PLANIFICACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN (SGSI), PARA EL PROCESO DE GESTIÓN DE REQUERIMIENTOS DE LA EMPRESA SITIS S.A.S., BASADO EN LA NORMA ISO/IEC 27001:2013

CASO DE ESTUDIO: PROCESO DE LA GESTIÓN DE REQUERIMIENTOS DE EMPRESA SITIS S.A.S.

MARÍA CAMILA HOYOS ORTEGA
JULY ANDREA INCHIMA GARZÓN

CORPORACIÓN UNIVERSITARIA COMFACAUCA – UNICOMFACAUCA
FACULTAD DE INGENIERÍA
POPAYÁN - CAUCA
2020

PLANIFICACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN (SGSI), PARA EL PROCESO DE GESTIÓN DE REQUERIMIENTOS DE LA EMPRESA SITIS S.A.S., BASADO EN LA NORMA ISO/IEC 27001:2013

CASO DE ESTUDIO: PROCESO DE LA GESTIÓN DE REQUERIMIENTOS DE EMPRESA SITIS S.A.S.

MARÍA CAMILA HOYOS ORTEGA
JULY ANDREA INCHIMA GARZÓN

CORPORACIÓN UNIVERSITARIA COMFACAUCA – UNICOMFACAUCA
FACULTAD DE INGENIERÍA
CURSO DE ÉNFASIS
DIPLOMADO EN IMPLEMENTACIÓN Y AUDITORÍA INTERNA EN SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27001:2013
POPAYÁN - CAUCA
2020

NOTA DE ACEPTACIÓN

Aprobado por el comité de Grado en cumplimiento de los requisitos exigidos por la Corporación Universitaria Comfacauca para optar por el título de INGENIERO DE SISTEMAS.

_____

_____

_____

_____
Director

_____
Jurado

_____
Jurado

Popayán, 12 de agosto de 2021

DEDICATORIA

A *María Fabiola Garzón* por ser ejemplo de vida,
perseverancia, paciencia y amor.
Mi gratitud eterna a esta maravillosa mujer.

Andrea Inchima Garzón

A mis padres, *León Bolívar Hoyos* y *María del Carmen Ortega*
por brindarme su apoyo espiritual e incondicional y
demostrarme que los sueños si se trabajan
con esfuerzo y disciplina, se cumplen.

María Camila Hoyos

AGRADECIMIENTOS

Queremos agradecer principalmente a Dios por permitir la culminación de este proceso, a nuestra familia y amigos por cada día ser nuestro soporte.

Agradecemos a la Corporación Universitaria Comfacauca y a sus docentes por permitirnos hacer parte de sus estudiantes en formación, por guiarnos y brindarnos la oportunidad de enriquecer nuestro conocimiento.

A la organización SITIS S.A.S por otorgar el consentimiento de realizar este trabajo de grado en el proceso de “Gestión de Requerimientos” y especialmente al Ingeniero Francisco Ramírez por el apoyo incondicional en la construcción del procedimiento de seguridad de la información dentro del proceso que lidera.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

GLOSARIO

Activo (Asset): “En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización” [1].

Alcance (Scope): “Ámbito de la organización que queda sometido al SGSI” [1].

Amenaza (Threat): “Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización” [1].

Análisis de riesgos (Risk analysis): “Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo [1].

El análisis de riesgos proporciona la base para la estimación de riesgos y las decisiones sobre el tratamiento de riesgos. El análisis de riesgos incluye la estimación de riesgos”.

Análisis de riesgos cualitativo (Qualitative risk analysis): “Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia” [1].

Análisis de riesgos cuantitativo (Quantitative risk analysis): “Análisis de riesgos en función de las pérdidas financieras que causaría el impacto” [1].

CID (CIA): “Acrónimo español de confidencialidad, integridad y disponibilidad, las dimensiones básicas de la seguridad de la información” [1].

Confidencialidad (Confidentiality): “Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados” [1].

Control: “Medida por la que se modifica el riesgo [1].

Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. El término salvaguarda o contramedida son utilizados frecuentemente como sinónimos de control” [1].

Disponibilidad (Availability): “Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada” [1].

Evaluación de riesgos (Risk assessment): “Proceso global de identificación, análisis y estimación de riesgos” [1].

Gestión de riesgos (Risk management): “Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Se compone de la evaluación y el tratamiento de riesgos” [1].

Identificación de riesgos (Risk identification): “Proceso de encontrar, reconocer y describir riesgos.

La identificación de riesgos implica la identificación de las fuentes del riesgo, eventos, sus causas y sus posibles consecuencias. La identificación de riesgos puede involucrar datos históricos, análisis teóricos, opiniones informadas y de expertos, y las necesidades de las partes interesadas” [1].

Impacto (Impact): “El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc-“ [1]

Integridad (Integrity): “Propiedad de la información relativa a su exactitud y completitud” [1].

Inventario de activos (Assets inventory): “Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos” [1].

ISO/IEC 27001: “Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial” [1].

Plan de tratamiento de riesgos (Risk treatment plan): “Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma” [1].

Política (Policy): “Intenciones y dirección de una organización, expresada formalmente por su alta dirección” [1].

Probabilidad (Likelihood): “Posibilidad de que ocurra algo” [1].

Riesgo (Risk): “Efecto de la incertidumbre sobre los objetivos” [1].

Salvaguarda (Safeguard): “Véase: Control” [1].

Seguridad de la información (Information security): “Preservación de la confidencialidad, integridad y disponibilidad de la información” [1].

Tratamiento de riesgos (Risk treatment): “Proceso para modificar el riesgo” [1].

