organización en la realización de un proyecto de análisis de riesgos
Productos de entrada
PAR: Proyecto de análisis de riesgos ***PAR.1: Actividades preliminares*** ***PAR.11: Determinar la oportunidad***
Productos de salida • **Informe preliminar** recomendando la elaboración del proyecto • Sensibilización y apoyo de la Dirección a la realización del proyecto • Creación del comité de seguimiento
Técnicas, prácticas y pautas •
Participantes • El promotor

Fuente: https://administracionelectronica.gob.es/ctt/magerit#.WcMlq8bavIV

De acuerdo con la ficha técnica de la tarea de estudio de oportunidad del proyecto, el promotor se encarga de recolectar la información importante a los responsables de los activos y sistemas de información de la organización, donde tendrá una aproximación sobre los procesos, procedimientos, funciones y los servicios implicados en temas de seguridad de los recursos tecnológicos y de comunicaciones de la misma. Obteniendo de esta forma, la información que le permitirá elaborar un informe preliminar que deberá presentar a la Dirección de la organización, y contendrá los siguientes aspectos[28]:

- Presentación de los argumentos básicos.
- Relación de informes y/o antecedentes sobre la seguridad de los activos y sistemas de información.
- Aproximación inicial del dominio o contexto del proyecto en función de: los objetivos de las dependencias, disposiciones gerenciales y técnicas, estructura de la organización y el entorno técnico.

[28] PAE PORTAL ADMINISTRACIÓN ELECTRÓNICA. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. <https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WcgqkMbavIU>.[Citado el 24 de Septiembre de 2017]

- Aproximación inicial del recurso humano y material, para la realización del proyecto.

Finalmente, el promotor del proyecto presenta el informe preliminar a la dirección de la organización para que este pueda decidir: aprobar el proyecto de análisis de riesgos, o modificar contexto de aplicación y/o sus objetivos, o retrasar el comienzo del proyecto.

- Tarea 2: determinar el alcance del proyecto de análisis de riesgos, se da inicio a esta tarea con la aprobación de la realización del proyecto de análisis de riesgo, el cual es avalado por la dirección de la organización, reflejando de esta forma el apoyo y los recursos para emprender esta labor. A continuación se muestra la ficha de esta tarea con el objeto de conocer puntualmente cada tarea a realizar.

Figura 18. Ficha técnica del alcance del proyecto análisis de riesgos

PAR: Proyecto de análisis de riesgos ***PAR.1: Actividades preliminares*** ***PAR.12: Determinación del alcance del proyecto***
Objetivos • Determinar los objetivos del proyecto, diferenciados según horizontes temporales a corto y medio plazo • Determinar las restricciones generales que se imponen sobre el proyecto • Determinar el dominio, alcance o perímetro del proyecto

PAR: Proyecto de análisis de riesgos ***PAR.1: Actividades preliminares*** ***PAR.12: Determinación del alcance del proyecto***
Productos de entrada • Recopilación de la documentación pertinente de la Organización
Productos de salida • Especificación detallada de los objetivos del proyecto • Relación de restricciones generales • Relación de unidades de la Organización que se verán afectadas como parte del proyecto • Lista de roles relevantes en la unidades incluidas en el alcance del proyecto • los activos esenciales • los puntos de interconexión con otros sistemas • los proveedores externos
Técnicas, prácticas y pautas • Entrevistas (ver "Guía de Técnicas") • Reuniones • *31010:B.1: Brainstorming* • *31010:B.2: Structured or semi-structured interviews* • *31010:B.3: Delphi technique*
Participantes • El comité de seguimiento

Fuente: https://administracionelectronica.gob.es/ctt/magerit#.WcMIq8bavIV

Con la determinación del alcance del proyecto, el comité de seguimiento realiza su participación, asegurando la disponibilidad del recurso humano con el perfil adecuado y de esta forma, llevar a cabo las siguientes actividades:

- Estimar los elementos de planificación del proyecto (participantes y sus cargas de trabajo).
- Tener en cuenta la existencia de otros planes de seguridad existentes en las dependencias en las cuales se realizara la aplicación del proyecto de análisis de riesgos.
- Considerar el tiempo para la puesta en marcha del proyecto.
- Definir plenamente los objetivos del proyecto, con relación a las dependencias, activos y sistemas de información que serán impactados.
- Identificar las posibles restricciones que deben ser tenidas en cuenta de acuerdo al análisis y gestión de riesgos.

