DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA EL PROCESO DE GESTION DE LA INFRAESTRUCTURA TECNOLOGICA DEL COLEGIO SALESIANO BASADO EN MAGERIT

Investigador:

EDUARDO ALFONSO ROSALES MONTALBAN

Director|:

RAUL MARTELO

Universidad de Cartagena
Facultad de Ingenierías
Ingeniería de Sistemas

AGOSTO 2019

Abstract

This research work proposes the design of an information security management system in the context of the Salesiano San Pedro Claver School of Cartagena, applied to the administrative process of technological infrastructure management. Identify the elements that must be taken into account by an organization for the implementation of a management system by aligning its internal policies, according to international standards for the protection of information. The ISO 27001 standard is used as a standard model for the implementation of the management system; and MAGERIT as a methodology for risk analysis. Emphasis is placed on the analysis and management of risks, showing the protection measures for their treatment, as well as the characterization and valuation of assets, threats and safeguards, in the management of the technological infrastructure of the organization. With all this, a series of recommendations revolves around the solution of the findings, notice: the unplanned use of infrastructure, system crash due to resource depletion, denial of service and unauthorized access, threats which represents the highest levels of risk in the institution, mitigated with the implementation of control mechanisms and security policies, framed in the cycle of continuous improvement.

Resumen

Este trabajo investigativo, plantea el diseño de un sistema de gestión de seguridad de la información en el contexto del colegio salesiano San Pedro Claver de Cartagena, aplicado al proceso administrativo de gestión de infraestructura tecnológica. Identifica los elementos que deben ser tenidos en cuenta por una organización para la implementación de un sistema de gestión alineando sus políticas internas, de acuerdo a las normas internacionales para la protección de la información. Se hace uso de la norma ISO 27001 como modelo estándar para la implementación del sistema de gestión; y de MAGERIT como metodología para el análisis de riesgos. Se hace énfasis en el análisis y la gestión de riesgos, mostrando las medidas de protección para el tratamiento de los mismos, así como la caracterización y valoración de los activos, amenazas y salvaguardas, en la gestión de la infraestructura tecnológica de la organización. Se produce con todo ello, una serie de recomendaciones que giran en torno a la solución de los hallazgos, a saber: el uso no previsto de la infraestructura, caída del sistema por agotamiento de recursos, denegación de servicio y el acceso no autorizado, amenazas que representa los mayores niveles de riesgo en

la institución, mitigados con la implementación de mecanismos de control y políticas de seguridad, enmarcado en el ciclo de mejora continua.

Tabla de contenido

Introducción 1
Antecedentes locales 6
Antecedentes nacionales e internacionales 9
Capítulo I 12
La seguridad de Información y los sistemas de gestión 12
Etapas del ciclo Deming dentro de un SGSI 15
Capitulo II 18
Capitulo III 24
Identificación de los Activos 26
Valoración de los activos 29
Identificación de las amenazas 32
Caracterización y valoración de las amenazas 37
Caracterización de las salvaguardas 38
Estimación del impacto 39
Estimación del Riesgo 41
Capitulo IV 43
Riesgos en estado Crítico o Grave 46
Capítulo V 50
Resultados y recomendaciones 56
Conclusiones 57

INDICE DE TABLAS

Tabla 1. Relación de actividades del MAR y documentos generados. 26
Tabla 2. Identificación de Activos. 26
Tabla 3. Índices de valor de los activos. 30
Tabla 4. Criterios de valorización de activos. 30
Tabla 5. Relación error y ataque. 32
Tabla 6. Relación de identificación de las amenazas. 33
Tabla 7. Degradación del valor del activo. 37
Tabla 8. Probabilidad de ocurrencia de la amenaza. 38
Tabla 9. Tipos de protección 38
Tabla 10. Medición de Salvaguardas 39
Tabla 11. Estimación del Impacto 40
Tabla 12. Valorización del impacto 40
Tabla 13. Calificación del Riesgo 44

ÍNDICE DE ILUSTRACIONES

Figura 1 Modelo del ciclo Deming aplicado a los procesos de un SGSI..... 14
Figura 2. Mapa de procesos del Colegio Salesiano San Pedro Claver. 19
Figura 3. Diseño del proceso de gestión de Infraestructura Tecnológica. 20
Figura 4. Flujograma del mantenimiento preventivo..... 22
Figura 6. Grafica de estimación del riesgo del proceso de gestión..... 41

Introducción

"La información es un recurso estratégico para las empresas, pero su valor no suele estar reconocido, y por ende, no suele potenciarse ni gestionarse eficazmente, poniendo en peligro el desenvolvimiento y la supervivencia de dichas organizaciones" (Abu Talib, Khelifi, & Ugurlu, 2012). Como activo intangible la información constituye un componente indispensable, es la principal fuente de conocimientos de las empresas, es la base de los procesos de investigación, desarrollo e innovación tecnológica y su uso eficiente permite la mejora de los flujos de trabajo y optimiza los procesos organizacionales.

La forma en que la información se mueve en una organización depende de muchos factores tanto internos como externos, por ende, se debe entender que su administración no siempre depende de un solo ente. Para definir una buena gestión se debe conocer bien el ámbito de la organización y determinar los niveles de importancia o de valorización que tiene la información para las diferentes esferas de la organización.

En este orden de ideas, se debe tener en cuenta que la buena gestión de la información depende de la forma en que esta se documenta y organiza, y que es propio de la empresa la definición de métodos para almacenarla. Sin embargo en la actualidad se evidencia la tendencia al uso de la digitalización y de archivos informáticos como medios de documentación. Es por ello que los equipos de cómputo y las redes de comunicación se convierten en elemento esencial en organización empresarial.

Con este incremento de la informatización aumenta proporcionalmente la dependencia con relación a las tecnologías, que permite optimizar tiempos y recursos, pero que a su vez, representa nuevos riesgos a las organizaciones de acuerdo al modo específico en que operen. Es esta la razón por la que las compañías estén invirtiendo tantos recursos en la gestión de la tecnologías de la información y en la seguridad de sus infraestructuras (Goeke, Alebrahim, & Hatebur, 2014).

De acuerdo a lo consignado en el proyecto educativo de la facultad de Ingeniería para el programa de Ingeniería de sistemas, en el perfil profesional, se evidencia la necesidad de un carácter investigativo en quienes se forman para ser los ingenieros del futuro comprometidos con

el desarrollo tecnológico, científico, social y cultural de la región Caribe y del país, de tal modo que esto se refleje en el liderazgo de proyectos que promuevan el desarrollo de la disciplina, y la construcción de trabajos interdisciplinarios que den soluciones integrales y fomenten el avance científico técnico en esta área propiamente dicha.

Bajo estos términos, la presente propuesta investigativa diseña un sistema de gestión de la información, identificando amenazas y a su vez, el fortalecimiento de las mismas halladas en la seguridad de la información, bajo la metodología MAGERIT.

En este sentido, es manifiesta la articulación de un proyecto como este, que relaciona las políticas de seguridad, la implementación de un sistema de gestión y los recursos para el hallazgo de soluciones respecto a la administración de los recursos de software y hardware, que contribuyen a la optimización del manejo de la información empresarial, el diseño de procedimientos organizacionales, y la asesoría en un proceso interdisciplinario desde la perspectiva informática. Todos estos, elementos inmersos en el perfil ocupacional de los Ingenieros de sistema que promueve e intenta generar la Universidad de Cartagena.

Entendiendo la necesidad de gestionar de manera eficiente la información y los sistemas informáticos que la soportan, las organizaciones han desarrollado diferentes métodos y prácticas para proteger sus sistemas, estos mecanismos han llevado al desarrollo de estándares de calidad que permiten certificar la buena gestión de estos recursos por parte de las empresas. Uno de estos estándares y que además es base para el diseño de este sistema de gestión, es el estándar ISO 27001, un estándar diseñado para la gestión de la seguridad de la información y que hace uso de las prácticas desarrolladas en la familia de la ISO 27000.

Para el diseño y desarrollo de este estudio se parte de la necesidad de las organizaciones de proteger su información y su infraestructura, y se determinan las oportunidades e identifican las mejoras que la organización debe realizar para satisfacer los requisitos de la norma ISO 27001 al establecer un sistema de gestión de la seguridad de la información. Específicamente se ha tomado el proceso de “Gestión de la Infraestructura Tecnológica” del Colegio Salesiano San Pedro Claver de la ciudad de Cartagena, y en el marco de este proceso se hace un análisis de todos los elementos que lo componen, buscando de este modo alinear las políticas, directrices y procedimientos con la norma.

Este trabajo investigativo se constituye como una guía para las organizaciones con la función de realizar análisis y gestión de riesgos basados en la norma ISO 27001 de manera que se pueda tomar a modo de ejemplo en la implementación de un sistema de seguridad de la información. Ya que está aplicado a una organización educativa, resultarán como beneficiarios de primer grado el colegio Salesiano San Pedro en la ciudad de Cartagena, específicamente en los procesos administrativos, por otra parte, tanto estudiantes como profesionales del campo de la seguridad informática interesados en fortalecer las practicas organizacionales y así disminuir el déficit de profesionales de capacitados en la aplicación de estas normas. (Abu Talib, Khelifi, & Ugurlu, 2012)

En el ámbito de la practicidad, este trabajo investigativo tiene implicaciones positivas en la solución de problemas organizacionales referentes a la seguridad de la información. La organización, ha de propender mejorar, de acuerdo a los requisitos de la norma evidenciado en el diseño de un sistema de gestión que además de cumplir con la norma ayude al mejoramiento de los procesos propios de una institución educativa.

Así, se comprende que se atiende a un problema real organizacional, y se convierte en un primer paso de una investigación en donde se tome solo un proceso de la institución, permite abrir el campo a revisar cómo se comportaría el sistema cuando entran en juego campos no relacionados con la informática. De igual manera no pretende agotar la información a la que se refiere, sino que está abierta a la crítica constructiva para su futura construcción o complemento por posteriores investigaciones.

La importancia de este estudio se soporta en la necesidad conjunta de las organizaciones y entidades estatales para fortalecer el buen uso de la información y su protección, aspecto que se afianza a nivel nacional e internacional.

Actualmente en Colombia existen varias estrategias y estándares normativos que fomentan el desarrollo y la implementación de estas prácticas a nivel organizacional, tales como:

Ley 1266 de 2008: “Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”

Ley 1273 de 2009: “La cual determina el acceso abusivo a un sistema informático u obstaculiza ilegítimamente sistemas informáticos o redes de telecomunicación, la interceptación de datos informáticos, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte.”

Ley 1341 de 2009: "Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones"

Instrumento de Evaluación MSPI: “Es una herramienta que fue creada con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Públicas”

El Ministerio de tecnologías de la información y comunicaciones ha venido promoviendo la implementación de sistemas de gestión de seguridad de información Y se han ido trabajando desde los últimos 10 años, sin embargo la implementación y la adopción de estos conceptos son aún muy inmaduros, para 2013, “según los resultados del Formulario Único Reporte de Avances de la Gestión (FURAG), que tuvo en cuenta a 186 entidades del orden nacional, 88,5% del total de la Rama Ejecutiva: el 66% de las entidades ha iniciado el proceso de implementación de un SGSI, el 21% afirman no haber implementado el sistema y el 13% restante no respondió”. (Ministerio de Tecnologías de la Información y Comunicaciones, 2014)

Adicionalmente, el Min TIC promueve la educación formal sobre seguridad mediante becas condonadas hasta en un 100%, a través de Icetex y con el acompañamiento de entidades del Estado, para promover el conocimiento e implementación de la mejor cultura en seguridad TI. Esto demuestra el esfuerzo por parte del gobierno Colombiano para promover la implementación de buenas prácticas para la seguridad de la información.

Teniendo en cuenta todo lo anterior, esta monografía identifica las debilidades actuales dentro del proceso de ‘gestión de la infraestructura tecnológica’ y determina la manera en que este debe ser alineado con la norma para asegurar que se cumplan los requisitos de la misma, ayudando a la organización a determinar mejoras y a su vez servirá de guía para otras entidades que busquen fortalecer su sistema en el área de la seguridad informática.

En últimas, esta monografía busca presentar un análisis del sistema de gestión de la seguridad de la información en donde se determine el compromiso que la organización debe asumir para su implementación manteniendo las directrices estipuladas por la norma ISO 27001 y el uso de la metodología MAGERIT en el análisis y tratamiento de riesgos. Mostrando los beneficios que otorga la implementación de una metodología sistematizada en el análisis de riesgos, motivando la adopción de políticas que tengan como base la seguridad de la información.

Antecedentes locales

En el contexto en que se desarrolla este trabajo investigativo, encontramos el proyecto presentado por el ingeniero Luis Carlos Díaz Ricardo, para la obtención del título de especialista en seguridad informática de la universidad abierta y a distancia UNAD, en el municipio de corozal en noviembre del 2017, denominado: "**Diseño de un sistema de gestión de la seguridad de la información en la IPS ASSALUD de corozal sucre, mediante la implementación de la metodología magerit (v3.0) y la norma ISO 27001:2013**". Tiene como base la necesidad de una IPS de asegurar su servicio en el municipio y diseña un SGSI como solución a una problemática real de dicha organización.

El trabajo comienza con un interesante marco teórico y conceptual de la seguridad de la información mostrando diferentes técnicas y prácticas aplicadas en el desarrollo de su implementación, se puede deducir por el título, que **magerit** y la norma ISO 27001 fueron las guías normativas que utilizó para diseñar su solución.

Una fortaleza evidente de este proyecto radica en la contextualización de la organización y en cómo se levanta una rigurosa documentación del estado actual, de las percepciones de sus trabajadores y de los clientes con una serie de encuestas que toma como guía para la fase de análisis y valoración. El desarrollo de la solución esta guiado por el uso de la aplicación EAR/PILAR que lo apoya en el cálculo y la estimación de los valores que utiliza magerit para establecer un diagnóstico, en la documentación del proyecto no se dan detalles de las métricas utilizadas para establecer los valores que permitan un análisis continuo.

Para esta investigación que me he permitido traer como punto de referencia, se determinan los riesgos a los que la IPS está expuesta y se entrega una lista de recomendaciones para hacer el respectivo tratamiento de los mismos, pero se deja claro que la implementación y el seguimiento de estas técnicas no harían parte del proyecto y se continua con el levantamiento de las políticas de gestión que apoyan la implementación del sistema. Una limitante de esta investigación está relacionada con los aspectos de la norma, pues aunque toma muchos de requisitos de la misma no determina ni diseña técnicas de seguimiento o evaluación que son tan representativos en un sistema de gestión.