Vulnerabilidad (Vulnerability): “Debilidad de un activo o control que puede ser explotada por una o más amenazas” [1].

RESUMEN

SITIS Soluciones Informáticas Integrales en Salud SAS, es una empresa caucana que cuenta con una larga trayectoria en el desarrollo e implementación de sistemas que apoyan la optimización en el uso de la información y el mejoramiento de procesos en el sector salud. Posee un equipo experto y comprometido que tiene capacidades en el uso de herramientas informáticas que contribuyen a humanizar el cuidado de la salud. Ofrece servicios de Consultoría de Normatividad, Desarrollo de Software, Interoperabilidad, Expediente Clínico Electrónico e Integración de equipos Biomédicos en países como Colombia, México y Ecuador.

Este documento propone la planificación del sistema de gestión de la seguridad de la información basado en la norma 27001:2013 y en la metodología de Magerit V3 Libro II, adaptada al proceso de gestión de requerimientos en la empresa SITIS S.A. como caso de estudio, ya que en la actualidad y a pesar de los años de experiencia que posee como organización de base tecnológica, tiene un cumplimiento parcial de sus políticas establecidas y no cuenta con un SGSI que contenga las medidas orientadas a proteger la información de sus diferentes áreas lo que ha conllevado a enfrentar incidentes como accesos no autorizados en sus procesos, generando perdida de la información.

En la etapa inicial de este proyecto se realiza el conocimiento del contexto de la organización mediante visitas, entrevistas y el desarrollo de una encuesta acerca del conocimiento sobre la seguridad de la información por parte del equipo de trabajo del área de producto, con la cual se efectúa primer acercamiento a su problemática.

Posteriormente se realiza el análisis del proceso para identificar el inventario de activos de información, los cuales se clasifican según la metodología escogida y se realiza la identificación de las amenazas, las vulnerabilidades y riesgos a los que está expuesto el proceso; de esta manera se plantea o establece los controles o mecanismos con los cuales se puede reducir el impacto y las probabilidades de ocurrencia de las incidencias de seguridad.

Por último, se desarrolla la declaración de aplicabilidad, el plan de tratamiento y generación de la política de seguridad, los cuales son los entregables para la empresa SITIS SAS.

ABSTRACT

SITIS Integrated informatics solutions in Health SAS, it is a Caucana enterprise which has a long trajectory in the development and system implementation that support optimization in the use of information and process improvement in the health sector. It has an expert team and committed that has capabilities in the use of information technology tools that contribute to humanizing health care. It offers Regulatory Consulting, Software Development, Interoperability, electronic clinical file also Integration of biomedical equipment in countries such as Colombia, México and Ecuador.

This document proposes the design of the stage in the standard-based information security management system planning 27001:2013, accordance with the methodology by Magerit V3 Book II, conditioned to the process of requirements management in the company SITIS S.A. Therefore as a case study, because today and despite years of experience as a technology-based organization, has partial compliance with its established policies and it does not have a ISMS containing measures to protect information of its different areas which has led to facing incidents as unauthorized access in its processes, generating loss of information.

In addition, the initial stage of this project is realized the knowledge in the context of the organization through visits, interviews and the development of a knowledge survey on information security by the product area work team, with which the first approach is made of its problematic.

The process analysis is then carried out to identify the inventory of information assets, which are classified according to the chosen methodology and the identification of threats, vulnerabilities and risks to which the process is exposed; in this way controls are considered or established as well as mechanisms by which impact could be reduced and the probability of occurrence of safety incidents.

Finally, the Declaration of Applicability is developed, the security policy processing and generation plan, which are the deliverables for the company SITIS SAS.

1. CAPÍTULO I INTRODUCCIÓN Y CONTEXTO

1.1. Introducción

Sin lugar a duda podemos observar en la actualidad como la tecnología, las telecomunicaciones, la informática y el internet, se han convertido en una necesidad; siendo hoy en día una parte fundamental desde toda perspectiva, sobre todo en el sector institucional y/ o empresarial. El manejo de la información física o digital de los diferentes procesos de las organizaciones permiten la toma de decisiones, por lo tanto, merecen el cuidado y la atención adecuada, pues al estar expuesta a múltiples riesgos, se vuelve un aspecto crítico que requiere asegurar la integridad, disponibilidad y confidencialidad de la misma.

La familia de la norma ISO 27000 [2], especialmente la norma ISO 27001 proporciona directrices para la gestión del riesgo en la seguridad de la información y es aplicable a cualquier tipo de organización, aunque esta norma no provee una metodología en específico para la gestión del riesgo, se apoya de otras metodologías como ISO 31000 [3], ISO 27005 [4], Octave Allegro [5] o Margerit [6] que son muy utilizadas en la actualidad. Para el presente proyecto se utiliza la metodología Margerit [6] versión 3.0 libro II, la cual es un catálogo de elementos que tiene principalmente como objetivo “homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios que permitan comparar e incluso integrar análisis realizados por diferentes equipos” [7]. Teniendo en cuenta aspectos como tipos de activos, dimensiones de valoración, criterios de valoración, amenazas, y salvaguardas.

Con base en lo expuesto anteriormente, se realiza un análisis de riesgos del proceso misional “Gestión de Requerimientos” de la empresa SITIS SAS, en relación a la gestión de la seguridad de la información, el resultado de este análisis servirá como insumo para la propuesta de implementación de al menos una política para el SGSI basado en la norma ISO 27001:2013, la cual contribuirá a la protección los activos de información, ayudando a conservar la confidencialidad, integridad y disponibilidad de cada uno, así mismo poder garantizar la continuidad del proceso.