De acuerdo con las actividades a realizar, en el alcance del proyecto es necesaria la aplicación de técnicas de recolección de información, las cuales pueden ser consultadas y seleccionadas según el interés de la organización. Estas técnicas están definidas en el libro III de la metodología y a través de las cuales los participantes del comité de seguimiento podrán aplicarlas para identificar los activos esenciales objeto del análisis, además de los sistemas de información, los servicios que prestan, la información que se transmite a partir de ellos y si existen proveedores en los que posiblemente se apoyan los recursos tecnológicos y de servicios de la organización.

- Tarea 3: planificación del proyecto de análisis de riesgos, esta tarea inicia con la determinación del alcance del proyecto de análisis de riesgos, ya que en esta planificación se elabora el plan de trabajo para el desarrollo del proyecto. En esta tarea es fundamental la participación del director del proyecto y el comité de seguimiento, el cual puede apoyarse en la ficha técnica para esta tarea.

Figura 19. Ficha técnica de planificación del proyecto análisis de riesgos

Proyecto de análisis de riesgos *PAR.1: Actividades preliminares* *PAR.13: Planificación del proyecto*
Objetivos • Definir los grupos de interlocutores: usuarios afectados en cada unidad • Planificar las entrevistas de recogida de información • Determinar el volumen de recursos necesarios para la ejecución del proyecto: humanos, temporales y financieros • Elaborar el calendario concreto de realización de las distintas etapas, actividades y tareas del proyecto • Establecer un calendario de seguimiento que defina las fechas tentativas de reuniones del comité de dirección, el plan de entregas de los productos del proyecto, las posibles modificaciones en los objetivos marcados, etc
Productos de entrada • Resultados de la actividad A1.2, Determinación del alcance del proyecto
Productos de salida • Relación de participantes en los grupos de interlocutores • Plan de entrevistas • Informe de recursos necesarios • Informe de cargas
Técnicas, prácticas y pautas • Planificación de proyectos
Participantes • El director de proyecto • El comité de seguimiento

Fuente: https://administracionelectronica.gob.es/ctt/magerit#.WcMIq8bavIV

Durante esta tarea de planificación, la organización establecerá completamente un plan de trabajo, acompañado de: la determinación de recursos necesarios para la ejecución del proyecto, los usuarios que serán impactados, los tiempos de cada tarea y los seguimientos a realizar por parte del comité de seguimiento del proyecto.

- Tarea 4: lanzamiento del proyecto de análisis de riesgos, para esta tarea el equipo del proyecto y su director toman como parámetro principal el marco de trabajo del proyecto definido en la tarea de planificación, por lo cual para el lanzamiento del proyecto de análisis se deberán estructurar y adecuar los cuestionarios que permitan identificar plenamente los activos de información, amenazas, vulnerabilidades, impactos, controles existentes y demás aspectos para llevar a cabo el análisis y evaluación de riesgos en la organización. En virtud de lo anterior, el equipo del proyecto puede apoyarse en la ficha de la actividad de planificación definida por la metodología.

Figura 20. Ficha técnica de lanzamiento del proyecto análisis de riesgos

Proyecto de análisis de riesgos ***PAR.1: Actividades preliminares*** ***PAR.14: Lanzamiento del proyecto***
Objetivos • Disponer de los elementos de trabajo para acometer el proyecto
Productos de entrada • Marco de trabajo establecido en el Proceso de Gestión de Riesgos: criterios y relaciones con las partes afectadas
Productos de salida • Cuestionarios adaptados • Determinar el catálogo de tipos de activos • Determinar las dimensiones de valoración de activos • Determinar los niveles de valoración de activos, incluyendo una guía unificada de criterios para asignar un cierto nivel a un cierto activo • Determinar los niveles de valoración de las amenazas: frecuencia y degradación • Asignar los recursos necesarios (humanos, de organización, técnicos, etc.) para la realización del proyecto • Informar a las unidades afectadas • Crear un ambiente de conocimiento general de los objetivos, responsables y plazos
Técnicas, prácticas y pautas • Cuestionarios (ver "Catálogo de Elementos")
Participantes • El director del proyecto • El equipo de proyecto

Fuente: https://administracionelectronica.gob.es/ctt/magerit#.WcMlq8bavIV

Con las actividades realizadas en esta tarea, el equipo del proyecto tiene los insumos para pasar a la fase de la elaboración del análisis de riesgos y además, las partes implicadas de la organización se han sensibilizado respecto de los objetivos principales del proyecto.