Desde otra perspectiva, Betin, Madera y Martelo, en el marco del grupo de investigación GIMATICA desarrollan la tesis de grado "**Software de apoyo para el proceso de implantación del sistema de gestión de seguridad de la información en organizaciones basado en la norma ISO 27001**" en el año 2015, para la obtención del título de ingenieros de sistemas en la Universidad de Cartagena. Este proyecto entra en detalle en los elementos que componen la norma ISO 27001 y genera una base teórica sobre la seguridad de la información y el ciclo de vida de un sistema de gestión de seguridad de la información.

Aunque esta investigación se concentra en el diseño de una aplicación para el apoyo de la implementación de SGSI, establece para su desarrollo una fuerte investigación sobre la seguridad de la información y la norma ISO 27001.

Esto permitió entender el ciclo de la norma y establecer la documentación necesaria para satisfacer los requisitos que esta presenta. De igual manera establece un estudio del estado del arte en el campo de la seguridad de la información y los estándares que la soportan. Sin embargo al ser un proyecto que busca soportar la implementación de un SGSI por medio de una herramienta informática, no entra en detalle en la manera en que estos procedimientos se realizan dentro de una organización.

Conviene distinguir que en la universidad tecnológica de Bolívar de la ciudad de Cartagena de Indias, Michelle Urruchurtu Gómez presento en Octubre del 2013 su proyecto de grado para optar por el título de ingeniera de sistemas que se llamó "**Plan estratégico de seguridad de información en una empresa del sector industrial basado en ISO/IEC 27001 caso de estudio: COTECMAR (corporación de ciencia y tecnología para el desarrollo de la industria naval, marítima y fluvial)**" En donde presenta situación de COTECMAR que busca alinear la organización con prácticas vigentes en la protección de datos, haciendo uso de la norma ISO 27001.

Hay que aclarar que aunque este proyecto no está directamente relacionado con magerit pues no lo implementa en su totalidad, si señala que usó la metodología para el análisis de riesgos y más importante aún hace referencia directa a la norma ISO 27001 de la cual apoya fuertemente el desarrollo de la implementación. Este proyecto se centró en los aspectos organizacionales de la norma y como la corporación tiene que adaptar su marco estratégico para alinearse con la norma.

Es importante señalar que la motivación principal de este proyecto es la búsqueda de la mejora continua de la organización en donde observan que tienen una oportunidad de mejora y deciden desarrollarla con base a las normas internacionales, pues en la investigación se define que se tenía un sistema de gestión para los riesgos pero que su nivel de especificación era muy vago por lo que buscaban establecer con claridad el estado de la corporación.

Como conclusiones en este proyecto se definen los hallazgos principales del análisis de riesgos y se establecen compromisos e iniciativas de los proyectos para enfrentar la situación en corto, mediano y largo plazo. Se entrega una lista de recomendaciones finales y se establece la importancia del constante seguimiento al proyecto para mantener los niveles de seguridad deseados.

Es inevitable notar la escasa documentación que existe en la región caribe sobre la implementación de sistemas de gestión de seguridad de la información o de metodologías como Magerit que buscan proteger la información. La mayoría de proyectos que se investigaron tenían como base normativa la ISO 27001 y se enfocaban más en el aspecto organizacional que en las bondades técnicas que se pueden definir en sistemas basados en tecnología.

Este comportamiento no se evidencia solamente en la región caribe sino que es una problemática a nivel nacional, basados en esto es que se puede afirmar que el gobierno ha generado políticas que incentiven a las organizaciones a implementar estas prácticas y que de manera conjunta y transversal se fortalezca el uso de mecanismos de control y medición de la seguridad de la información. Sin embargo, probablemente esto no tomara fuerzas hasta que los gobiernos comiencen a regular el uso de estas metodologías en sus instituciones. (Ministerio de Tecnologías de la Información y Comunicaciones, 2014)

Antecedentes nacionales e internacionales

En el contexto nacional, en la ciudad Tuluá del valle del cauca existe un estudio muy interesante en la aplicación de la metodología magerit: "**Análisis y gestión de riesgos de los sistemas de información de la alcaldía municipal de Tuluá aplicando la metodología magerit**", este fue desarrollado por el ingeniero Yamilet Bocanegra Quintero, que buscaba obtener el título de especialista en seguridad informática en la Universidad Nacional Abierta y a Distancia UNAD. En este proyecto se toma como necesidad la naturaleza de los servicios y tramites prestados por la entidad territorial en la que se hace necesario cumplir con requisitos de calidad y mejores prácticas de seguridad teniendo en cuenta el impacto de los procesos que aquí se efectúan.

Tomando como justificación estas necesidades, el ingeniero define las 3 etapas que constituyen el proyecto a saber: 1. el análisis y la valoración de los activos, 2. la detección y valoración de las amenazas y termina con la estimación del riesgo y 3. La definición de salvaguardas. Como resultado de esta investigación Yamilet presenta los hallazgos del análisis, identificando las amenazas que mayor riesgo representan para la organización y sugiere los tratamientos que se deben dar a cada uno, además lista una serie de recomendaciones para la alcaldía de Tuluá en donde busca fortalecer la implementación del sistema.

De este proyecto cabe resaltar el enfoque técnico que se le da a las soluciones implementadas; deja claro que el tratamiento de los riesgos es un trabajo en conjunto pero al mismo tiempo define técnicas específicas para la confrontación de las amenazas. Como limitantes de este proyecto se evidencia que aunque hace salvedad de la importancia del personal a la hora de hacerle seguimiento a la seguridad de la información, se concentra demasiado en la soluciones técnicas y deja pasar el apoyo logístico que lo acompaña, tal vez por el tipo de enfoque que se le da al proyecto.

De igual forma el proyecto presentado por Bastidas, López, Peña y Solarte quienes desarrollaron la tesis de grado "**Análisis de riesgos y recomendaciones de seguridad de la información al área de información y tecnología del hospital Susana López de Valencia de la ciudad de Popayán**" en octubre 2014, para optar por su título de ingenieros de sistemas en la Universidad Nacional Abierta y a Distancia UNAD. En este trabajo se desarrolla la importancia del análisis de riesgo para la seguridad de la información de una organización.

En este orden de ideas, la investigación se enmarcó en un caso de estudio que busca determinar la importancia de la seguridad de la información con las técnicas de análisis de riesgos como: MAGERIT, la guía COBIT y la aplicación PILAR. Su principal motivación fue la implementación de medidas de seguridad haciendo énfasis en la detección de los activos y sus amenazas, usando como técnicas de recolección de datos la encuesta y la entrevista, teniendo como resultado una serie de recomendaciones para la organización.

A partir de este estudio, se pudo establecer la metodología para la realización del análisis de riesgo del sistema de gestión que se presenta en esta monografía.

En contraste a lo mencionado antes, fue evidente que la investigación usó la norma ISO 27001 para su desarrollo, pero no hizo señalamientos sobre los procedimientos de seguimiento y mejora, dejando la posibilidad de continuar con el caso de estudio en próximas oportunidades, como lo señalan en la conclusión.

A nivel internacional podemos señalar como un proyecto muy importante el informe sobre la implementación de un análisis de riesgos usando esta metodología en la agencia estatal de meteorología AEMET. Este informe fue elaborado por Julio González Breña en el año 2008. En este informe se detalla como la organización tiene sistemas abiertos de información y publicación de informes que ameritan una constante revisión de la veracidad e integridad de su información.

La AEMET informa que desde tiempo atrás han encaminado sus esfuerzos para modernizar sus procesos y fortalecer los pilares de la seguridad en las unidades que componen su distribución territorial, compuesta por más de 50 oficinas. Sin embargo sienten la necesidad de formalizar la gestión de los riesgos diseñando un sistema de gestión de la protección que toma como base normativa la ISO 17799, la UNE 71503, la UNE 71501, magerit y la aplicación PILAR, además de normativas de marcos legales y reglamentarios para la organización.

Presentan como conclusiones del proyecto los beneficios que trae usar la aplicación PILAR teniendo en cuenta la amplitud del análisis, en donde existían más de 230 tipos de activos, y esto le convierte en una justificación necesaria para hacer uso de la aplicación adicional a esto, el hecho de diseñar las relaciones de dependencias de un sistema tan grande funda una maraña interminable de conexiones. Señalan que su hallazgo más valioso es el poder involucrar las preocupaciones

técnicas de la seguridad con la dirección de la organización de manera que todos los integrantes de la agencia estén alineados con las políticas requeridas.

A nivel nacional existe nuevamente la dificultad de encontrar casos de estudios para apoyar la investigación, es muy común encontrar proyectos de implementación de SGSI basados en la norma ISO 27001 pero desarrollados en contextos administrativos, muchas veces guiados por ingenieros industriales y administradores de empresas que enfocan su desarrollo más a las políticas y gestión de procesos que a la implementación y detección especifica de salvaguardas o mecanismos de tratamiento de riesgos en el área de tecnología. Esto no quiere decir que las implementaciones no son válidas pero para el contexto de esta monografía no presentaban mayor valor argumentativo.

A nivel internación sin embargo se encontraron varios proyectos que hacían uso tanto de la norma ISO 27001 y de la metodología magerit, muchos de ellos han sido citados en el desarrollo de esta monografía tomando las enseñanzas más importantes como justificación y guía para la toma de decisiones. Un comportamiento común encontrado en la mayoría de los proyectos es el uso de partes de la norma ISO 27001 que se apoyan del análisis de riesgos y acotando la implementación o el diseño de los requisitos de la norma que hablan de la gestión organizacional, haciendo una interesante comparación con lo que se encontraba con los proyectos de áreas más administrativas.

Por último se hace necesario señalar como las investigaciones citadas, describen la importancia del trabajo en equipo y de la creación de una cultura transversal que busque fortalecer los aspectos de la seguridad de la información, aspecto que nos permite comprender que no es tan importante el uso de una tecnología o una metodología en específico ya que estas pueden adaptarse al tipo de negocio, pero el trabajo en conjunto por un objetivo, en este caso la seguridad de la información representa un beneficio mayor que el uso de una metodología especifica.

Capítulo I

La seguridad de Información y los sistemas de gestión

La seguridad de la información es una disciplina asociada tradicionalmente a la gestión de tecnologías de la información, cuyo propósito es mantener niveles aceptables de riesgo de la información organizacional y de los dispositivos tecnológicos que permiten su recolección, procesamiento, acceso, intercambio, almacenamiento, transformación y adecuada presentación (Valencia Duque, 2017). Esta misma, ha sido definida por la norma ISO/IEC 27000 como la preservación de la confidencialidad, integridad y disponibilidad de la información.

En el constante avance de las TIC como soporte primordial de la información y la documentación empresarial, se ha creado una falsa comparación de la seguridad informática con la seguridad de la información, guiando de manera errónea los esfuerzos de las organizaciones para implementar soluciones tecnológicas como el objetivo de la seguridad de la información.

De modo que identificar el esfuerzo de una organización para garantizar la seguridad de la información permite entender el concepto de SGSI, el cual Seclén Arana define como : "*Un Sistema de Gestión de Seguridad de la Información - SGSI - es un conjunto de políticas y procedimientos cuyo objetivo es administrar la Seguridad de la Información de una organización, proporcionando una metodología sistemática, documentada y fuertemente enfocada en los riesgos que pueda enfrentar una organización*" (Seclén Arana , 2016).

Desde esta perspectiva se entiende que lo que persigue un Sistema de Gestión de Seguridad de la Información es proteger la información como recurso valioso, para lo cual debe proteger de igual forma los diferentes medios a través de los cuales se genera, almacena, procesa, transmite, circula y transforma en un recurso útil para los negocios (Valencia Duque, 2017). Ahora bien, un SGSI se conforma de un trabajo en conjunto entre las herramientas, tecnologías, políticas, procedimientos, metodologías y personal para garantizar niveles adecuados de protección de la información.

En este contexto, se ha observado, que existe una alta gama de directrices, normas técnicas, estándares y mejores prácticas desarrolladas por diferentes entidades tanto privadas, como gubernamentales, desde las que se ha creado una visión fortalecida y documentada de los sistemas

de gestión de la seguridad de la información (Susanto, Nabil Almunawar, & Chee Tuan, 2011). Sin embargo no existe una formula única que garantice la seguridad de la información, y por ello la necesidad por parte de las organizaciones de mantener un cuadro de referencia que asegure la adopción de mejores prácticas de seguridad para alcanzar un nivel adecuado en la protección y madurez del sistema.

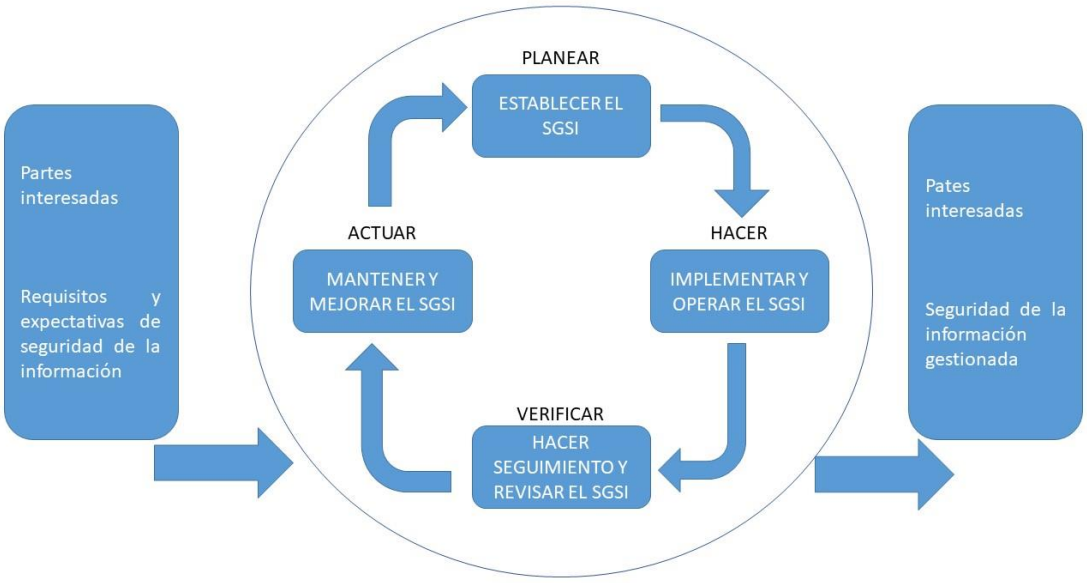
A este propósito, alinear las organizaciones para cumplir con las demandas de seguridad es una tarea desafiante, por ello existen normas como la ISO 27000 que ofrece una manera de lograr este objetivo (Beckers, Fabender, Heisel, & Schmidt, 2012). El estándar normativo de la serie mencionada, la ISO 27001 contiene los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI). La norma prescribe un proceso que se adapta a las necesidades de cualquier tipo de organización para la implementación de dichos sistemas.