1.2. Planteamiento del problema

En la actualidad, se evidencia que la tecnología avanza a pasos agigantados, y con ella se observa la gran cantidad de riesgos a los que se está propenso por el uso de la misma, afectando entre otros, a las organizaciones debido a la información que manejan. [8]

Las empresas de base tecnológica buscan producir bienes y/o servicios de innovación a partir del diseño, desarrollo y producción de nuevos productos, donde su principal activo es la información y conocimiento, por medio de la cual se toman decisiones fundamentales para su avance y progreso. [9]

Los activos de este tipo de empresas están expuestos a riesgos de seguridad de la información que pueden llegar a representar problemas considerables como perdida financiera, de confianza o de reputación de los clientes. El no poseer una buena gestión de riesgos con lleva a ser vulnerables ante amenazas como, fugas de información, accesos no autorizados, perdida de la información, etc. que pueden afectar el funcionamiento e incluso, dependiendo del incidente, puede llevar a la quiebra a la organización. [10]

SITIS SAS es una empresa tecnológica con más de 13 años de experiencia en ejecución de proyectos Nacionales e Internacionales en la implementación e implantación de soluciones informáticas y servicios para el sector salud. A pesar de la larga trayectoria que posee la empresa, en la actualidad, no cuenta con medidas orientadas a proteger la información de sus clientes, ni de sus diferentes áreas como, por ejemplo: desarrollo, pruebas, operaciones, administrativa y especialmente el área de análisis o producto que se encuentra dentro del proceso de “Gestión de Requerimientos”, siendo catalogado por la alta gerencia como un proceso de vital importancia debido a que la organización se reserva el derecho de realizar su propia documentación y es el punto de partida de su ciclo de desarrollo de software.

A causa de esto, la organización se ha enfrentado a accesos no autorizados generando perdida de información vital para su buen funcionamiento, adicional a esto se evidencia falencia en la aplicación de su política de copias de seguridad, que, aunque se realizan periódicamente no son validadas oportunamente y ha generado de igual manera perdida de la información.

1.3. Justificación

Hoy en día las organizaciones evidencian el uso de la tecnología para realizar cada uno de sus procesos generando progreso y crecimiento, así mismo con el auge tecnológico han crecido las amenazas a las que estas están expuestas, llevando a buscar métodos o estándares que contribuyan a regular un comportamiento seguro para salvaguardar sus activos de información. [11]

Es por ello que la seguridad de la información definida como todo el conjunto de técnicas y acciones que se implementan para controlar y mantener la privacidad de la información y datos de una institución asegurando que estos no caigan en manos equivocadas [12], es el medio por el cual se busca la protección de los activos de las organizaciones enfocados a preservar la confidencialidad, disponibilidad e integridad de la información, de esta manera se previene o reduce los posibles daños causados por la explotación de vulnerabilidades existentes dentro de las empresas.

De acuerdo a lo anterior, Implementar un sistema de gestión de la información basado en la norma ISO 27001:2013 tiene como beneficios el análisis de riesgos, la identificación de tratamientos de incidencias, el incremento del nivel de confianza de los clientes, el aumento de valor comercial y mejoramiento de la imagen de la organización.

Dentro de este orden de ideas, la planificación de SGSI en la empresa SITIS SAS en su proceso misional de Gestión de Requerimientos asegura la continuidad del negocio debido a que prepara a la organización para reaccionar rápidamente ante cualquier amenaza o incidente de seguridad, adicionalmente aumenta la confianza de los clientes por la protección y confidencialidad de los datos que suministran. También se evidencia como beneficio la reducción del riesgo de que se produzcan pérdidas de información generados dentro del proceso como robos o corrupción en la manipulación de la misma, a través de la implementación de controles o mecanismos con los cuales se minimiza el impacto, las probabilidades o incluso evitando la ocurrencia de los incidentes de seguridad.

De acuerdo a lo mencionado anteriormente se propone la planificación de un sistema de gestión de seguridad de información (SGSI), para el proceso de gestión de requerimientos de la empresa SITIS S.A.S., basado en la norma ISO/IEC 27001:2013.

1.4. Objetivos

1.4.1. Objetivo general

Planificar un sistema de gestión de seguridad de información (SGSI), para el proceso de Gestión de Requerimientos de la empresa SITIS S.A.S., ubicada en la ciudad de Popayán, basado en la norma ISO 27001:2013.

1.4.2. Objetivos específicos

- Determinar los activos y amenazas que se presenten en el proceso de “Gestión de Requerimientos” de la empresa SITIS S.A.S.

- Realizar el análisis y la valoración de los riesgos que se presentan en el proceso de “Gestión de Requerimientos” de la empresa SITIS SAS, basados en la metodología Magerit.

- Identificar las salvaguardas que protegen los activos de información del proceso de “Gestión de Requerimientos” de la empresa SITIS SAS, basados en la metodología Magerit.

- Construir el plan de tratamiento de riesgo que permita mitigar las amenazas y vulnerabilidades identificadas dentro de los activos de información del proceso de “Gestión de Requerimientos” de la empresa SITIS SAS.

1.5. Contexto de la empresa

SITIS SAS es una empresa con más de 13 años de experiencia en ejecución de proyectos Nacionales e Internacionales en la implementación e implantación de soluciones informáticas y servicios para el sector salud, los cuales cumplen con los estándares de normatividad, técnicos y de calidad para el desarrollo de los mismos. Su propósito es apoyar la optimización en el uso de la información y el mejoramiento de procesos, busca satisfacer al cliente con productos y servicios de calidad.