- Elaboración de análisis de riesgos: el equipo del proyecto de análisis de riesgos, mediante la aplicación de entrevistas a los usuarios definidos dentro del grupo de interlocutores de la organización, recolectarán la información que servirá como insumo para iniciar con el desarrollo de cada una de las tareas del análisis y evaluación de riesgos que permiten determinar los riesgos a los que están expuestos los activos de información de la organización, así:

- Identificación de activos esenciales.
- Valoración de cada activo en las cinco dimensiones de seguridad.
- Definición del esquema de dependencias entre activos esenciales y otros activos.
- Identificación de posibles amenazas sobre los activos.
- Estimación de efectos con la materialización de las amenazas identificadas.
- Determinación de la probabilidad de materialización de las amenazas identificadas.
- Determinación de impactos y riesgos potenciales inherentes del sistema.
- Identificación de controles (salvaguardas) para detener los impactos y riesgos potenciales identificados.
- Valoración de los controles aplicados.
- Determinación de los valores de impacto y riesgo residuales, con los controles aplicados.

Finalmente cada tarea desarrollada y sus resultados deberán ser documentados, ya que cada actividad constituye la evidencia de la determinación de todos los aspectos del proyecto de análisis de riesgos.

- Comunicación de resultados: en esta última tarea, el equipo del proyecto presentará los resultados obtenidos con la elaboración de análisis de riesgos, donde se han determinado del impacto y riesgo residuales, los cuales deberán ser valorados con el objeto de que la organización pueda decidir respecto de las opciones de tratamiento de riesgos, es decir, establecer si el nivel de los riesgos identificados son aceptables, o de lo contrario deben aplicarse nuevos controles para eliminar, reducir y transferir o compartir los riesgos determinados.

7 RESULTADOS E IMPACTO ESPERADOS

Los resultados que pueden obtenerse a través del desarrollo de la presente monografía son los siguientes:

- Con el estudio de las metodologías de gestión de riesgos de los sistemas de información MAGERIT versión 3 y la guía de seguridad NIST SP800-30 revisión 1, se realiza un aporte significativo donde se muestra cada una de las actividades que contemplan las metodologías para llevar a cabo el análisis y evaluación de riesgos dentro de una organización u otras organizaciones.

- Con el comparativo realizado entre las metodologías de gestión de riesgos de los sistemas de información MAGERIT versión 3 y la guía de seguridad NIST SP800-30 revisión 1, se resaltan las características de seguridad que ofrece cada una de ellas, dejando ver fortalezas y debilidades que son fundamentales a la hora en que una organización pueda decidir, cual responde significativamente a sus requerimientos de seguridad y así identificar los riesgos a los que se encuentra expuesta.

- De acuerdo con el estudio realizado al sistema actual de administración de riesgos de la Dirección Ejecutiva Seccional de Administración Judicial de Tunja – DESAJT, se logró identificar la similitud con las actividades para la determinación del riesgo de la metodología MAGERIT versión 3, permitiendo de esta forma, proponer la integración de esta metodología al sistema de administración de riesgos de la organización y robustecerla con las características de seguridad que MAGERIT versión 3 ofrece.

Con base en los resultados obtenidos se pueden apreciar los siguientes impactos:

- Al establecer una guía para el análisis y evaluación de los riesgos para los activos de información de la Dirección Ejecutiva Seccional de Administración Judicial de Tunja – DESAJT, integrando la metodología de gestión de riesgos MAGERIT versión 3, a través del proyecto de análisis de riesgos que esta ofrece, la organización podrá gestionar los riesgos a los que están sometidos sus activos de información, e identificará las actividades del análisis y evaluación de riesgos siguiendo una metodología propia en materia de seguridad de la información.