La ISO 27001 se diseñó para garantizar la selección de controles de seguridad adecuados y proporcionales para proteger los activos de información, introduce un modelo cíclico conocido como modelo Deming o PHVA (Planear-Hacer-Verificar-Actuar) y tiene como objetivo establecer, implementar, monitorear y mejorar la efectividad de los procedimientos de seguridad de la información (Susanto, Nabil Almunawar, & Chee Tuan, 2011). Según el estudio realizado por (Shojaie, Federrath, & Saberi, 2014) En diciembre de 2011, se emitieron más de 17000 certificados en todo el mundo, mostrando la importancia de tener un sistema de gestión certificado en la industria y el impacto que tiene en la sociedad la seguridad de la información en la era de la digitalización.

Comprendamos que la Norma ISO 27001 hace parte de la familia de normas 27000, todas ellas enfocadas a la seguridad de la información e interesadas específicamente en aspectos de su implementación así: gestión de riesgos en la ISO 27005, medición de la seguridad en la ISO 27004, código de prácticas en el desarrollo de un SGSI en la ISO 27002, entre otros, y por último, las directrices para la implementación de un SGSI están en la ISO 27001, la cual se soporta fuertemente en la ISO 27000 para la definición de los aspectos más relevantes y los términos en el enfoque de la seguridad informática.

Este trabajo investigativo busca diseñar un SGSI teniendo como guía las directrices plasmadas por la ISO 27001, lo que hace capital el conocimiento de la estructura de esta norma, para comprender con claridad los requisitos propios de su implementación. Se hace uso de MAGERIT, un proceso de análisis y gestión de riesgo, como metodología de implementación de las fases Planear y Hacer del ciclo Deming.

Figura 1 Modelo del ciclo Deming aplicado a los procesos de un SGSI



Tomada de (Urruchurtu Gomez & Zuñiga Silgado, 2013)

El ciclo Deming o PHVA consiste en 4 etapas que buscan asegurar la mejora continua de un sistema, pueden ser implementadas sobre cualquier sistema de gestión definiendo de manera particular las actividades de acuerdo al contexto y los objetivos del mismo. La ISO 27001 usa este modelo para asegurar que el sistema de gestión evolucione y mejore constantemente con cada iteración del ciclo, manteniendo un sistema cada vez más maduro; los parámetros iniciales del ciclo para un SGSI son los requisitos y expectativas de seguridad de la información y el resultado de su implementación es una seguridad de la información gestionada.

Etapas del ciclo Deming dentro de un SGSI

Planear: La planificación es la etapa inicial del ciclo, conlleva todas las actividades relacionadas con la documentación del sistema. En esta fase se busca realizar un estudio para conocer el estado de la organización, representa su base fundamental, pues es aquí, donde se define el alcance que tendrá de acuerdo a sus objetivos.

Para establecer estos objetivos y metas, se debe conocer todos los elementos que componen la organización o el proceso a evaluar. Esto requiere la presencia de un análisis de riesgo en donde se identifiquen los elementos y se determine el riesgo al que están expuestos. De igual manera se establece el tratamiento que se le dará a los riesgos encontrados para reducir su nivel de afectación, documentando cada uno de estos hallazgos.

Dentro de la norma ISO 27001 en el capítulo 6:*"PLANEACIÓN",* se dan los detalles y requisitos para la correcta implementación de esta etapa en un SGSI.

Hacer: Esta etapa consiste en la implementación de todas las políticas y medidas de seguridad diseñadas en la fase de planeación. Aquí, la organización instala las nuevas tecnologías utilizadas para la protección informática, así como desde esta etapa entran en vigencia los procedimientos establecidos en la etapa de planeación, se concentra el esfuerzo en garantizar la seguridad, capacitar y formar el personal.

La ISO 27001 hace referencia a esta fase en sus numerales *7. Soporte* y *8. Operación*, en ellos describe los compromisos por parte de la organización para implementar un SGSI. Dentro de este proyecto el Hacer se establece en los manuales de procedimientos y en la definición de responsabilidades, los cuales se presentan como documentos anexos a la investigación y se desarrollan en el ámbito del sistema.

Verificar: La fase de verificación consiste en evaluar la eficacia del sistema y de los controles implementados. Esta etapa presta especial importancia al levantamiento de registros y a la creación de indicadores de desempeño. Dentro de esta fase se establece la forma en que se registra y mide el correcto funcionamiento del sistema, todo esto en base al análisis realizado con anterioridad.

En la ISO 27001 se evidencia la fase de verificación en el numeral *9. Evaluación del desempeño,* en donde se establece como requisito la medición del sistema y de sus implementaciones.

Actuar: En esta fase se interviene el sistema de acuerdo a los niveles encontrados en la etapa de verificación. La fase actuar está estrechamente relacionada con la verificación y normalmente se pueden implementar en un mismo procedimiento, dado que de acuerdo a los hallazgos de la etapa anterior, se tomaran las acciones de mejora.

La ISO 27001 habla sobre los procedimientos de la fase Actuar en el capítulo *10. MEJORA* y detalla sobre las acciones para controlar y corregir las no conformidades que se identifican en la fase de verificación.

Teniendo en cuenta las fases y los requisitos de la norma señalados, la ISO 27001 hace referencia a la necesidad de documentar las actividades relacionadas tanto con la implementación del sistema como con el desarrollo de los procedimientos. A este respecto, se debe tener en cuenta el proyecto presentado por (Urruchurtu Gomez & Zuñiga Silgado, 2013) que describe que un SGSI conforme con el estándar ISO/IEC 27001:2005 consta de los siguientes elementos:

- Análisis de riesgos
- Cuerpo normativo, incluyendo:
- Definición del alcance del SGSI
- Política de seguridad.
- Declaración de aplicabilidad, que detalla los controles necesarios para alcanzar los objetivos de seguridad fijados.
- Procesos de seguridad.
- Procedimientos de seguridad.
- Registros de seguridad
- Asignación de funciones y responsabilidades:
- Dirección
- Ejecución de procesos y controles
- Revisión del SGSI
- Formación a todos los participantes

Y basando el análisis de riesgos en la metodología MAGERIT se tiene que los elementos que la componen son:

- **Modelo de Valor**: Informe que detalla los activos, sus dependencias, las dimensiones en las que son valiosos y la estimación de su valor en cada dimensión.
- **Mapa de Riesgos:** Informe que detalla las amenazas sobre cada activo, caracterizándolas con su frecuencia y su degradación potencial.
- **Declaración de Aplicabilidad:** Informe que recoge las contramedidas que se consideran apropiadas para defender el sistema de información bajo estudio.
- **Evaluación de Salvaguardas:** Informe que detalla las salvaguardas existentes calificándolas en su eficacia para reducir el riesgo que afrontan.
- **Estado de riesgo:** Informe que detalla para cada activo el impacto y riesgo potencia frente a cada amenaza.

En resumen, se tiene que el sistema de gestión de la seguridad de la información esta soportado por un modelo PHVA y busca mejorar a través del tiempo y aprender de su propia implementación, y ya que se hace uso de la metodología MAGERIT para el análisis de riesgos, se incorporan nuevos requisitos y actividades para su implementación.

Capitulo II
Contexto de la organización y alcance del sistema

La importancia de los sistemas de gestión en las organizaciones se enmarca en el manejo de la información y la sistematización de la misma, para llevar a cabo cuanto se propone en la misión y visión que la rige, en este sentido el presente proyecto tiene por objeto diseñar un SGSI como solución específica para el proceso de gestión de la infraestructura tecnológica del colegio salesiano San Pedro Claver, debido a que se entra en detalle en los componentes de la institución como caso de estudio, se hace necesario describir con claridad la constitución de la organización y del proceso mencionado.

Así mismo, interesa centrarse en los elementos que componen el proceso 'gestión de la infraestructura tecnológica', sin embargo siendo un proceso de apoyo se entiende que tiene una relación directa o indirecta con muchas otras entidades y gestiones dentro de la organización. Existe pues, una fina línea que separa los elementos que le pertenecen y con los que tiene relación. Sin embargo se determina que un activo posee incidencia dentro del proceso y es por ello que se debe documentar.

En otras palabras, entender el contexto de la organización permite establecer con claridad el alcance del sistema, teniendo en cuenta que su implementación está ligada directamente al proceso.

Por consiguiente se tiene que, el colegio Salesiano san Pedro Claver de Cartagena es una institución educativa con una población estudiantil 1300 estudiantes aproximadamente, que brinda servicio educativo en los niveles de pre-escolar, básica primaria, básica secundaria y media para la obtención del título de bachiller académico; que en la búsqueda de brindar un servicio de educación óptima, ha establecido un Sistema integrado de Gestión de Calidad, de acuerdo a los criterios de la NTC ISO 9001.

Esta organización posee una política de gestión que busca establecer su compromiso con el mejoramiento continuo del sistema de gestión de calidad, seguridad, salud en el trabajo, y medio ambiente, atendiendo la satisfacción de las necesidades y expectativas de la comunidad educativa en general, en el marco de cumplimiento de los requisitos legales vigentes y de los propios suscritos por la institución.

En el desarrollo de este compromiso, y para cumplir los requisitos de la norma ISO 9001, la institución posee un conjunto de procesos y procedimientos, en donde se definen las actividades que realiza la organización en busca de garantizar la misión y de orientar la obtención de la visión que se establecen en el direccionamiento estratégico de la organización. En este sentido, tenemos definidos estos elementos así:

Misión: El colegio Salesiano San Pedro Claver es una Institución Educativa, de carácter privado, que con la participación de la Comunidad Educativo Pastoral, se integra en la misión evangelizadora de la Iglesia. Fiel al carisma de Don Bosco ofrece educación académica formal integral a niños, niñas y adolescentes para hacer de ellos "buenos cristianos y honestos ciudadanos"

Visión: El Colegio Salesiano San Pedro Claver se proyecta hacia el 2020, como una obra significativa para la ciudad de Cartagena, porque logra ser:

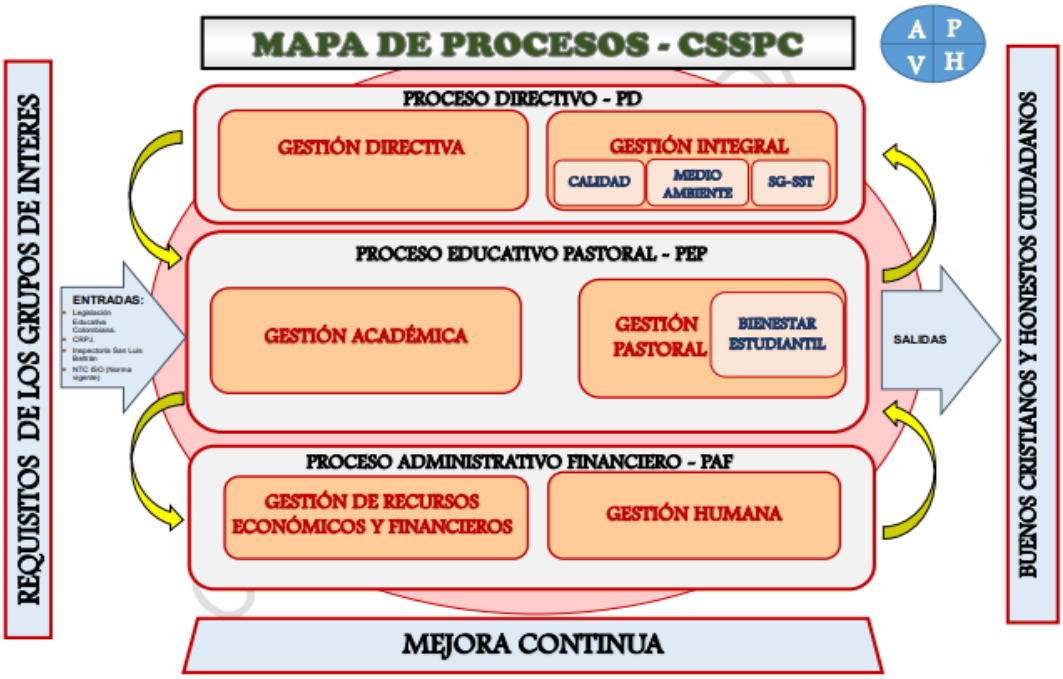
Una casa que acoge familiarmente,

Una escuela que educa integralmente,

Una parroquia que educa en la fe cristiana,

Un patio en donde se comparte y se hacen amigos.

Figura 2. Mapa de procesos del Colegio Salesiano San Pedro Claver.

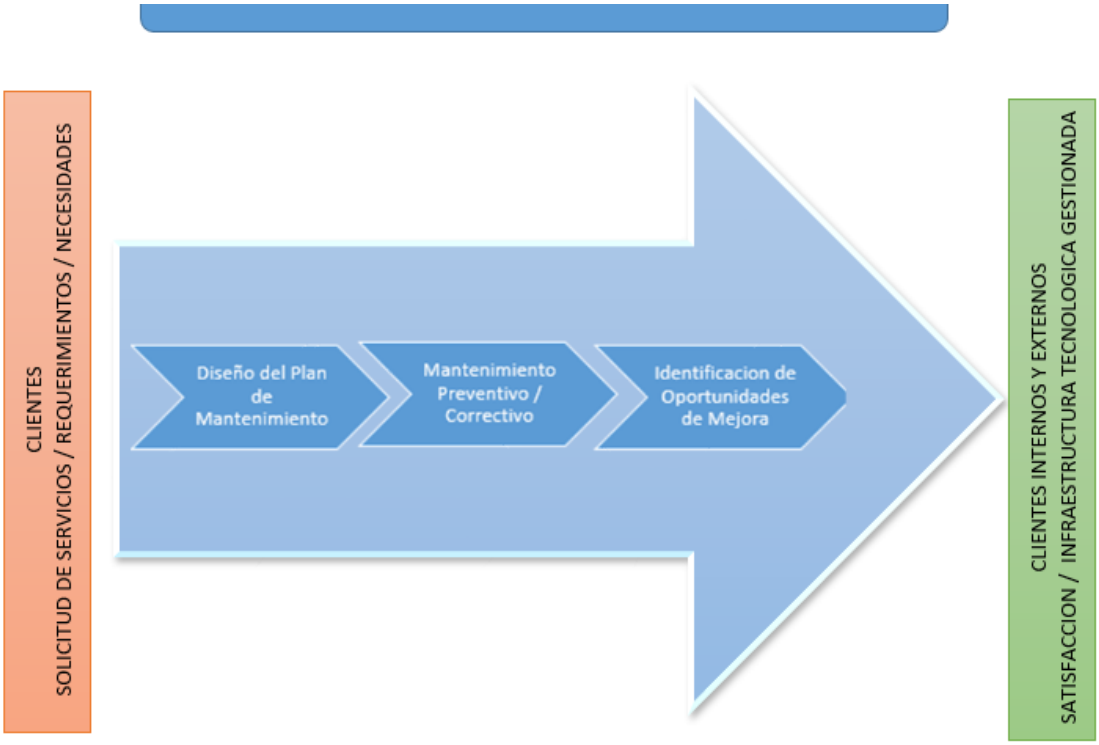


Suministrado por la administración de la organización.