SITIS Soluciones Informáticas Integrales en Salud S.A.S, está conformada por un equipo joven, experto, entusiasta y comprometido, que cree en la capacidad de las herramientas informáticas para mejorar la calidad de vida de las personas, no sólo desde el punto de vista de la seguridad que las TIC le pueden dar al manejo de la información, sino en la habilidad de gestión y procesamiento de la información, en reemplazo de los procesos manuales.

SITIS es una empresa colombiana, con presencia Regional, comprometida con su labor y con la calidad de sus procesos. El sistema de calidad y gestión de procesos que aplica a sus proyectos la hace competitiva y costo-efectiva. SITIS posee certificación en la norma ISO/IEC 15504, un modelo actualizado y específico para desarrollo de software, que ya está aplicando. Sus metodologías de desarrollo son ágiles 100%, con énfasis en grupos pequeños, lo cual mejora la velocidad y calidad del proceso. La plataforma de certificación ISO/IEC 15504 provee herramientas que facilitan el acceso y el cumplimiento de las reglas de otras certificaciones. La empresa surge en el año 2000, a la luz de la reforma en Salud en Colombia, la cual mejora el acceso a las tecnologías de la información al modelo de atención vanguardista del país.

1.5.1. Visión

SITIS SAS es una empresa exitosa con talento humano comprometido y calificado, aliado de los prestadores de salud en el mejoramiento de su gestión.

1.5.2. Misión

Satisfacer al cliente con productos y servicios de calidad, implementados por un equipo de trabajo responsable e idóneo.

1.5.3. Proceso misional de Gestión de Requerimientos

SITIS SAS tiene definido en su plan estratégico el de mapa de procesos en el cual se encuentre el cómo proceso misional la Gestión de Requerimientos.

Mapa de procesos SITIS SAS

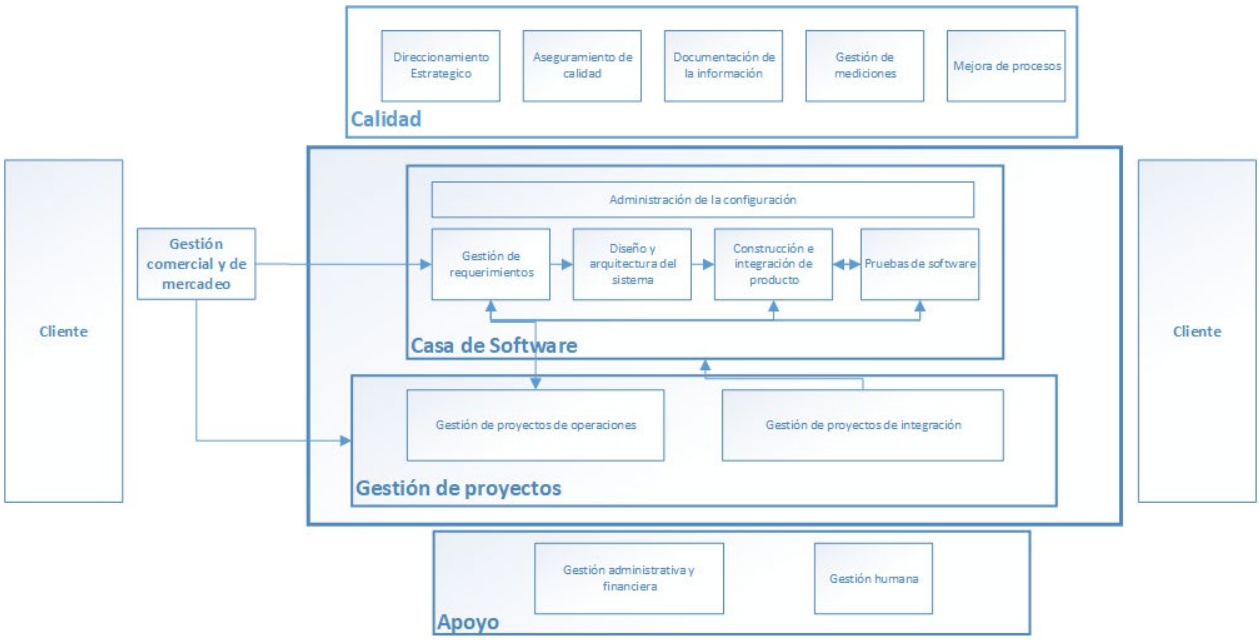

Figura 1. Mapa de procesos SITIS SAS
Fuente: Sistema de Gestión de Calidad SITIS SAS

Este proceso tiene como objetivo definir de forma detallada y clara los requerimientos que dan solución a las necesidades de los clientes internos y externos, los cuales serán implementados en los productos construidos por SITIS SAS. Este procedimiento debe ejecutarse por todo personal que desempeñe actividades de licitación, captura y documentación para definir todos los requerimientos reportados por el cliente interno y externo hacia la casa de software, requerimientos identificados como funcionalidad nueva, mejora o inconsistencia.

El proceso de Gestión de Requerimientos es de vital importancia para la empresa y se convierte en un proceso misional debido a que de todos los procesos existentes que se realizan en la casa de software, como por ejemplo el desarrollo, las pruebas de software, la administración de la base de datos o la gestión de la configuración, entre otros, se pueden tercerizar, pero lo que no se puede tercerizar es la gestión del conocimiento, por lo cual la empresa se reserva el derecho de hacer sus propios casos de uso debido a que el activo más importante de la empresa está en la documentación del producto y en el código fuente.