- La Dirección Ejecutiva Seccional de Administración Judicial de Tunja – DESAJT, a través de esta monografía podrá apoyarse para promover el emprendimiento

del proyecto de análisis de riesgos y obtener resultados frente a la identificación y valoración de los riesgos, permitiéndole determinar los controles efectivos que puedan ser implementados con la finalidad de preservar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los recursos informáticos y de comunicaciones con los que cuenta la organización.

8 DIVULGACIÓN

La divulgación de esta monografía se realizará con el aval del presente proyecto de grado, por parte Escuela de Ciencias Básicas Tecnología E Ingenierías (ECBTI), con el ánimo de ser publicado en el repositorio de la Universidad Nacional Abierta y A Distancia – UNAD.

De igual forma, esta monografía será presentada ante el Director Ejecutivo Seccional de Administración Judicial Tunja y el Coordinador del área de Soporte Tecnológico, como propuesta para ser considerada en el Comité de Dirección de la Organización y de esta forma, se tenga en cuenta la oportunidad de su aplicación.

9 CRONOGRAMA

Para el desarrollo de la presente monografía se definió el siguiente cronograma de actividades:

Tabla 12. Cronograma

ACTIVIDADES	Mes 1: Febrero				Mes 2: Marzo				Mes 3: Abril				Mes 4: Mayo	
	Sem 1	Sem 2	Sem 3	Sem 4	Sem 5	Sem 6	Sem 7	Sem 8	Sem 9	Sem 10	Sem 11	Sem 12	Sem 13	Sem 14
Conocer la estructura organizacional de la empresa caso de estudio.														
Estudiar los procesos del Sistema Integrado de Gestión de la Calidad y Medio Ambiente de la entidad.														
Realizar un listado de los activos de información de la entidad de acuerdo con los procesos de apoyo del SIGCMA.														
Estudiar las metodologías de gestión de riesgos MAGERIT V.3 y 3 y NIST SP800-30 revisión 1.														
Realizar un estudio comparativo de cada metodología de gestión de riesgos MAGERIT V.3 y 3 y NIST														

ACTIVIDADES	Mes 1: Febrero				Mes 2: Marzo				Mes 3: Abril				Mes 4: Mayo	
	Sem 1	Sem 2	Sem 3	Sem 4	Sem 5	Sem 6	Sem 7	Sem 8	Sem 9	Sem 10	Sem 11	Sem 12	Sem 13	Sem 14
SP800-30 revisión 1														
Tomar la matriz de riesgos del SIGCMA de la entidad y determinar los aspectos en los cuales la metodología seleccionada de gestión de riesgos de la seguridad le aporta mayor seguridad.														
Proponer una guía para el análisis y evaluación de los riesgos para los activos de información de la Dirección Ejecutiva Seccional de Administración Judicial de Tunja – DESAJT, de acuerdo con la metodología de gestión de riesgos seleccionada.														
Fuente: el autor														

10 CONCLUSIONES

- Mediante la identificación de los activos de información de la Dirección Ejecutiva Seccional de Administración Judicial de Tunja DESAJT, se lograron reconocer los activos de información esenciales de la organización, los cuales son el insumo para acometer el proyecto de análisis de riesgos propuesto en esta monografía, y se fundamenta el desarrollo de cada una de las actividades tendientes para determinar los riesgos a los cuales se encuentran expuestos, evaluar su nivel de criticidad y formular los controles que la organización podrá gestionar para tratar los riesgos en materia de seguridad de la información.

- Con el estudio realizado a cada una de las metodologías: MAGERIT versión 3 y la guía de seguridad NIST SP800-30 revisión 1, los profesionales en seguridad informática o interesados en la materia, podrán tomar el presente proyecto como referencia documental y conocer cada una de las actividades de análisis y evaluación de riesgos que brinda cada una de ellas y las cuales pueden ser adoptadas dentro de una ámbito corporativo, con activos de información específicos, de acuerdo con las necesidades de seguridad que se requieran.