La institución está compuesta por tres macro procesos que representan los tipos de procesos de una organización: Los procesos estratégicos representados en el proceso directivo - PD, los procesos misionales en el proceso educativo pastoral - PEP, y los procesos de apoyo en el proceso administrativo financiero - PAF. Cada uno de estos macro procesos se apoya de procesos de gestión para el desarrollo de sus actividades y el cumplimiento de los objetivos.

Ahora bien, un proceso que interesa con particularidad es el de gestión de la infraestructura tecnológica, que hace parte de la gestión de recursos económicos y financieros, tiene como objetivo, garantizar el correcto funcionamiento de los equipos informáticos de la institución y satisfacer las necesidades de la comunidad con relación al uso de tecnología.

Figura 3. Diseño del proceso de gestión de Infraestructura Tecnológica.



Como se observa en el diagrama este proceso está implementado desde tres procedimientos que describen con detalle las actividades; toma como entradas las necesidades de la institución y a través del procedimiento de diseño del plan de mantenimiento, se estructura un programa para

desarrollar las actividades que a su vez garantizan el buen funcionamiento de la infraestructura ejecutadas desde los procedimientos de Mantenimiento preventivo y correctivo para resolver una falla en el funcionamiento de la infraestructura o satisfacer una necesidad que responda a las competencias del área de tecnología.

Por último, en busca de la mejora continua, se establece el procedimiento de Identificación de oportunidad de mejora**,** que consiste en el análisis de los registros y documentos que se generan en el desarrollo del proceso, analiza el comportamiento de su implementación para identificar oportunidades de mejora. Basados en este análisis se pueden establecer acciones correctivas en caso de ser necesarios o modificar la implementación del proceso en busca de su correcta ejecución.

Adviértase que, el proceso de gestión de infraestructura tecnológica, vela por garantizar el correcto funcionamiento de los equipos informáticos de la institución y por ende proteger la información que en ellos reposa.

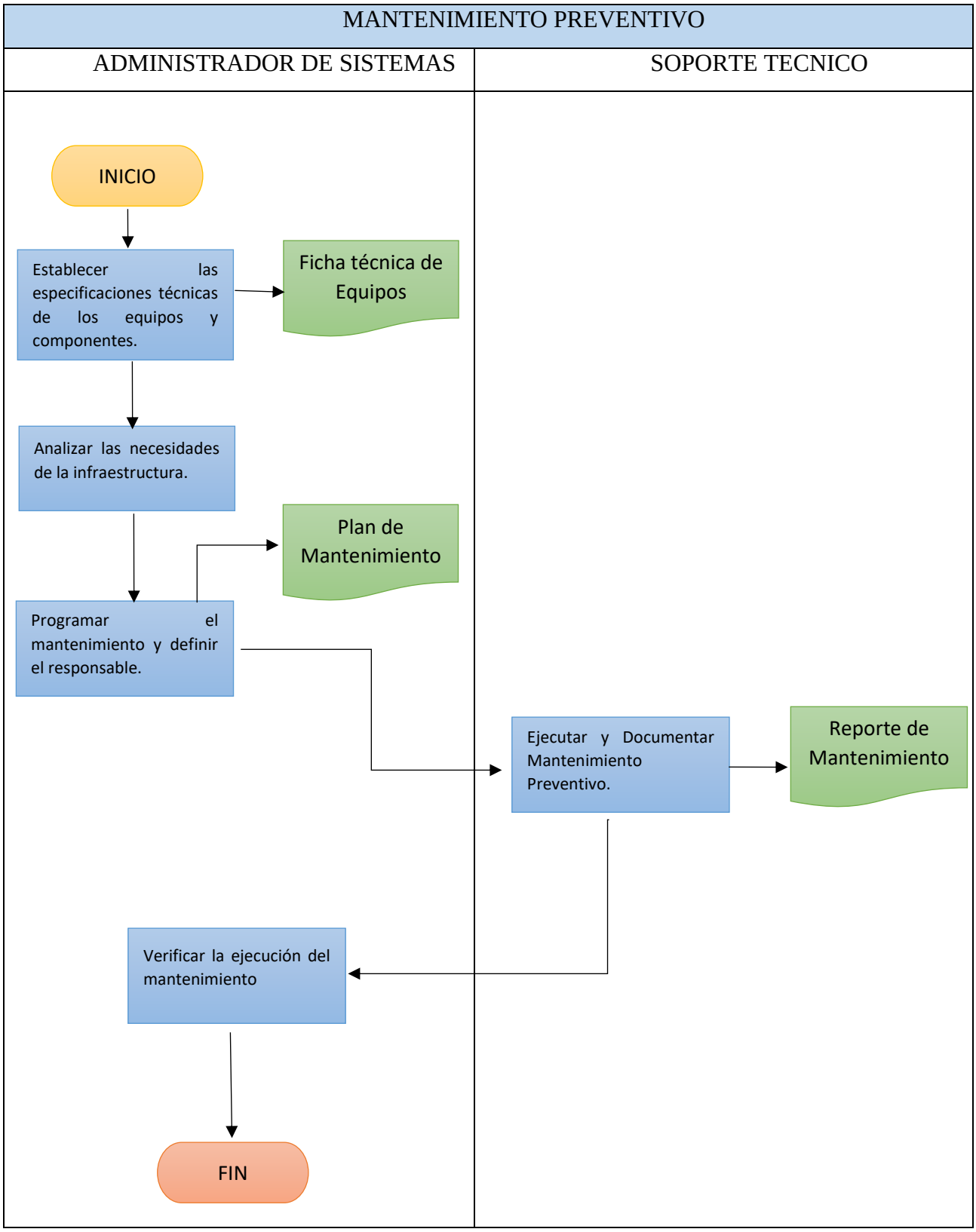


Figura 4. Flujograma del mantenimiento preventivo

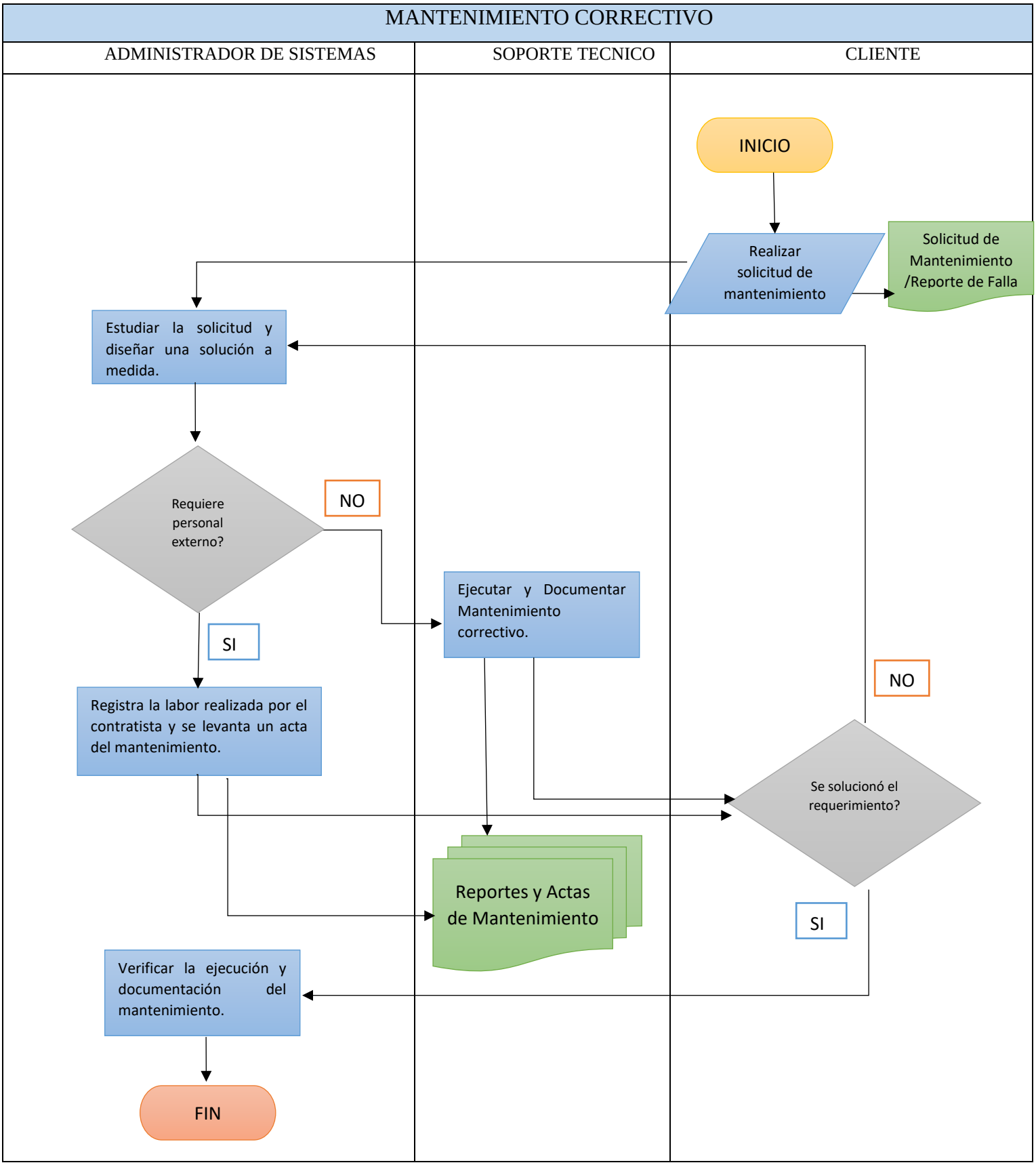


Figura 5. Flujograma del mantenimiento Correctivo

Capitulo III

Análisis de Riesgo

El análisis de riesgo consiste en un proceso sistemático para estimar la magnitud de los riesgos a los que está expuesta una organización (Gobierno de España, 2012) .Sobran razones para comprender que su implementación no es un fin en sí mismo, sino un medio que ayuda a determinar la gestión que se debe realizar dentro de la entidad para garantizar la seguridad de la información.

El análisis de riesgo se convierte en la base fundamental de un SGSI ya que ofrece un reporte del estado actual de la seguridad de la información en la entidad. Su objetivo general, es identificar las causas potenciales de los principales riesgos que amenazan el entorno informático. Esta identificación se realiza en una determinada área para que se pueda tener información suficiente, optando por un adecuado diseño e implantación de mecanismos de control con el fin de minimizar los efectos de eventos no deseados (Bastidas Paruma, Lopez Ortiz, & Peña Hidalgo, 2014).

De manera más específica, se entiende el análisis de riesgo como *"una herramienta que permite identificar las necesidades de seguridad sobre los distintos activos del sistema para determinar la vulnerabilidad del mismo ante amenazas y estimar el impacto potencial que podría ser causado por la pérdida de confidencialidad, integridad, disponibilidad de la información y recursos del sistema" (Garcia Vasquez & Bojorque, 2013).*

Ahora bien, la importancia de este proceso radica en su pertinencia al iniciar el diseño de un sistema de gestión, pues en base a este, se consolidan los procesos que garantizan la seguridad de la información. Como se indicó, el análisis de riesgos debe hacerse de manera rigurosa y coherente para no poner en peligro la información y la actividad de la organización.

Adviértase, pues que existe gran cantidad de métodos para realizar un análisis de riesgo, sin embargo, debido a que el presente está basado en la seguridad de la información se hará uso de MAGERIT v3.0 por su enfoque al área informática y su compatibilidad con la ISO 27001. Esta es una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica del gobierno Español, para minimizar los riesgos de la implantación y

uso de las Tecnologías de la Información, enfocada a las Administraciones Públicas (Gobierno de España, 2017).

Si bien, MAGERIT posee una guía detallada en 3 libros donde describen las actividades y pasos que se deben seguir para desarrollar un eficiente análisis de riesgo, se dividen en: métodos, catálogo de elementos y guía de técnicas. Aunque la guía es muy específica le da toda libertad al analista de elegir las herramientas y técnicas que crea convenientes en su investigación pero define un método que organiza por tareas y actividades definidas en el MAR – *'Método de Análisis de Riesgos'* de la siguiente manera:

MAR.1 Caracterización de los Activos

MAR.11 – Identificación de los activos

MAR.12 – Dependencias entre activos

MAR.13 – Valoración de los activos

MAR.2 Caracterización de las amenazas

MAR.21 – Identificación de las amenazas

MAR.22 – Valoración de las amenazas

MAR.3 Caracterización de las salvaguardas

MAR.31 – Identificación de las salvaguardas pertinentes

MAR.32 – Valoración de las salvaguardas

MAR.4 Estimación del estado de riesgo

MAR.41 – Estimación del impacto

MAR.42 – Estimación del riesgo

El resultado de estas actividades hace parte de la documentación del sistema de gestión de la seguridad de la información y conforman la creación del cuerpo normativo tanto de la norma como de la metodología MAGERIT, teniendo como desarrollo la creación de esto documentos con respecto a las actividades:

Tabla 1. Relación de actividades del MAR y documentos generados.

Modelo de Valor	MAR.1 Caracterización de los Activos
Mapa de Riesgos	MAR.2 Caracterización de las amenazas
Evaluación de Salvaguardas	MAR.3 Caracterización de las salvaguardas
Declaración de Aplicabilidad	MAR.4 Estimación del estado de riesgo
Estado de riesgo	MAR.4 Estimación del estado de riesgo

Identificación de los Activos

Esta actividad consiste en identificar los activos que componen el sistema, determinando sus características, atributos y clasificación en los diferentes tipos. La clasificación de los activos depende de su naturaleza, generando políticas de acuerdo a la organización y su interés. Las técnicas que son utilizadas en la identificación de activos en este proyecto son la observación directa y la entrevista, aplicadas a los funcionarios que tuviesen relevancia dentro del sistema.

MAGERIT establece un estándar de documentación para la identificación de activos esenciales del sistema, que consiste en agruparlos por la naturaleza del activo y asignarles un código de identificación como primera tarea. A continuación se describen los activos que componen el sistema:

Tabla 2. Identificación de Activos.

[D] Datos
La información es uno de los activos más importantes para cualquier organización, en el Colegio Salesiano San Pedro Claver los datos están almacenados de distinta manera, están agrupados en forma de archivos físicos, archivos de texto, ficheros, bases de datos y otros. Sin embargo el alcance de este proyecto estableció que se estudiaría todo lo relacionado con un proceso en específico *'la gestión de la infraestructura tecnológica'*, por ende los activos que hace referencia esta naturaleza son los relacionados con la infraestructura tecnológica. Aunque muchos de los Datos de la organización están soportados por esta infraestructura, su gestión no está dentro de las actividades del proceso. ➢ **Datos Vitales:** Son esenciales para la supervivencia de la empresa, su carencia o daño afectarían directamente los procesos realizados o la existencia de la organización.