En este momento unos de los elementos más importantes para la organización es el análisis, ya que, a partir de una buena documentación de análisis de requerimientos se realiza los planes de desarrollo, los planes de despliegue, se proyecta el Roadmap, organizar las iteraciones e incluso calcular cuantas células de desarrollo se necesitan para llevarlas a cabo, una buena documentación del producto permite planear correctamente el proyecto.

1.5.4. Equipo de trabajo

El equipo de trabajo del proceso de gestión de requerimientos se evidencia en la *Tabla 1. Roles y responsabilidades.*

Tabla 1. Roles y responsabilidades

Rol	Nombre	Responsabilidad
Coordinador o líder Producto	Francisco Ramírez	Prioriza los requerimientos a implementarse. Consulta y se asesora para la implementación de requerimientos con equipo consultor. Dirige al equipo de trabajo encargado de documentar la propuesta para dar una solución al requerimiento del cliente.
	Rene Caicedo	
Analista Funcional	Natalia Recalde	Genera los documentos que permiten detallar los requerimientos solicitados por el cliente.
	Paola Hurtado	
	Karen Zúñiga	
	Marisol Valencia	
Experto de dominio	Montserrat Mora	Es un usuario que es especialista y que conoce los procesos de negocio y ayuda a delimitar el alcance funcional de la solución propuesta

Con el fin de conocer las bases de conocimiento del equipo de producto respecto a la Seguridad de la Información, se realiza una encuesta que se puede evidenciar en el Anexo 01 - Encuesta sobre conocimientos de Seguridad de la información, con la cual se inicia el proceso de análisis y enfoque con el que se desarrolla la presente propuesta.
Esta información se concluye que el 100% de los encuestados ratifica la importancia que tiene Seguridad de la información y que es vital realizar el tratamiento indicado, pues en su gran mayoría presentan desconocimiento sobre el buen manejo de la seguridad.

1.5.5. Documentación

Dentro del proceso de gestión de requerimientos se generan los siguientes documentos, estos serán descritos en el inventario de activos de información:

1. Conceptos Generales (Basados en normas oficiales)
2. Alcance funcional
3. Prototipos (Mockups)
4. Conjunto Mínimo de datos básicos
5. Historias de usuario
6. Criterios de aceptación
7. Reglas de negocio
8. Casos de uso
9. Roadmap
10. Plan de Liberación

2. CAPÍTULO II – MARCO TEÓRICO

2.1. Estado del arte

La información en una organización es uno de los activos más importantes que se deben proteger, a través, de mecanismos de seguridad como la aplicación de estándar ISO 27001:2013, que permite manejar todas las medidas preventivas para salvaguardar cada uno de los activos y lograr evitar la pérdida de la confidencialidad, disponibilidad e integridad de sus sistemas y aplicaciones.

A partir de la revisión y consulta de documentos de investigación que se encuentran relacionados al análisis y gestión de riesgo de un SGSI teniendo en cuenta el estándar ISO 27001 y la implementación de la metodología Magerit, se toman como base para el desarrollo del presente proyecto los siguientes estudios:

En [13], se analiza y se compara la gestión del riesgo a través de metodologías como Octave y Magerit, que están destinadas a identificar qué tipo de amenazas y vulnerabilidades están expuestas las organizaciones y como combatirlas o evitarlas.

En [14], se evidencia la implementación de una guía de un SGSI para entidades de Contac Center basado en la norma ISO/IEC 27001, en donde se da cumplimiento a los objetivos propuestos por sus autores, realizando el análisis y la gestión de los riesgos con los fundamentos de la metodología Magerit.

En [15], especifica el uso de la metodología de las elipses para determinar el alcance de SGSI de los procesos internos y externos para el caso de estudio seleccionado por el autor, el cual funciono exitosamente.

2.2. Marco Conceptual

Norma internacional ISO/IEC 27001:2013 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos

Norma elaborada con el fin de suministrar requisitos para el establecimiento, implementación mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información [16] basado en el Ciclo de Deming (Planificar, Hacer, Verificar, Actuar). Su primera versión publicada en el año 2005 y su última actualización

realizada en el año 2013 por la International Organization for Standardization y por la comisión International Electrotechnical Commission. Este estándar de seguridad de la información permite la protección de la confidencialidad, integridad y disponibilidad por medio de la evaluación de los riesgos y la aplicación de controles para mitigarlos.

Contiene una estructura de alto nivel de los requisitos de la sección 4 al 10 y adicional el Anexo A. Esta norma está organizada de la siguiente manera:

1. **Objeto y campo de aplicación:** Orienta en el uso, finalidad y modo de aplicación del estándar.
2. **Referencias Normativas:** Referencia documentos normativos indispensables para la aplicación de ISO/IEC 27001.
3. **Términos y Definiciones:** Describe la terminología aplicable al estándar presentados en la ISO/IEC 27000.
4. **Contexto de la Organización:** Este es el primer requisito de la norma, el cual determina indicaciones externas e internas sobre el conocimiento de la organización y su contexto, la comprensión de las necesidades y expectativas de las partes interesadas y la determinación del alcance del Sistema Gestión de la Seguridad de la Información.
5. **Liderazgo:** Esta sección da directrices en donde la organización debe contribuir al establecimiento de la norma. Por medio de alta dirección debe demostrar su liderazgo y compromiso, elaborando una política de seguridad que se de conocimiento para toda la organización asignando roles, responsabilidades y autoridades dentro de la misma.
6. **Planificación:** Determina las acciones para tratar riegos y oportunidades asegurando que el SGSI de resultados, mediante la valoración y el tratamiento de los mismo para lograr una mejora continua.
7. **Soporte:** La organización determina los requisitos de soporte de recursos, competencias, conciencia, comunicación e información documentada para establecer, implementar, mantener y mejorar continuamente el SGSI.
8. **Operación:** Establece el plan y el control operacional, la valoración y el tratamiento de los riesgos de la seguridad de la información para cumplir con lo que dispone la norma ISO 27001:2013.
9. **Evaluación del Desempeño:** Se trata del seguimiento, medición, análisis y evaluación de la eficacia y desempeño del SGSI, así mismo de la realización de auditorías internas y revisiones de la dirección de la organización para garantizar el cumplimiento de los objetivos del SGSI.