- Con el establecimiento de la guía de análisis y evaluación de riesgos, para los activos de información de la Dirección Ejecutiva Seccional de Administración Judicial de Tunja DESAJT, la entidad podrá integrar a su actual administración de riesgos todos los aspectos relacionados sobre el uso y protección de su información, sistemas de información, de comunicaciones y recursos tecnológicos; fortaleciendo sus requerimientos de seguridad con relación a la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

- Al emprender un proyecto de seguridad de la información, se afianzan los conocimientos y destrezas adquiridas durante el desarrollo del presente proyecto, y más aún si este estudio se realiza en un entorno social y corporativo, donde se pueda realizar un aporte significativo sobre la materia.

BIBLIOGRAFÍA

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Norma Técnica Colombiana para la presentación de Tesis, trabajos de grado y otros trabajos de investigación. Sexta actualización. Bogotá. ICONTEC. 2008.26p. NTC 1486.

PAE – PORTAL DE ADMINISTRACIÓN ELECTRÓNICA. "MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" {En línea} {1 diciembre 2015} disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WNvTsvnhCM8

UNIVERSIDAD AUTÓNOMA DE OCCIDENTE "Cómo usar Word para trabajos de grado y proyectos". {En línea}. {1 diciembre 2015} disponible en: http://uao.libguides.com/content.php?pid=482863&sid=3979499

ESCUELA EUROPEA DE EXCELENCIA "ISO 9001:2015 Gestión del Riesgo". {En línea}. {1 diciembre 2014} disponible en: http://www.nueva-iso-9001-2015.com/2014/12/iso-90012015-gestion-riesgo/

DEJAN. Kosutic "Usar la ISO 9001 para implementar la ISO 27001". {En línea}. {2 abril 2010} disponible en: http://advisera.com/27001academy/es/blog/2010/04/02/usar-la-iso-9001-para-implementar-la-iso-27001.

CÁRDENAS. Elvis "Metodologías para el análisis de riesgos en Seguridad Informática". {En línea}. {18 agosto 2012} disponible en: http://msnseguridad.blogspot.com.co/2012/08/seguridad-informatica-la-seguridad.html.

ABRIL, Ana. Pulido, Jarol. A. Bohada, Jhon "Análisis de Riesgos en Seguridad de la Información". {En línea}. {05 septiembre de 2016} disponible en:http://www.revistasjdc.com/main/index.php/rciyt/article/download/292/283

VALERIANO OROZCO, Meztli "1.6 Activos Informáticos". {En línea}. {11 septiembre de 2013} disponible en:http://es.slideshare.net/meztli9/16-activos-inf

TRELLEZ ARAUJO, Pedro "Seguridad Informática". {En línea}. {11 febrero de 2010} disponible en: http://es.slideshare.net/Tcherino/seguridad-informatica-3143924?next_slideshow=2

WIKIPEDIA "Análisis de riesgo informático". {En línea}. {09 marzo 2016} disponible en:https://es.wikipedia.org/wiki/An%C3%A1lisis_de_riesgo_inform%C3%A1tico

INTERIANO, Adán “Evaluación de riesgos informáticos". {En línea}. {26 marzo 2014} disponible en: https://prezi.com/xxpupj8h5fuc/evaluacion-de-riesgos-informaticos/

CHÁVEZ, Robert "Gestión del riesgos de seguridad de la información" {En línea}. {25 septiembre 2013} disponible en:http://es.slideshare.net/roberth.chavez/gestin-del-riesgos-de-seguridad-de-la-informacin?next_slideshow=1

ETEROVIC, Jorge. PAGLIARI, Gustavo "Metodología de Análisis de Riesgos Informáticos" {En línea}. {15 enero 2011} disponible en: http://www.cyta.com.ar/ta1001/v10n1a3.htm

ARÉVALO BERNAL, Oscar William. Otros "Metodología de análisis de riesgo de la empresa la casa de las BATERIAS S.A DE C.V" {En línea}. {01 mayo 2009} disponibleen:https://upload.wikimedia.org/wikipedia/commons/8/87/Riesgoinformatico.pdf

RAMÍREZ CASTRO, SANDRA. ORTÍZ BAYONA, Zulima "Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios" {En línea}. {15 agosto 2011} disponible en: https://dialnet.unirioja.es/descarga/articulo/4797252.pdf