- **Datos de carácter personal:** cualquier información concerniente a personas físicas identificadas o identificables. Estos datos están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y derechos fundamentales de los trabajadores.
- **Datos Clasificados:** Son los que están sometidos a normatividad de acceso y distribución, son confidencialmente relevantes.

[Activos]

- **[d_scode_si]Código Fuente del sistema integrado**
- **[d_passw]Credenciales de Acceso**
- **[d_DB_incrip]Base de datos de inscripciones y matriculas**
- **[d_DB_encuest]Base de datos de encuestas**
- **[d_DB_si]Base de datos del sistema integrado**
- **[d_drivers]Archivos de configuración y controladores de equipos**
- **[d_doc_infrs]Archivos de documentación de infraestructura**
- **[d_backup_files]Ficheros de Respaldo y Copias de seguridad**

[S] Servicios

Los servicios son las funciones que satisfacen a un usuario, tanto interno como externo. Los clientes internos serían los docentes y administrativos que hacer uso de la infraestructura y los externos serían los estudiantes y padres de familia.

También existen tipos de servicio: Los servicios contratados y los servicios internos:

- **Servicios Internos:** Son los servicios prestados por un departamento, para satisfacer las necesidades de otro dentro de la misma organización.

- **Servicios Contratados:** Son los servicios que prestan otras organizaciones (Outsourcing), y que se requieren en la empresa para llevar a feliz término un proceso y cumplir con los objetivos propuestos.

[Activos]

- **[s_mails]Servidor de correos**
- **[s_ftp]Servicio de trasferencia de archivos**
- **[s_web]Servicios del portal web**

[SW] Aplicaciones (Software)

Este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.

[Activos]

- **[sw_si]Sistema integrado**

- **[sw_siigo]Sistema de gestión contable**
- **[sw_school]Sistema de gestión académica**
- **[sw_so]Sistemas operativos**
- **[sw_office]Ofimática**
- **[sw_antivirus]Antivirus**
- **[sw_browser]Navegador Web**
- **[sw_dev]Entorno de Desarrollo**
- **[sw_mang]Aplicaciones de Gestión y Monitoreo**

[HW] Equipos Informáticos las avanza

Este epígrafe se refiere a todos los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos

[Activos]

- **[hw_server]Servidor**
- **[hw_pc_adm]Equipos de informática de uso administrativo**
- **[hw_pc_edu]Equipos de informática de uso educativo**
- **[hw_vbeam]Proyectores**
- **[hw_printer]Impresoras**
- **[hw_firewall]Fortigate**
- **[hw_accespoint]Puntos de acceso**
- **[hw_sw_route] Switches y routers**

[COM] Redes de comunicaciones

Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.

[Activos]

- **[com_pstn]Red telefónica**
- **[com_radio]Red Inalambrica**
- **[com_lan]Red Local**
- **[com_internet]Internet**

[Media] Soportes de información

En este epígrafe se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

[Activos]

❖ **[media_net]Almacenamiento en red** ❖ **[media_hd_ext]Disco externo de respaldo**
[AUX] Equipamiento Auxiliar
En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
[Activos] ❖ **[aux_ups]Sistemas de alimentación ininterrumpida** ❖ **[aux_furnit]Gabinetes y mobiliario**

Valoración de los activos

Una vez identificados los activos se procede a documentar sus características y atributos dentro de la ficha técnica de activos esenciales, que se encuentra en los anexos del libro 2 de MAGERIT versión 3.0. Aquí, se declara la descripción del activo, el propietario o el responsable, la ubicación en los casos correspondientes, las dependencias entre ellos y la valoración en las distintas dimensiones.

Ya hemos, pues, descubierto que la metodología para determinar las valoraciones de los activos varía de acuerdo a la naturaleza de la organización, del activo y del entorno del sistema. En este caso, los activos están relacionados directamente con el área de informática se establecieron como técnicas de valoración una tabla de índices cualitativos y se determinó su criterio por medio de reuniones con los funcionarios dentro del proceso.

Los activos fueron valorados dentro de tres dimensiones independientes a saber:

La disponibilidad: Propiedad de ser accesible y utilizable a pedido de una entidad autorizada.

La integridad de los datos: Propiedad de proteger la precisión y completitud de los activos.

La confidencialidad de la información: Es la propiedad que define que la información no está disponible o está protegida a individuos, entidades o procesos no autorizados.

En el proceso de valoración se establece un índice correspondiente a la dimensión del activo en caso de que esta sea afectada, es decir, la importancia de ese activo para la organización. El índice de valor se establecerá a través de criterios cualitativos organizados en una tabla y

representados en una escala de 0 a 10 en donde cero es un valor despreciable y 10 es un valor de daño extremo para la organización:

Tabla 3. Índices de valor de los activos.

Valor		Criterio
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante

A continuación se presenta la tabla que relaciona los criterios de evaluación y el valor que tienen dentro de la escala de 0 a 10.

Tabla 4. Criterios de valorización de activos.

VALOR	CRITERIO
0	1. No supondría daño a la reputación o buena imagen de las personas u organizaciones. 2. No afectaría la seguridad de las personas. 3. No detendría la prestación del servicio. 4. Supondría pérdidas económicas mínimas. 5. Tiempo de recuperación del servicio es más de 5 días.
1	1. Pudiera causar la interrupción de actividades propias de la organización. 2. Pudiera impedir la operación efectiva de una parte de la organización. 3. Pudiera causar una pérdida menor de la confianza dentro de la Organización. 4. Pudiera causar molestias a un individuo. 5. Pudiera causar una merma en la seguridad o dificultar la investigación de un incidente 6. Tiempo de recuperación del servicio está entre uno y cinco días. 7. Información sin clasificar.
2	1. Probablemente cause una pérdida menor de la confianza dentro de la Organización. 2. Pudiera causar retraso a un individuo u organización. 3. Información sin clasificar.
3	1. Probablemente afecte a un individuo. 2. Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente. 3. Causa de pérdidas financieras o merma de ingresos.

	4. Constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros. 5. Probablemente cause la interrupción de actividades propias de la Organización. 6. Probablemente impediría la operación efectiva de una parte de la Organización. 7. Probablemente afecte negativamente a las relaciones internas de la Organización. 8. De cierto valor para la competencia, de cierto valor comercial. 9. Difusión limitada.
4	1. Probablemente afecte a un grupo de individuos. 2. Probablemente cause daños menores a varios individuos. 3. Dificulte la investigación o facilite la comisión de delitos. 4. Tiempo de recuperación del servicio tiene que ser entre 4 horas y un día. 5. Difusión limitada.
5	1. Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones. 2. Probablemente impediría la operación efectiva de más de una parte de la organización. 3. Probablemente sea causa una cierta publicidad negativa. 4. Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local. 5. Información personal: probablemente afecte gravemente a un individuo. 6. Difusión limitada.
6	1. Información personal: probablemente afecte gravemente a un grupo de individuos. 2. Seguridad de las personas: probablemente cause daños de cierta consideración, restringidos a un individuo. 3. Difusión limitada.
7	1. Probablemente cause una interrupción seria de las actividades propias de la Organización. 2. Probablemente impediría la operación efectiva de la organización. 3. Probablemente causaría una publicidad negativa generalizada. 4. Probablemente cause serios daños a misiones importantes de inteligencia o información. 5. Seguridad: probablemente sea causa de un grave incidente de seguridad (ejecución de tareas no deseadas, robo de contraseñas. 6. De alto interés para la competencia, de elevado valor comercial. 7. Cause graves pérdidas económicas. 8. Proporciona ganancias o ventajas desmedidas a individuos u organizaciones. 9. Tiempo de recuperación del servicio tienes que ser menor de 4 horas. 10. Confidencial.
8	1. Impida la investigación de delitos graves o facilite su comisión. 2. Datos clasificados como confidenciales. 3. Confidencial
9	1. Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización. 2. Probablemente impediría seriamente la operación efectiva de la organización, pudiendo llegar a su cierre. 3. Seguridad: probablemente sea causa de un serio incidente de seguridad (Beneficios a algún(os) individuo de la empresa o robo). 4. Probablemente cause un serio impacto en las relaciones con otras empresas y organizaciones, o con entes de regulación. 5. De enorme interés para la competencia, de muy elevado valor comercial.

	6. Cause perdidas económicas excepcionalmente elevadas 7. Reservado.
10	1. Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística 2. Deteriore de forma permanente los datos y la información de la organización. 3. Secreto

Identificación de las amenazas

La identificación de las amenazas consiste en listar y documentar a lo que se exponen los activos, para determinar las medidas pertinentes y poder garantizarles la seguridad. La metodología para la identificación de las amenazas consiste en tomar cada uno de los activos que hacen parte del sistema y determinar a qué amenazas está expuesto dicho activo por medio de entrevistas y reuniones con los funcionarios que tengan relación directa o indirecta con el activo, haciendo uso del catálogo de amenazas proveído por magerit como guía de referencia.

El resultado de este análisis se plasma en la tabla que relaciona los activos y las amenazas con su valoración en el mapa de riesgos. Con respecto al contexto de este proyecto los arboles de ataque solo llegaran hasta donde el ámbito del sistema lo permita, e ignorará los escenarios que estén fuera del sistema o del proceso al que se hace referencia en esta monografía.

Se debe tener en consideración que al realizar la identificación de las amenazas se tiene en cuenta la dimensión más valiosa por la que cada activo es importante en la organización y los tipos de fallas que presentaron en el pasado.

De igual forma se define que por cada amenaza identificada se documentará la descripción del efecto y los antecedentes si los hubiera en la organización. Con respecto a los errores que causan perdidas en la organización, MAGERIT determina una tabla para definir la línea entre los diferentes tipos de errores y la contraparte como ataque, esta es:

Tabla 5. Relación error y ataque.

ERROR	ATAQUE
Error de los usuarios	
Error del administrador	
Errores de monitorización (log)	Manipulación de los registros de actividad
Errores de configuración	Manipulación de la configuración
	Suplantación de la identidad del usuario
	Abuso de privilegios de acceso

Deficiencia en la organización	Uso no previsto
Difusión de software dañino	Difusión de software dañino
Errores de [Re-]encaminamiento	[Re-]encaminamiento de mensajes
Errores de secuencia	Alteración de secuencias
	Acceso no autorizado
	Análisis de trafico
	Repudio
Escapes de información	Interceptación de información (escucha)
Alteración accidental de la información	Modificación deliberada de la información
Destrucción de información	Destrucción de información
Fugas de información	Revelación de información
Vulnerabilidades de los programas	
Errores de mantenimiento	
	Manipulación de programas
Errores de mantenimiento	Manipulación de equipos
Caída del Sistema por agotamiento de recursos	Denegación de servicio
Perdida de equipos	Robo
	Ataque destructivo
	Ocupación enemiga
Indisponibilidad del personal	Indisponibilidad del personal
	Extorción
	Ingeniería social

Para ilustrar mejor, con ayuda de esta tabla, se identifican con mayor facilidad los contextos en donde una falla y un ataque muestran comportamientos parecidos pero que deben ser tratados de forma diferente, aunque tengan la misma consecuencia. Dentro del estándar de codificación de las amenazas se hace referencia a los errores con la letra E al inicio. A continuación se listaran los activos que hacen parte del sistema y las amenazas identificadas a las que dichos activos están expuestos.

Tabla 6. Relación de identificación de las amenazas.

ACTIVOS	AMENAZAS
[d_scode_si] Código Fuente del sistema Integrado	Errores de monitorización Errores de escapes de información Alteración accidental de la información
[d_passw] Credenciales de Acceso	Error de los usuarios Error del administrador Escapes de información Acceso no autorizado

	Divulgación de información Destrucción de información
[d_DB_incrip]Base de datos de inscripciones y matriculas	Errores del administrador Errores de monitorización Alteración accidental de la información Destrucción de Información Manipulación de los registros Modificación deliberada de la información
[d_DB_encuest]Base de datos de encuestas	Errores de los usuarios Errores del administrador Errores de monitorización Alteración accidental de la información Destrucción de información Manipulación de los registros Modificación deliberada de la información
[d_DB_si]Base de datos del sistema integrado	Errores de los usuarios Errores del administrador Errores de monitorización Alteración accidental de la información Destrucción de información Manipulación de los registros Modificación deliberada de la información
[d_drivers]Archivos de configuración y controladores de equipos	Destrucción de información
[d_doc_infrs]Archivos de documentación de infraestructura	Alteración accidental de la información Destrucción de la Información
[d_backup_files]Ficheros de Respaldo y Copias de seguridad	Destrucción de Información Acceso no Autorizado Modificación Deliberada de la Información Alteración accidental de la información
[sw_si]Sistema integrado	Caída del Sistema por agotamiento de recursos Denegación de Servicio Acceso no autorizado Abuso de privilegios de acceso
[sw_siigo]Sistema de gestión contable	Caída del Sistema por agotamiento de recursos Denegación de Servicio Destrucción de Información Divulgación de información Acceso no autorizado Abuso de privilegios de acceso
[sw_school]Sistema de gestión académica	Caída del Sistema por agotamiento de recursos Denegación de Servicio Destrucción de Información

	Divulgación de información Acceso no autorizado Abuso de privilegios de acceso
[sw_so]Sistemas operativos	Uso no previsto Denegación de servicio
[sw_office]Ofimática	Errores de mantenimiento / Actualización de programas Difusión de software dañino
[sw_antivirus]Antivirus	Difusión de software dañino Errores de mantenimiento / Actualización de programas Uso no previsto Acceso no autorizado
[sw_browser]Navegador Web	Difusión de software Dañino Uso no previsto Errores del usuario
[sw_dev]Entorno de Desarrollo	Uso no previsto Alteración de secuencia Acceso no autorizado Errores del Administración
[sw_mang]Aplicaciones de Gestión y Monitoreo	Uso no previsto Alteración de secuencia Acceso no autorizado
[hw_server]Servidor	Fuego Agua Avería Corte suministro eléctrico Humedad Uso no previsto Denegación de servicio Robo Ataque destructivo Error de Mantenimiento Caída del sistema por agotamiento de recursos Acceso no autorizado
[hw_pc_adm]Equipos de informática de uso administrativo	Fuego Avería Humedad Ataque destructivo Robo Error de mantenimiento Manipulación de Equipo Uso no previsto Acceso no autorizado
[hw_pc_edu]Equipos de informática de uso educativo	Fuego Avería Humedad Ataque destructivo Robo