10. **Mejora:** Tiene como elemento fundamental la detección de No conformidades y sus acciones correctivas que conlleven a la mejora continua de la conveniencia, y eficacia del SGSI.
11. **Anexo A:** Objetivos de control y controles de referencia:
    Está compuesta por 14 Cláusulas de control, 35 Objetivos de control y 114 Controles.
    - ❖ A.5. Políticas de seguridad de la información.
    - ❖ A.6. Organización de la seguridad de la información.
    - ❖ A.7. Seguridad de los recursos humanos.
    - ❖ A.8. Gestión de Activos.
    - ❖ A.9. Controles de acceso.
    - ❖ A.10. Criptografía – Cifrado y gestión de claves.
    - ❖ A.11.Seguridad física y ambiental.
    - ❖ A.12. Seguridad operacional.
    - ❖ A.13. Seguridad de las comunicaciones.
    - ❖ A.14. Adquisición, desarrollo y mantenimiento del Sistema.
    - ❖ A 15 Relaciones con los proveedores.
    - ❖ A.16. Gestión de incidentes de seguridad de la información.
    - ❖ A.17. Continuidad de Negocio
    - ❖ A.18.Cumplimiento.

Norma internacional ISO/IEC 27002:2013 Tecnología de la información. Técnicas de seguridad. Código de práctica para controles de seguridad de la información

La Norma Internacional 27002, hace parte del grupo de normas de la serie de la 27000, esta norma nos describe como se establecen directrices y principios generales para poder realizar, implementar y mejorar un SGSI, apoyándose en los controles pactados en la norma 27001:2013 de la seguridad de la información para el uso por parte de las organizaciones.

Esta norma está organizada de la siguiente manera

0. **Introducción**: Descripción general sobre los sistemas de seguridad.
1. **Objeto y Campo de Aplicación:** Descripción el objetivo principal de la norma.
2. **Referencias Normativas**: Descripción de las referencias normativas que contiene la norma.
3. **Términos y Definiciones**: Descripción de los términos y definiciones pactados en la norma ISO 27000.

4. **Estructura de la Guía:** La norma se encuentra organizada con 14 dominios, 35 Objetivos y 1124 Controles.
   4.1 Numerales
   4.2 Categorías de Control
5. **Políticas de la seguridad de la información:** Se debe crear y revisar de manera pertinente la política de seguridad de la información.
   5.1 Directrices establecidas por la dirección para la seguridad de la información
6. **Organización de la seguridad de la información:** Se debe gestionar la seguridad de la información en la empresa.
   6.1 Organización Interna
   6.2 Dispositivos móviles y Teletrabajo
7. **Seguridad de recursos humanos: Asegurar** que todos los funcionarios de las organizaciones se adapten a cada responsabilidad que sea asignado y se sensibilicen con la protección de la información.
   7.1 Antes de asumir el empleo
   7.2 Durante la ejecución del empleo
   7.3 Terminación y cambio de empleo
8. **Gestión de Activos:** Permite lograr y mantener la protección de los activos que se encuentren en la empresa.
   8.1 Responsabilidad por los activos
   8.2 Clasificación de la información
   8.3 Manejo de Medios
9. **Control de acceso**: Se encargar de limitar el acceso no autorizado a la información y a las instalaciones en donde se procese información confidencial**.**
   9.1 Requisitos del negocio para control de acceso
   9.2 Gestión de acceso de usuarios
   9.3 Responsabilidades de los usuarios
   9.4 Control de acceso a sistemas y aplicaciones
10. **Criptografía:** Asegurar el uso de la criptografía para proteger los pilares importantes de la seguridad de la información.
    10.1 Controles Criptográficos
11. **Seguridad física y del entorno**: Se encarga de prevenir el acceso físico de personas no autorizadas a las instalaciones de la empresa.
    11.1 Áreas seguras
    11.2 Equipos
12. **Seguridad de las operaciones:** Asegurar las operaciones de manera correcta y la seguridad de las instalaciones de la empresa.

12.1 Procedimientos operacionales y responsabilidades
12.2 Protección contra códigos maliciosos
12.3 Copias de respaldo
12.4 Registro y seguimiento
12.5 Control de software operacional
12.6 Gestión de la vulnerabilidad técnica
12.7 Consideraciones sobre auditorias de sistema de la información