CAMELO, Leonardo "Marco legal de Seguridad de la Información en Colombia" {En línea}. {23 febrero 2010} disponible en: http://seguridadinformacioncolombia.blogspot.com.co/2010/02/marco-legal-de-seguridad-de-la.html

RINCÓN CÁRDENAS, Erick "Instrumentos Normativos de Ciberseguridad" {En línea} disponible en: https://web.certicamara.com/media/58493/normativa-colombiana-en-materia-de-ciberseguridad-y-ciberdefensa-1-marzo-2014.pdf

MATEO, C. Rafael J. “Sistemas de Gestión de la Calidad – Un camino hacia la satisfacción del cliente – Parte I” {En línea}. {21 Agosto 2009} disponible en: http://qualitytrends.squalitas.com/index.php/item/108-sistemas-de-gestion-de-la-calidad-un-camino-hacia-la-satisfaccion-del-cliente-parte-i

NOVOA, A. Helena. “Metodologías para el análisis de riesgos en los sgsi” {En línea}. {Octubre 2015} disponible en: https://www.researchgate.net/publication/317149870_Metodologias_para_el_analisis_de_riesgos_en_los_sgsi

CONSEJO SUPERIOR DE LA JUDICATURA. Sala Administrativa. Manual de Calidad – Instrumentos internacionales Cumbre Judicial Iberoamericana – Sistema Integrado de Gestión y Control de Calidad. Colombia, 2013.

GUTIÉRREZ AMAYA, Camilo. "¿El mejor estándar para gestionar la seguridad de la información?" {En línea}. {08 junio 2012} disponible en: http://www.welivesecurity.com/la-es/2012/06/08/mejor-estandar-gestionar-seguridad-informacion/

SOSA, Johana. "Análisis de Riesgos" {En línea}. {27 enero 2012} disponible en: http://pegasus.javeriana.edu.co/~CIS1130SD03/Documentos_files/Analisis_de_Riesgos.pdf

DE FREITAS, Vidalina. "Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar" {En línea}. {Abril 2009} disponible en: http://www.scielo.org.ve/scielo.php?script=sci_arttext&pid=S1690-75152009000100004

DUQUE OCHOA, Blanca Rubiela. "METODOLOGÍAS DE GESTIÓN DE RIESGOS (OCTAVE, MAGERIT, DAFP)" {En línea}. {Octubre 2010} disponible en: https://auditoriauc20102mivi.wikispaces.com/file/view/Metodolog%C3%ACas+deGesti%C3%B2n+de+Riesgos.pdf

CENTRO CRISTOLÓGICO NACIONAL. EAR/PILAR. {En línea}. {Mayo 2018} disponible en: https://www.ccn-cert.cni.es/herramientas-ciberseguridad/ear-pilar.html

NIST, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guía para realizar evaluaciones de riesgos. {En línea}. {Mayo 2018} disponible en:https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

AGENCIA DE LA UNIÓN EUROPEA PARA LA SEGURIDAD DE LAS REDES Y LA INFORMACIÓN - ENISA. Inventario de gestión de riesgos / métodos y herramientas de evaluación de riesgos. {En línea}. {Mayo 2018} disponible en: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory

CONSEJO SUPERIOR DE LA JUDICATURA. Normatividad del SIGC. {En línea}. {Mayo 2018} disponible en: http://sistemagestioncalidad.ramajudicial.gov.co/ModeloCSJ/portal/index.php?idcategoria=219

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Decreto 4485 de 18 de noviembre de 2009. Elizabeth Rodríguez Taylor.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Norma Técnica de Calidad en la Gestión Pública. NTCGP 1000: 2009. {En línea}. {Mayo 2018} disponible en: http://sistemagestioncalidad.ramajudicial.gov.co/ModeloCSJ/documentos_portal/NTCGP1000-2009.pdf

INSTITUTO NACIONAL DE CIBERSEGURIDAD – INCIBE. Gestión de Riesgos, una guía de aproximación para el empresario. {En línea}. {Mayo 2018} disponible en: https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia_gestion_riesgos/guiagestionriesgos.pdf