	Error de mantenimiento Manipulación de Equipo Uso no previsto
[hw_vbeam]Proyectores	Humedad Avería Humedad Uso no previsto
[hw_printer]Impresoras	Fuego Avería Robo Ataque destructivo
[hw_firewall]Fortigate	Fuego Agua Robo Error en el mantenimiento Caída del sistema por agotamiento de recursos Error del Administrador Acceso no autorizado
[hw_accespoint]Puntos de acceso	Robo Caída del sistema por agotamiento de recursos Acceso no Autorizado
[hw_sw_route] Switches y routers	Robo Caída del sistema por agotamiento de recursos Acceso no Autorizado Condiciones de temperatura y humedad Corte de suministro eléctrico Avería
[com_pstn]Red telefónica	Fallo del servicio de comunicaciones Uso no previsto
[com_radio]Red Inalambrica	Fallo del servicio de comunicaciones Errores del Administrador Caída del sistema por agotamiento de recursos Abuso de privilegios Acceso no autorizado Divulgación de la información
[com_lan]Red Local	Fallo del servicio de comunicaciones Errores del Administrador Caída del sistema por agotamiento de recursos Abuso de privilegios Acceso no autorizado Divulgación de la información Denegación de servicio
[com_internet]Internet	Fallo servicio de comunicaciones Uso no previsto Denegación de servicio

[media_net]Almacenamiento en red	Denegación de servicio Fallo servicio de comunicaciones Uso no previsto Fallo del servicio de comunicaciones Errores del Administrador Caída del sistema por agotamiento de recursos
[media_hd_ext]Disco externo de respaldo	Fuego Destrucción de información Perdida de Equipo Acceso no Autorizado Destrucción de información Robo
[aux_ups]Sistemas de alimentación ininterrumpida	Agua Fuego Error en el mantenimiento Falla de suministro eléctrico Daño en el equipo
[aux_furnit]Gabinetes y mobiliario	Ataque destructivo Falla en el mantenimiento Fuego Avería Agua Uso no previsto

Caracterización y valoración de las amenazas

Consiste en tomar la lista de las amenazas identificadas previamente y asignarles un código de identificación. En la valoración de las amenazas se evalúa cada dimensión del activo expuesto y se le asigna un valor teniendo en cuanta los índices de la tabla 6 y la degradación que causaría la amenaza si llegara a materializarse. De igual manera se estima la probabilidad de ocurrencia dicha amenaza usando un sistema de valor cualitativo establecido en la tabla 7.

Tabla 7. Degradación del valor del activo.

MA	MUY ALTA	10
A	ALTA	8-9
M	MEDIA	5-7
B	BAJA	3-4
MB	MUY BAJA	1-2

Tabla 8. Probabilidad de ocurrencia de la amenaza.

CS	CASI SEGURO
MA	MUY ALTO
P	POSIBLE
PP	POCO PROBABLE
MB	MUY BAJO
0	

Caracterización de las salvaguardas

Una vez identificadas todas las amenazas potenciales del sistema se continúa con la identificación de las salvaguardas, que se trata de la selección de mecanismos, técnicas, políticas y procedimientos que ayuden a la protección del activo en una eventual materialización de la amenaza.

Existen distintos tipos de protecciones los cuales se pueden agrupar en 3 categorías de acuerdo a su efecto: las preventivas, las que acotan la degradación y las que consolidan los efectos de otras, tal como se evidencia en la siguiente tabla.

Tabla 9. Tipos de protección

EFECTO	TIPO
Preventivas: Reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
Acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
Consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [SW] de concienciación [AD] administrativas

Llegado a este punto, la caracterización de las amenazas puede determinar las medidas a implementar para garantizar la seguridad de los activos dentro del sistema. Sin embargo a estas

medidas se le debe establecer el nivel de eficacia dentro del sistema, y signarle una valoración a la salvaguarda.

Para determinar la eficacia de una salvaguarda se debe evaluar tanto desde el punto de vista técnico, si esta es suficiente para proteger el activo, como desde el punto de vista operacional, si es bien implementada en la institución, si tiene mecanismos bien definidos, si tiene usuarios capacitados para su despliegue, entre otros.

Para la estimación de este valor MAGERIT sugiere medir su eficacia y madurez de la siguiente manera:

Tabla 10. Medición de Salvaguardas

Factor	Nivel	Significado
0%	L0	Inexistente
	L1	Inicial / ad hoc
	L2	Reproducible, pero intuitivo
	L3	Proceso definido
	L4	Gestionado y medible
100%	L5	optimizado

Estimación del impacto

Una vez caracterizados los activos, las amenazas y las salvaguardas se continúa con la estimación del impacto potencial y residual del sistema. El impacto potencial consiste en estimar el nivel al que está expuesto el sistema teniendo en cuenta el valor de los activos y la degradación causada por la amenazas pero despreciando la eficacia de las salvaguardas, teniendo una estimación de lo que podría suceder en una posible materialización de la amenaza.

El impacto potencial se estima basado en la valoración de los activos plasmados en el Modelo de Valor y el valor de las amenazas plasmado en el mapa de riesgos, el método de valoración se basa en un análisis de tablas, cruzando los valores del activo y la degradación de las amenazas teniendo como resultado un mapa del impacto potencial. Como se puede deducir el

impacto potencial se calcula por cada amenaza sobre cada activo y se registrara en el informe de Estado de Riesgos, a continuación se observa la tabla de estimación del impacto:

Tabla 11. Estimación del Impacto

IMPACTO		VALOR DEL ACTIVO				
		MB	B	M	A	Extremo
DEGRADACION	MA	B	M	A	MA	MA
	A	B	M	A	A	MA
	M	B	B	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Tabla 12. Valorización del impacto

INDICE	VALOR
MA	10
A	8-9
M	5-7
B	3-4
MB	1-2

Después de realizado el análisis del impacto potencial, se continúa con el análisis del impacto residual, que consiste en efectuar el mismo estudio que el impacto potencial pero teniendo en cuenta las salvaguardas implementadas o las salvaguardas proyectadas. Al realizar el análisis del impacto residual se debe tener en consideración que las salvaguardas poseen dos escenarios de estudio: el estado actual del sistema y el estado aceptable de implementación de las salvaguardas. Cada una de ellas posee un nivel diferente de valoración.

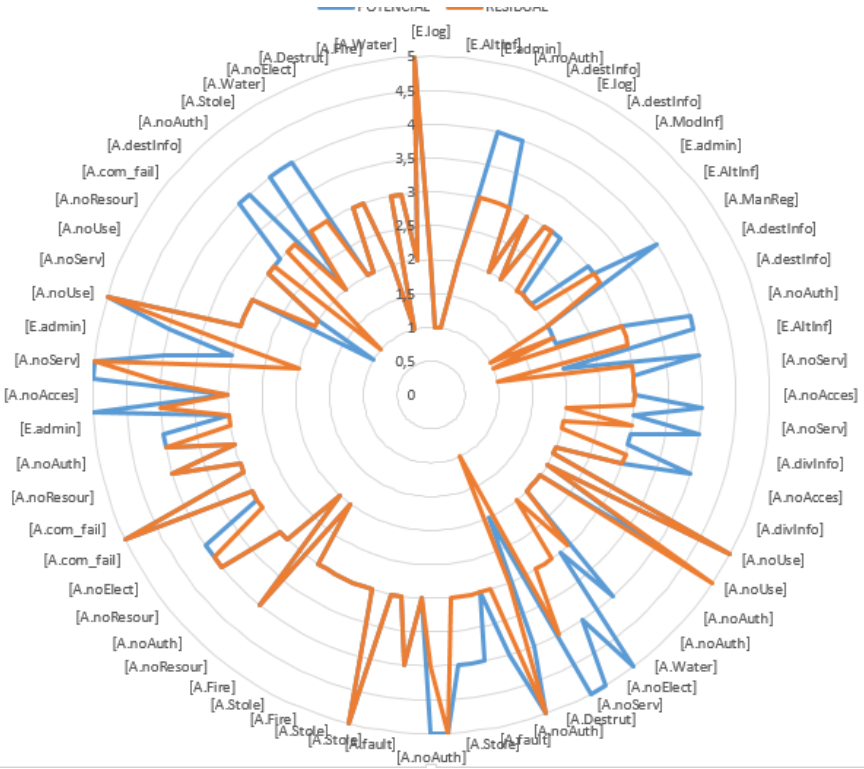
Estimación del Riesgo

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es consecuente estimar el riesgo haciendo uso de la probabilidad de ocurrencia. El riesgo crece de manera proporcional al valor del impacto y a la probabilidad de ocurrencia, por lo que estas dos variables permiten generar un mapa de valor para observar con mayor claridad el comportamiento del riesgo.

De manera similar a la estimación del impacto, el riesgo posee 3 estados de acción que son: el riesgo potencial, cuando se hace el análisis ignorando las salvaguardas implementadas o proyectadas a implementar; el riesgo residual con la eficiencia de las salvaguardas implementadas actualmente y el riesgo residual con la eficiencia de las salvaguardas proyectadas a implementar con el desarrollo del sistema de gestión.

Como consecuencia del análisis realizado en la estimación del impacto y del riesgo, nace el 'Estado de Riesgos', que no es más que un expediente donde reposa toda la documentación de esta actividad y que básicamente debe estar constituido por registros de los valores del impacto potencial, el impacto residual, el riesgo potencial y el riesgo residual por cada dimensión de cada activo dentro del sistema, el análisis de esos registros es el objetivo principal del análisis de riegos. A continuación se muestra una gráfica con el resumen del resultado del análisis de riesgos.

Figura 5. Grafica de estimación del riesgo del proceso de gestión



En la gráfica se observan todas las amenazas con sus diferentes valores de afectación en los distintos activos del sistema. Se pueden ver dos series de colores diferentes, azul y naranja, para describir los dos estados del análisis de riesgos: potencial y residual respectivamente.

A primera vista se observa la diferencia en los rangos de las dos series, el azul en la mayoría de los puntos presenta niveles superiores, pero nunca está por debajo de la serie naranja. Con esta representación podemos determinar las amenazas que por medio de las salvaguardas y medidas de protección fueron controladas por ejemplo: Los errores de destrucción de la información, fallas causadas por agua o fuego, o la alteración de la información, fueron controlados a niveles de riesgo bajo y muy bajo cuando en el impacto potencial tenían valores medios y altos.

De la misma manera se pueden identificar con facilidad las amenazas en donde la implementación de las salvaguardas no fueron suficientes, esto se visualiza en la gráfica en los puntos donde existen picos de la serie naranja. En la gráfica se identifica que las amenazas de errores por el uso, falla de red o fallas por la autenticación, aun presentan niveles inaceptables de riesgos.

Con estos resultados se puede diseñar una capa de protección para fortalecer las amenazas que muestran niveles inaceptables de riesgos; es responsabilidad del analista y de la organización determinar las medidas que se van a tomar, pues de acuerdo al contexto se puede fortalecer las salvaguardas ya implementadas o simplemente documentar de manera más precisa para determinar su comportamiento.

Capitulo IV
Gestión de riesgos y Políticas de Seguridad

Siento en efecto, la necesidad de recordar que el análisis de riesgos se concentra en determinar impactos y riesgos, los impactos recogen daños absolutos sin tomar en cuenta la probabilidad de su ocurrencia, mientras que el riesgo no solo toma en cuenta el impacto sino la probabilidad de que ocurra. *"El impacto refleja el daño posible (lo peor que puede ocurrir), mientras que el riesgo refleja el daño probable (lo que probablemente ocurra)." (Gobierno de España, 2012).*

Entonces una vez realizado el análisis de riesgos, se define e implementan las acciones pertinentes frente al resultado de este análisis. La gestión de riesgos la podemos definir de acuerdo a la ISO 31000, como las "*Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.*".

Comprendemos una vez más, que la gestión de riesgos está compuesta por todo el esfuerzo realizado por la organización para el tratamiento de los riesgos, teniendo en cuenta mecanismos, políticas, procesos, procedimientos y tecnologías implementadas.

Los resultados del análisis de riesgo permiten prestar mayor atención a los activos que necesitan un tratamiento especial dentro del sistema, es decir los activos que aun con las salvaguardas implementadas poseen niveles de riesgos muy altos se deben gestionar de manera correcta para asegurar que no afecten el funcionamiento de la organización.

En primera instancia, se identifican los niveles de riesgo aceptables para la organización, para establecer los rangos de acción y determinar el tratamiento que se le ha de dar. Una vez se identifiquen los niveles de riesgos de los activos, se procede a establecer las acciones por cada nivel identificado. Teniendo en cuenta las salvaguardas implementadas, se hace una descripción de las medidas a tomar para enfrentar el nivel del riesgo. Con respecto a esta apreciación se considera que:

1. Un riesgo es **crítico** en el sentido de que requiere atención urgente.

2. Un riesgo es **grave** en el sentido de que requiere atención.

3. Un riesgo es **apreciable** en el sentido de que pueda ser objeto de estudio para su tratamiento.

4. Un riesgo es **asumible** en el sentido de que no se van a tomar acciones para atajarlo.

A continuación se presenta la relación entre el valor de la estimación y la calificación del riesgo:

Tabla 13. Calificación del Riesgo

VALOR DE LA ESTIMACIÓN	CALIFICACIÓN DEL RIESGO
Muy Alto	Critico
Alto	Grave
Media	Apreciable
Bajo	Asumible
Muy Bajo	Asumible

Hay que tener claridad del sistema y del contexto de la organización para tomar la decisión de asumir o no un riesgo, pues aunque los niveles de estimación sean bajos o muy bajos, la afectación puede llegar a ser más grande de lo que se estima. Como también se debe comprender que un riesgo con una estimación crítica no requiere necesariamente protección de último nivel en tecnología, sino un refuerzo en la implementación y la coordinación del personal para cambiar su nivel de afectación.

Por otra parte, hay que decir, que la gestión de los riesgos depende de características directamente relacionadas con la organización tales como: Las leyes a la que está sometida la organización, los tipos de contratación que se manejan, la estructura organizacional, la relación de los clientes externos e internos, las políticas internas o la imagen pública, entre otros. Aunque la mayoría del análisis está basado en estudios técnicos, muchas de sus decisiones son de carácter político o gerencial.

En este contexto, sorprende la necesariedad de los métodos para el tratamiento y gestión de riesgos, si se tiene en cuenta que las opciones de tratamiento de riesgos son:

La **Eliminación**, que consiste en la supresión de la causa del riesgo que no es aceptable sin afectar la esencia de la organización. No se puede prescindir de la información o de los activos esenciales de una organización sin causar un enorme impacto a la misión y definición de la misma, sin embargo es viable pensar que se puede prescindir de métodos y componentes no esenciales que ponen en riesgo el sistema. La utilización de esta opción requiere un nuevo análisis de riesgos sobre el sistema modificado.