13. **Seguridad de las comunicaciones:** Asegurar la protección de la información en el uso de las redes.
    13.1 Gestión de la seguridad de las redes
    13.2 Transferencia de información
14. **Adquisición, Desarrollo y mantenimiento de sistemas:** Asegurar que la información sea parte integrar los sistemas de información dentro de la organización.
    14.1 Requisitos de la seguridad de los sistemas de información
    14.2 Seguridad en los procesos de desarrollo y de soporte
    14.3 Datos de prueba
15. **Relaciones con los proveedores:** Asegurar la protección de los activos que se encuentren relacionados con los proveedores**.**
    15.1 Seguridad de la información en las relaciones con los proveedores
    15.2 Gestión de la presentación de servicios de proveedores
16. **Gestión de incidentes de seguridad de la información:** Asegurar los activos que se encuentren sensibles para los riegos aplicando una gestión de incidentes.
    16.1 Gestión de incidentes y mejoras en la seguridad de la información
17. **Aspectos de seguridad de la información de la gestión de continuidad de negocio:** Se debe tener un plan de continuidad dentro de la organización
    17.1 Continuidad de seguridad de la información
    17.2 Redundancias
18. **Cumplimiento:** Maximizar la eficacia del cumplimiento de las obligaciones que se encuentren relacionadas en la empresa**.**
    18.1 Cumplimiento de requisitos legales y contractuales
    18.2 Revisiones de seguridad de la información

Conceptos Generales

Se describe a continuación los conceptos fundamentales para el desarrollo del proyecto y entendimiento de la terminología utilizada a lo largo del documento.

Teniendo en cuenta que un activo de información según la norma ISO/IEC 27001 es: “algo que una organización valora y por lo tanto debe proteger”, debido a que es el insumo principal para el funcionamiento del negocio y consecución de los objetivos propuestos por la alta dirección, este se constituye como el activo más importante de la organización.

La seguridad de la información se orienta a establecer las medidas preventivas y reactivas que las organizaciones implementan para salvaguardar y proteger los activos de información basados en sus 3 pilares fundamentales que son la Confidencialidad que es la propiedad que determina que la información no está disponible ni es revelada a quien no esté autorizado [2], la Integridad que se refiere la protección de la exactitud y completitud de la información, evitando modificaciones no autorizadas y la Disponibilidad que es la propiedad que la información sea accesible y utilizable por solicitud de los autorizados [2].

Partiendo de estos elementos, se evidencia la importancia y la necesidad de gestionar la seguridad de la información, y una de las maneras de realizarlo es mediante las buenas prácticas de la norma ISO/IEC 27001:2013 [16] a través de la implementación de un sistema de gestión de seguridad de la información, mediante el cual se busca la protección de amenazas que pueden perjudicar a los activos de información.

El sistema de gestión de seguridad de la información está basado en el ciclo de Deming teniendo en cuenta 4 fases que son Planificar, Hacer, Verificar y Actuar, proyectando de la mejora continua; de esta manera se organizan las gestiones que alineadas completan y soportan el cumplimiento de los objetivos de la seguridad de la información. [17]

A través del sistema de gestión, se busca identificar, clasificar y valorar los activos de información, de igual manera permite el análisis y valoración de los riesgos por medio de la identificación del impacto y la probabilidad de ocurrencia de las amenazas que pueden ser materializadas por las vulnerabilidades a las que están expuestos los activos de información. Tras haber determinación del nivel de riesgo se toman las medidas adecuadas para afrontarlo, a través de la eliminación, transferencia, aceptación y mitigación.

Mediante de la guía de buenas prácticas ISO/IEC 27002 [18] se establecen los controles como medidas de seguridad para mitigar los riesgos encontrados en el análisis de riesgos, estos controles son recogidos a través de la Declaración de Aplicabilidad SOA,

una vez son implantados a través del plan de tratamiento los controles estos ayudan a la disminución de las incidencias de seguridad.

Es importante que se contemple que con la implementación del SGSI se requiere un proceso de sensibilización y concienciación sobre la gestión de los activos de información por parte de todos los miembros de la organización.

2.3. Metodologías

Para la realización del análisis de los riegos existen en la actualidad diferentes metodologías, la organización debe seleccionar aquella que se ajuste a sus necesidades y de fácil aplicación debido a que se debe ejecutar periódicamente.
A continuación, se detalla dos de las metodologías más reconocidas:

2.3.1. Octave

“(Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE®), desarrollado en EEUU por el SEI, es una metodología para recoger y analizar información de manera que se pueda diseñar una estrategia de protección y planes de mitigación de riesgo basados en los riesgos operacionales de seguridad de la organización. Hay dos versiones, una para grandes organizaciones y otra para pequeñas, de menos de 100 empleados” [19].

2.3.2. Magerit V3

“Desarrollado por el Ministerio de Administraciones Públicas español, es una metodología de análisis de riesgos que describe los pasos para realizar un análisis del estado de riesgo y para gestionar su mitigación, detalla las tareas para llevarlo a cabo de manera que el proceso esté bajo control en todo momento y contempla aspectos prácticos para la realización de un análisis y una gestión realmente efectivos.
Cuenta con detallados catálogos de amenazas, vulnerabilidades y salvaguardas. Cuenta con una herramienta, denominada PILAR para el análisis y la gestión de los riesgos de los sistemas de información que tiene dos versiones, una completa para grandes organizaciones y otra simplificada para las pequeñas” [19].

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el antiguo Consejo Superior de Administración Electrónica (actualmente Comisión de Estrategia

TIC), como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.
La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza [6]

La metodología MAGERIT se basa en analizar el impacto que puede tener para la empresa la violación de la seguridad, buscando identificar las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas [20]

Objetivos de Magerit [6]:

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos:
4. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

MAGERIT versión 3 se estructura en tres libros: "Método", "Catálogo de Elementos" y "Guía de Técnicas".

Libro I Método: Corresponde a la introducción de metodología Magerit, en el cual está estipulado por diversos capítulos [6].