La **Mitigación** es otra opción de tratamiento de riesgo y hace referencia a reducir la degradación causada por una amenaza o reducir la probabilidad de que una amenaza se materialice. Esto se obtiene en la ampliación y mejora de las salvaguardas, tanto en niveles técnicos como en niveles de madurez, muchas veces se implementan estas mejoras del sistema con el ingreso de nuevas tecnologías que a su vez aumentan el inventario de activos generando la necesidad de un nuevo análisis.

La **Compartición** como método de tratamiento de riesgo, consiste en que se comparte por medio de la externalización de componentes del sistema, de forma que se reparten responsabilidades: unas técnicas para el que opera el componente técnico; y otras legales. La compartición también se conoce como 'transferir el riesgo' y se puede realizar de manera parcial o total, es más general hablar de compartir el riesgo.

Por ultimo esta la **Financiación,** cuando se acepta un riesgo, la Organización hará bien en reservar fondos para el caso de que el riesgo se concrete y haya que responder de sus consecuencias. A veces se habla de 'fondos de contingencia' y también puede ser parte de los contratos de aseguramiento. Normalmente esta opción no modifica nada del sistema y mantiene el análisis de riesgos disponible.

A continuación se listaran las amenazas que presentan riesgos graves y críticos, y se hará una descripción del tipo de tratamiento que se debe implementar para reducir el nivel del riesgo:

Riesgos en estado Crítico o Grave

Uso no previsto: Esta amenaza fue encontrada de manera recurrente en el análisis, afectando a muchos de los activos informáticos, tiene una alta probabilidad de ocurrencia. Aunque los activos no fuesen de gran valor para el sistema, la alta probabilidad de que esta amenaza ocurriera determina que los activos se encuentran en un alto nivel de riesgo. Los activos que esta amenaza puede afectar y que muestran un alto riesgo para la organización son: El sistema operativo, el navegador web, los computadores administrativos, los computadores educativos y el internet.

Aunque esta amenaza se encuentra controlada con varias salvaguardas, es claro que se deben implementar mejoras en el sistema para garantizar un riesgo menor, en este caso se mitiga la probabilidad de ocurrencia con recomendaciones y políticas de seguridad:

- Hacer uso de una versión licenciada de Windows profesional, preferiblemente las más recientes y hacer uso de la administración de privilegios que estas ofrecen para acotar los accesos de las cuentas de estudiantes, docentes e invitados.
- Crear puntos de recuperación del sistema para proteger la configuración de los equipos y la integridad del sistema operativo.
- Crear un manual de uso de los equipos de cómputo para los integrantes de la comunidad y realizar su respectiva socialización.
- Establecer cuentas de acceso usando la administración de los directorios activos de Windows server. (Esta solución solo aplica para las oficinas administrativas).
- Programar capacitaciones para fortalecer el buen uso de las tecnologías, incluyendo los sistemas operativos, servicios web y ofimática.
- Fomentar el uso ambientes digitales por medio de la comunicación y la motivación.
- Utilizar bloqueos de publicidad en los navegadores para evitar la probabilidad de que caigan en la técnica de suplantación de identidad '*Phishing'*.
- Implementar políticas de bloqueo en el firewall de la red para fortalecer el buen uso del internet, realizar constantes monitorios a los bloqueos más comunes del sistema.
- Definir un procedimiento para el seguimiento de las fallas más comunes por mal uso que se estén llevando a cabo.

Caída del sistema por agotamiento de recursos: Esta amenaza afecta a varios de los activos del sistema, algunos de ellos, presentan un alto riesgo a la exposición de esta amenaza: El servidor, El Firewall y Accespoints. Se evidencia una relación entre los activos y esta amenaza: su función y necesidad en la red local. Cada uno de estos componentes responde a servicios de red de carácter esencial por lo que si sus recursos no son bien protegidos pueden causar un desborde de memoria en sus sistemas y una falla en su disponibilidad.

A diferencia del uso no previsto, el agotamiento de recursos no es muy probable, sin embargo afecta de manera crítica la disponibilidad de estos activos, los cuales poseen un alto valor para las funciones de la organización. Creando así, un punto de riesgo critico en el sistema. A continuación se presentan las medidas de seguridad para mitigar el impacto y su probabilidad de ocurrencia:

- Implementar alertas de seguridad en el servidor en caso de que los recursos estén llegando a grandes niveles de uso.
- Definir puntos de control tanto en el servidor como en los accespoint para el servicio DHCP, dependiendo del tipo de uso que se le da por dispositivo.
- Definir un procedimiento de monitoreo a los niveles de los recursos de los activos que sean pertinentes.
- Establecer un pool de direcciones estáticas a los dispositivos de alta prioridad en la red.
- Establecer sistemas de recuperación y respaldo en caso de fallas.

Denegación de Servicio: La denegación de servicios al igual que la caída por agotamiento de recursos afecta la disponibilidad de algunos dispositivos de red, en este caso el riesgo critico afecta al servidor y al servicio de red local; a la que hay que implementar medidas tales como:

- Políticas de acceso en cada uno de los dispositivos dentro de la red local y establecer privilegios de acuerdo al nivel.
- Asegurar que las contraseñas de la administración de sistemas tengan un alto nivel de protección
- Implementar un sistema de monitoreo sobre los accesos no autorizados.

- Usar técnicas de encriptación en las contraseñas de administración.

Acceso no autorizado: El acceso no autorizado es una amenaza que puede afectar a un gran número de activos en la organización. Los activos con un riesgo grave causado por esta amenaza son: Los puntos de acceso, computadores de uso administrativo y la red local. A diferencia de las otras amenazas en un alto riesgo, el acceso no autorizado tiene comportamientos muy diferentes dependiendo del activo.

La razón por la que los puntos de acceso tienen un nivel de riesgo grave se debe a que su configuración esta sobre el mismo dispositivo con la respuesta de una página web que responde a la dirección IP asignada, creando así un punto de vulnerabilidad a la red. De igual manera su ubicación en la institución es amplia y desprotegida en la mayoría de los casos por lo que físicamente también pueden ser accedidos con relativa facilidad.

Los equipos de uso administrativos también poseen un alto nivel de riesgo debido al tipo de información que en ellos reposa, dándoles un alto nivel en la integridad y disponibilidad del activo, creando así un margen de seguridad grande que en la actual condición de la organización no se cumple, por el bajo conocimiento que se tiene de las herramientas tecnológicas por parte de los funcionarios administrativos.

Por último la red local posee igualmente una afectación en la integridad y disponibilidad por parte de esta amenaza creando un alto estado de riesgo, debido a la infraestructura que este servicio soporta, pudiendo darles acceso a usuarios no deseados dentro de la red. A continuación se describe las políticas y medidas a tomar para mitigar este riesgo:

- Creación de contraseñas en cada uno de los dispositivos instalados.
- Ubicar los dispositivos de red en zonas elevadas de las habitaciones.
- Para proteger la red hay que desactivar los puertos de red que no estén siendo utilizados por ningún dispositivo.
- Se deben activar opciones de registro de logs para verificar si hubo un acceso no autorizado.
- Se debe diseñar un procedimiento para hacerle seguimiento a este riesgo en específico.
- Establecer un manual de buenas prácticas para la seguridad informática.

- Realizar capacitaciones y socialización del manual para fortalecer la cultura de la seguridad de la información.
- Configurar bloqueos de pantalla automáticos en los equipos administrativos.

Está claro que las amenazas relacionadas con la interacción de los usuarios y el ambiente laboral son las más comunes. Es por ello, que la organización debe prestar especial atención a la promoción y capacitación del uso de equipos informáticos.

Sin embargo de manera general el sistema presenta niveles de estimación muy controlados de los cuales se necesita aun estudiar de manera más detallada su comportamiento para saber qué tan determinante seria su gestión. La creación de procedimientos de medición permitirá estudiar esas amenazas a las que se calificó como apreciables dentro del sistema permitiendo en una siguiente iteración del ciclo entender mejor su afectación y determinar de manera más efectiva su tratamiento.

Capítulo V
Mejora continua y seguimiento del sistema

En esta etapa del proyecto se busca estudiar la efectividad del sistema y establecer una base para la mejora y evolución del mismo, esto se conoce como la mejora continua. Como se estableció en el primer capítulo, un SGSI es implementado con ayuda del ciclo PHVA en donde los primeros tres capítulos de esta monografía establecen la planificación e implementación del sistema los cuales corresponden al Planear y el Hacer del ciclo. Ahora en este capítulo se busca definir los indicadores para el seguimiento y las acciones de mejora que dentro del ciclo PHVA corresponden a verificar y el actuar.

La verificación consiste en crear indicadores de desempeño en donde se pueda evaluar el desarrollo de las actividades del sistema. La ISO 27001 define esta etapa del ciclo en el capítulo 9 titulado 'EVALUACION DEL DESEMPEÑO' y define que: *la organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión.* Se debe entender que la evaluación del desempeño no solo conlleva a evaluar la efectividad de las medidas de seguridad, sino a la forma en que el sistema en general está afectando la seguridad de la información en la organización.

En primer lugar se deben definir los métodos de seguimiento, medición y análisis que se establecerán sobre el sistema y la forma en que van a ser documentados. Dentro de esta etapa se deben definir de manera clara estos procedimientos entrando en detalle sobre cómo se va a implementar tanto la medición como el análisis. Los indicadores de desempeño están directamente relacionados con el comportamiento de las amenazas siendo claro que la reducción de su ocurrencia o la disminución de su impacto es el objetivo principal del sistema.

Los métodos de seguimiento consisten en documentar las actividades para hacerle revisión a su ejecución y así determinar el análisis de la eficacia del sistema, estos registros normalmente hacen parte de otros procedimientos pero generan fuentes de información para el cálculo de un indicador del desempeño. En el manual de procedimientos se entra en detalle de las actividades del sistema sin embargo no todos los procedimientos generan indicadores aun si es registrada la actividad.

Como se mencionó en el capítulo 2 el colegio Salesiano san Pedro Claver no es ajeno a los procesos de calidad, pues posee una certificación actualizada de la ISO 9001:2015 y la totalidad de sus procesos misionales están definidos y estructurados bajo esta norma. Entonces haciendo uso del formato ya establecido para el seguimiento del desempeño de su sistema integrado, se implementan los indicadores de desempeño del SGSI que cubre esta monografía y se describe en el manual de procedimientos y formatos.

En el capítulo anterior de gestión de riesgos se definió que existen diferentes métodos para el tratamiento de los riesgos, el más común fue el de mitigarlos, sin embargo esto se debe a que se estaban tratando solos los riesgos de calificación grave o crítico, pero la mayor parte de los riesgos fueron calificados como apreciables, y de los cuales se decidió estudiarlos más a fondo y hacerles un seguimiento a su comportamiento. Esto se implementa en la creación de los indicadores de desempeño de las amenazas que lo requieran.

"Los indicadores de desempeño son instrumentos que proporcionan información cuantitativa sobre el desenvolvimiento y logros de una institución, programa, actividad o proyecto en el marco de sus objetivos" (Ministerio de Economía y Finanzas, 2010). La creación de indicadores de desempeño permiten hacerle seguimiento de manera clara los logros de los objetivos, nos permite mejorar la gestión de las actividades y detectar el comportamiento no deseado dentro de un sistema. Usando los datos recolectados por los procedimientos, podemos crear fuentes de conocimiento y puntos de decisión sobre el desarrollo del SGSI.

Existen atributos de interés que se deben definir para cada indicador, tales como:

Formula: Es la lógica que precisa el modo de definir el valor del indicador.

Fuente de Información: Es el documento del cual se toman los valores de las variables para el cálculo de la formula.

Meta: Es el resultado que se busca obtener en el indicador.

Nivel de Aceptación: Es el último valor aceptable del indicador, todo valor fuera del rango del nivel de aceptación y la meta, es un nivel no aceptable que genera una no conformidad de la cual se deben tomar acciones de mejora.

Frecuencia de la revisión: Periodo de tiempo en el cual se calculara el indicador en el transcurso del año.

Persona a Cargo: Son los funcionarios encargados de realizar el cálculo y el análisis del indicador y de establecer las acciones de mejora que se tomaran en caso de ser necesario.

Procedimiento: Es el procedimiento que se afecta directamente por el indicador y el cual se evalúa directamente en su ejecución.

Formatos: Son los formatos que se utilizan para verificar las acciones tomadas para este indicador. A continuación se presentan los indicadores implementados para este sistema:

Indicadores de desempeño:

Nivel de cumplimientos del plan de mantenimiento de sistemas

FORMULA	Número de actividades realizadas a la fecha sobre el número de actividades programadas por 100.
FUENTE DE INFORMACION	Plan de mantenimientos
META	100%
NIVEL DE ACEPTACION	95%
FRECUENCIA DE REVISION	Mensual
PERSONA A CARGO	Ecónomo/ Administrador de Sistemas
PROCEDIMIENTO	Mantenimiento preventivo de equipos.
FORMATOS	Fichas técnicas de equipos Reportes de Mantenimiento

Ejecución de correcciones generales del sistema

FORMULA	Número de solicitudes realizadas a la fecha sobre el número de solicitudes por 100.
FUENTE DE INFORMACION	Reporte de Fallas
META	90%
NIVEL DE ACEPTACION	75%
FRECUENCIA DE REVISION	Trimestral
PERSONA A CARGO	Ecónomo/ Administrador de Sistemas
PROCEDIMIENTO	Mantenimiento preventivo de equipos.
FORMATOS	Fichas técnicas de equipos Reportes de Mantenimiento

Nivel de disponibilidad de la red

FORMULA	Si la Falla demora más de 1hora se cuenta como un día de no disponibilidad. Número de días no disponibles Sobre 30 por 100
FUENTE DE INFORMACION	Reporte de Fallas
META	90%
NIVEL DE ACEPTACION	80%
FRECUENCIA DE REVISION	Mensual
PERSONA A CARGO	Ecónomo/ Administrador de Sistemas
PROCEDIMIENTO	Monitoreo del funcionamiento de la infraestructura. Mantenimiento correctivo
FORMATOS	Reportes de Mantenimiento

Reportes de reparación de sistemas operativos y aplicaciones.

FORMULA	Número de fallas reportadas que tengan como causa componentes del sistema operativo.
FUENTE DE INFORMACION	Reporte de Fallas
META	5
NIVEL DE ACEPTACION	10
FRECUENCIA DE REVISION	Semestral
PERSONA A CARGO	Administrador de Sistemas
PROCEDIMIENTO	Mantenimiento correctivo
FORMATOS	Reportes de Mantenimiento

Numero de violaciones de acceso reportadas

FORMULA	Número de fallas reportadas que tengan como causa una violación de acceso
FUENTE DE INFORMACION	Reporte de Fallas y Reportes de mantenimiento
META	0
NIVEL DE ACEPTACION	1
FRECUENCIA DE REVISION	Semestral
PERSONA A CARGO	Ecónomo/ Administrador de Sistemas
PROCEDIMIENTO	Monitoreo del funcionamiento de la infraestructura. Mantenimiento correctivo
FORMATOS	Reportes de Mantenimiento

Nivel de velocidad de red

FORMULA	Velocidad de red contratada menos Velocidad de red medida.
FUENTE DE INFORMACION	Formato de Mantenimientos
META	0Mbps
NIVEL DE ACEPTACION	2MBps
FRECUENCIA DE REVISION	Mensual
PERSONA A CARGO	Ecónomo/ Administrador de Sistemas
PROCEDIMIENTO	Monitoreo del funcionamiento de la infraestructura.
FORMATOS	Reportes de Mantenimiento

Los indicadores de seguimiento poseen un formato individual, llamado *Ficha técnica del Indicador*, en donde se registran los valores obtenidos en el desarrollo de la actividad. La ficha posee 3 partes principales: Registro, descripción y análisis y acción de mejora. En el registro se hace la anotación de los datos encontrados en el periodo definido por la frecuencia. En la descripción y análisis se hace una breve descripción de lo que se encontró en el procedimiento y realizando un análisis de las posibles causas, observaciones e irregularidades. Por último la acción de mejora o correctivas es donde se establece las acciones que evitaran que se repita una situación no controlada y como debería implementarse.

Las acciones de mejora son las acciones que se toman para mejorar la eficacia, eficiencia y efectividad de los procesos, mientras que las acciones correctivas son tomadas para eliminar las causas de una No Conformidad detectada u otra situación indeseable (Superintendencia de sociedades, 2015). El registrar estas acciones en la ficha técnica de indicadores, permite establecer un compromiso por parte de la persona a cargo y la organización para enfrentar la situación y evitar que se repita en otra ocasión.

La norma ISO 27001 habla sobre la mejora en el capítulo *10. MEJORA* y describe la necesidad de las organizaciones de hacer seguimiento a las no conformidades por medio de acciones correctivas, las cuales deben ser documentadas y monitoreadas. También establece como requisito que las organizaciones deben mantener el compromiso en la mejora continua de la adecuación y eficacia del sistema de gestión de la seguridad de la información, por lo que estos

hallazgos no se deben quedar por ningún motivo en el documento, sino que deben ser reflejados en la implementación del sistema lo antes posible.

Resultados y recomendaciones

Como resultado de este proyecto de investigación se establece que el Colegio Salesiano San Pedro Claver en su proceso de gestión de la infraestructura tecnológica, posee varias necesidades que debe resolver antes de garantizar la seguridad de su información. Principalmente se puede observar que la falta de cultura en el uso de la tecnología desencadena una serie de riesgos con altos valores de estimación. La mayoría de estos, se pueden controlar por medio de re-inducciones y en la promoción de capacitación continua.

En un segundo momento nos encontramos con que posee una alta dependencia al uso de las TIC por lo que necesita garantizar niveles de disponibilidad bastante altos, los cuales en la actualidad no se ven reflejados en sus políticas ni tecnologías implementadas. Esto genera una oportunidad de mejora bastante importante en la cual se sugieren medidas de protección, mejora de la infraestructura y desarrollo de mejores políticas de usabilidad.

De manera positiva la institución sorprende al demostrar la buena relación que tiene con los sistemas de gestión de calidad y los SGSI, pues a nivel organizacional la estructura fuertemente documentada de un SGC facilita el control de versión de documentos y genera de manera positiva una armonía en la implementación del SGSI. La definición de los procesos y procedimientos permite entender con claridad el alcance y el comportamiento del sistema.

Es importante destacar que en el desarrollo de esta monografía se realizó la evaluación y el análisis de riesgos basados en metodologías enfocadas al área de las TIC, pues la investigación de estas áreas están ligadas a la administración de recursos corporativos y a los sistemas de gestión.

En tercera instancia, debemos recordar que el desarrollo de un SGSI es un trabajo en conjunto que se despliega de acuerdo a los esfuerzos de cada uno de los integrantes de la organización, es por ello que han de estar en sincronía cada una de las partes en la socialización de las nuevas actividades. La motivación con que se realice el seguimiento del sistema permitirá obtener datos representativos en el comportamiento del mismo.

Conclusiones

1. Teniendo como antecedente la poca claridad sobre lo que constituía el proceso de gestión de la infraestructura tecnológica en el Colegio San Pedro Claver, se estableció organización documental del proceso y los activos involucrados en el análisis de riesgos, además en el desarrollo de este ejercicio se establecen responsabilidades que responden a los requerimientos de los activos de la organización.

2. Con respecto al análisis de riesgo, se identificaron las amenazas del proceso, poniendo especial atención a las que son reiterativas de manera transversal en el proceso y a la organización. Se pueden enunciar el manejo del personal y el uso de la tecnología en la institución, con factores generadores como el uso no previsto, caída del sistema por agotamiento de recursos, denegación de servicio y el acceso no autorizado.

3. Teniendo en consideración las amenazas con mayor grado de riesgo ya sea por su probabilidad de ocurrencia o por su nivel de impacto a la organización, se estableció un plan para el tratamiento y la gestión de riesgos para la protección de la infraestructura y establecer mecanismos de detección y alertas que permitan mitigar sus efectos en la organización. Es preciso mencionar que la mayor parte de los riesgos encontrados fueron calificados como apreciables que requieren un constante seguimiento comportamental, generando a su vez la adopción de procesos de mejora continua y seguimiento.

4. Se implementan documentos, formatos y registros que necesita la organización para aumentar los niveles de seguridad de la información institucional, se establecieron ciertos indicadores de desempeño que se configuran en el ciclo laboral de quienes hacen parte de la gestión documental en la institución, fundamentados en la flexibilidad de la normal 27001.

El resultado de este trabajo investigativo no pretende tener la última consideración en esta temática, antes bien, se convierte en punto de partida para futuras investigaciones y se expone con claridad a críticas y aportes significativos de quien considere estudiarle o tomarle como referencia, así pues, se concluye que en el Colegio Salesiano San Pedro Claver se podrían implementar las

mejoras sugeridas para garantizar la seguridad de la información dentro de su proceso de gestión de infraestructura tecnológica, especialmente en el área de gestión administrativa, pues se hizo evidente la deficiente relación del recurso humano del área con el uso de la tecnología.

La consideración final que destaca la importancia de este trabajo investigativo en la organización en mención, se enmarca en la misma necesidad común empresarial de manejo adecuado de la información y por ende de su protección, puesto que de ello depende en gran medida el éxito de la proyección y consolidación empresarial. Se permite para lograrlo, identificar las debilidades actuales dentro del proceso de 'gestión de la infraestructura tecnológica' y determina la manera en que este debe ser alineado con la norma para asegurar que se cumplan los requisitos de la misma, por último, es importante en cuanto presenta un análisis del sistema de gestión de la seguridad de la información que determina el compromiso de la organización para asumir la implementación del mismo de acuerdo a la norma ISO 27001 y el uso de la metodología MAGERIT en el análisis y tratamiento de riesgos.

Una vez tratado el tema del análisis y la gestión de riesgo, es posible ampliar el espectro y observar interesantes oportunidades para desarrollar proyectos que innoven la actividad de la seguridad de la información. Una posible perspectiva seria realizar un estudio con carácter tecnológico en donde se puedan establecer sensores automatizados que registren la actividad de la organización y basados en análisis de patrones y comportamientos se determine si se presenta una situación de riesgo y se genere una alerta en tiempo real. Actualmente existen sistemas que permiten hacerle seguimiento a las metas establecidas para el SGSI pero que requiere que los usuarios ingresen los datos con que se alimenta la información, por lo que desarrollar un sistema que de manera automatizada este capturando estos datos y que al mismo tiempo se pueda establecer un componente de alertas tempranas, representaría una oportunidad competitiva para cualquier organización.

Referencias

Abu Talib, M., Khelifi, A., & Ugurlu, T. (2012). Using ISO 27001 in Teaching Information Security. *Institute of Electrical and Electronics Engineers*, 3149-3153.

Bastidas Paruma, H., Lopez Ortiz, I., & Peña Hidalgo, H. (2014). *ANÁLISIS DE RIESGOS Y RECOMEDACIONES DE SEGURIDAD DE LA INFORMACIÓN AL AREA DE INFORMACIÓN Y TECNOLOGÍA DEL HOSPITAL SUSANA LÓPEZ DE VALENCIA DE LA CIUDAD DE POPAYÁN (Tesis de Grado).* Universidad Nacional Abierta y a Distancia, Popayan. Recuperado el 7 de Agosto de 2017, de http://repository.unad.edu.co/handle/10596/2668

Beckers, K., Fabender, S., Heisel, M., & Schmidt, H. (2012). Using Security Requirements Engineering Approaches to Support ISO 27001 Information Security Management Systems Development and Documentation. *2012 Seventh International Conference on Availability, Reliability and Security; IEEE*, 242-248.

Bocanegra Quintero, Y., & Barajas, F. (2015). *ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDIA MUNICIPAL DE TULUÁ APLICANDO LA METODOLOGÍA MAGERIT (Tesis).* Universidad nacional abierta y a distancia , Valle dle Cauca, Tulua. Recuperado el 12 de Julio de 2018, de https://core.ac.uk/download/pdf/47279703.pdf

Diaz Ricardo, L. C. (2017). *DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA IPS ASSALUD DE COROZAL SUCRE, MEDIANTE LA IMPLEMENTACIÓN DE LA METODOLOGÍA MAGERIT (V3.0) Y LA NORMA ISO 27001:2013.* Sucre, Corozal. Recuperado el 30 de Julio de 2018, de https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/14386/5/1066172091.pdf

Garcia Vasquez, K., & Bojorque, R. (2013). *Aplicacion de la metodologia MAGERIT para el analisis y gestion de riesgos de la seguridad de la informacion aplicado a la empresa pesquera e industrial bravito S.A. en la ciudad de Machala (Tesis de Grado).* Universidad politecnica Salesiana, Cuenca. Recuperado el 20 de Agosto de 2017, de https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf

Gobierno de España. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid, España: Ministerio de Hacienda y Administraciones Públicas.

Gobierno de España. (13 de Octubre de 2017). *Portal de Administracion electronica* . Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Ws-LU4jwbIV

Goeke, L., Alebrahim, A., & Hatebur, D. (2014). Pattern-Based and ISO 27001 Compliant Risk Analysis for Cloud Systems. *Evolving Security and Privacy Requirements Engineering (ESPRE), 2014 IEEE 1st Workshop*, 42-47.

Gonzalez Breña, Julio. (2008). *Analisis de riesgos en la agencia estatal de meteorología mediante el empleo de magerit y PILAR.* Madrid. Recuperado el 10 de Agosto de 2018, de https://administracionelectronica.gob.es/pae_Home/dam/jcr:5ce286f2-c16f-4a6c-abb7-61d9622af6ef/MAGERIT_-_Analisis_de_riesgos_en_la_AEMET.pdf

ISO/IEC 27000. (2012). *Information technology — Security techniques — Information security management systems — Overview and vocabulary.*

ISO/IEC 27001:2013. (2013). *Tecnologia de la Informacion. Tecnicas de Seguridad. Sistemas de Gestión de la seguridad de la informacón. Requisitos.* Bogota: Instituto Colombiano de Normas Tecnicas y Certifiacion ICONTEC.

Martelo Gomez, R., Betin Rodriguez, A., & Jose, M. O. (2015). *SOFTWARE DE APOYO PARA EL PROCESO DE IMPLANTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN ORGANIZACIONES BASADO EN LA NORMA ISO 27001 (Tesis de Grado).* Universidad de Cartagena, Bolivar. Recuperado el 10 de Octubre de 2017, de http://repositorio.unicartagena.edu.co:8080/jspui/bitstream/11227/2944/1/SOFTWARE%20DE%20APOYO%20PARA%20EL%20PROCESO%20DE%20IMPLANTACI%C3%93N%20DEL%20SISTEMA%20DE%20GESTI%C3%93N%20DE%20SEGURIDAD%20DE%20LA%20INFORMACI%C3%93N%20EN%20ORGANIZACIONES%20BASADO%

Ministerio de Economía y Finanzas. (2010). *Instructivo para la Formulación de Indicadores.* Lima: DIRECCIÓN GENERAL DEL PRESUPUESTO PÚBLICO. Recuperado el 15 de Octubre de 2017, de Instructivo para la Formulación de Indicadores: https://www.mef.gob.pe/contenidos/presupuesto_publico/normativa/Instructivo_Formulacion_Indicadores_Desempeno.pdf

Ministerio de Tecnologías de la Información y Comunicaciones. (s.f.). *Fortalecimiento de la gestión TI en el estado*. Recuperado el 5 de Agosto de 2018, de ¿Y de seguridad TI qué hacen las entidades?: http://www.mintic.gov.co/gestionti/615/w3-article-7083.html

Seclén Arana , J. (2016). *Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001.* Universidad Nacional Mayor de San Marcos . Lima: http://cybertesis.unmsm.edu.pe/handle/cybertesis/4884. Recuperado el 10 de Octubre de 2017, de http://cybertesis.unmsm.edu.pe/handle/cybertesis/4884

Shojaie, B., Federrath, H., & Saberi, I. (2014). Evaluating the effectiveness of ISO 27001:2013 based on Annex A. *9th International Conference on Availability, Reliability and Security*, 259-264.

Superintendencia de sociedades. (2015). *ACCIONES CORRECTIVAS, PREVENTIVAS Y DE MEJORA.* Recuperado el 20 de Octubre de 2017, de https://www.supersociedades.gov.co/superintendencia/oficina-asesora-de-planeacion/polinemanu/sgi/Documents/Documentos%20Calidad/DOCUMENTOS/GC-PR-002%20ACCIONES%20CTVAS.pdf

Susanto, H., Nabil Almunawar, M., & Chee Tuan, Y. (2011). Information Security Management System Standards: A comparative Study of the Big Five. *International Journal of Electrical & Computer Sciences*, 23-29.

Urruchurtu Gomez, M., & Zuñiga Silgado, I. (2013). *"PLAN ESTRATÉGICO DE SEGURIDAD DE INFORMACIÓN EN UNA EMPRESA DEL SECTOR INDUSTRIAL BASADO EN ISO/IEC 27001" CASO DE ESTUDIO: COTECMAR (CORPORACIÓN DE CIENCIA Y TECNOLOGÍA PARA EL DESARROLLO DE LA INDUSTRIA NAVAL, MARÍTIMA Y FLUVIAL).* Universidad tecnologica de Bolivar, Cartagena de Indias. Recuperado el 8 de Julio de 2018, de http://biblioteca.utb.edu.co/notas/tesis/0065348.pdf

Valencia Duque, F. (2017). *Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000.* Universidad Nacional de Colombia. RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao. Recuperado el 10 de Octubre de 2017, de https://www.researchgate.net/publication/317904811