Libro II Catalogo de Elementos: Este libro se distingue porque tiene la guía de implementación de la metodología, en el cual marca unas pautas en cuanto a [6]:

- Tipos de activos
- Dimensiones de valoración de los activos
- Criterios de valoración de los activos
- Amenazas típicas sobre los sistemas de información

- ❖ Salvaguardas a considerar para proteger sistemas de información

Libro III Guías Técnicas: Aporta luz adicional y orientación sobre algunas técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos [6]:

- ❖ Técnicas específicas para el análisis de riesgos
  - Análisis mediante tablas
  - Análisis algorítmico
  - Árboles de ataque
  - Técnicas generales
  - Técnicas gráficas
  - Sesiones de trabajo: entrevistas, reuniones y presentaciones
- ❖ Valoración Delphi: Se trata de una guía de consulta. Según el lector avance por las tareas del proyecto, se le recomendará el uso de ciertas técnicas específicas, de las que esta guía busca ser una introducción, así como proporcionar referencias para que el lector profundice en las técnicas presentadas.

En la *Tabla 2* se detalla la comparación de las dos metodologías

Tabla 2. Comparativa de metodologías [13]

MAGERIT	**OCTAVE**
MAGERIT orienta sus objetivos en 2 fases: 1. El análisis de riesgo. 2. La gestión del riesgo	OCTAVE orienta sus objetivos en 3 fases: 1. La creación de amenazas. 2. La identificación de vulnerabilidades. 3. El planteamiento de estrategias pro a la mitigación de los riesgos.
MAGERIT promueve sensibilizar a los responsables de la existencia de riesgos en los activos que hacen parte de un sistema de información y con la necesidad de identificarlos inmediatamente.	OCTAVE está encaminado a involucrar los participantes en la organización con el propósito de estudiar las necesidad para la protección de la seguridad de la información.
MAGERIT le da importación a los riesgos que se encuentren relacionados a los activos de la empresa.	OCTAVE diseña una gestión de riesgo basada en la operatividad de la organización.

MAGERIT ofrece un método sistemático para analizar los riesgos.	OCTAVE maneja tres métodos: auto-dirigido, flexibles y evolucionado.
MAGERIT prepara a las empresas para procesos de evaluación, auditoría, certificación o acreditación.	OCTAVE Realiza los principios básicos y la estructura de las mejores prácticas-internacionales que guían los asuntos no técnicos
MAGERIT sensibiliza a los responsables de los sistemas de información de los riesgos que se relacionan con los activos que hacen parte del sistema de información.	OCTAVE Divide los activos en dos tipos: sistemas, (Hardware. Software y Datos) y personas
MAGERIT Genera el uso de las tecnologías de la información	OCTAVE Se genera uso en el riesgos organizacional y el foco son los temas relativos a la estrategia y la practica
MAGERIT relaciona las amenazas a que están expuestos los activos y se adapta en la metodología.	OCTAVE Se identifica y consolidad la información y creación de perfiles de amenazas.
MAGERIT Se encarga de caracterizar el valor que representan los activos para la Organización	OCTAVE Se encarga de desarrollar una estrategia de protección, Identifica los recursos importantes

Fuente propia basado en [6] [13] [19]

2.4. Ciclo PHVA

Actualmente las empresas están expuestas a amenazas y vulnerabilidades por la adopción de tecnologías para mejorar sus procesos, a razón de esto, las organizaciones podrían contar con un sistema de gestión de seguridad teniendo en cuenta sus 3 pilares fundamentales, la confidencialidad, disponibilidad e integridad que permita la protección de los activos de información que posean, esto permitirá la continuidad del negocio.

La norma ISO/IEC 27001:2013 adopta el modelo “Planear-Hacer-Verificar-Actuar” (PHVA) que se aplica para estructurar los procesos del SGSI, esta toma como elementos de entrada los requisitos de seguridad de la información y las expectativas de las partes interesadas y, a través de acciones y procesos necesarios produce resultados de seguridad de la información que cumplen con dichos requisitos y expectativas [21].

Ciclo PHVA

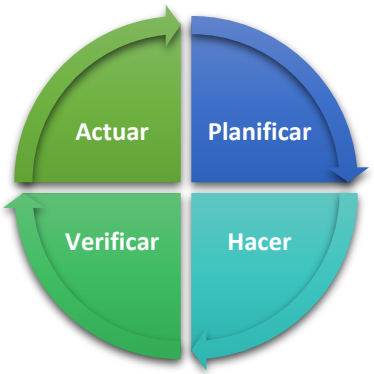

Figura 2. Ciclo PHVA del SGSI [17]

Descripción del modelo PHVA

Proceso PHVA	Descripción
Planificar: Establecer el SGSI	Establecer la politica, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información con el fin de entregar resultados acordes con las politicas y objetivos globales de una organización.
Hacer: Implementar y operar el SGSI	Implementar y operar la politica, los controles, procesos y procedimientos del SGSI
Verificar: hacer seguimiento y revisar el SGSI	Evluar, y, en donde sea apliucable, medir el desempeño del proceso contra la politica y los objetivos de seguridad y la experiencia practica y reportar los resultados a la direccion para su revisión.
Actuar: Mantener y mejorar el SGSI	Emprender acciones correctivas y preventivas con base en los resultados de la auditoria interna del SGSI y la revision por la direccion para lograr la mejora continua.

Figura 3. Descripción del modelo PHVA [17]

Teniendo en cuenta el estudio realizado en el proceso de Gestión de Requerimiento, se determina la planificación del SGSI, basado en la norma ISO/IEC 27001:2013.

Para realizar la planificación del sistema de gestión de seguridad de información (SGSI), para el proceso de Gestión de Requerimientos de la empresa SITIS se plantean los siguientes pasos a seguir y que serán expuestos a lo largo del documento

1. Etapa 1. Definir el alcance para el proceso
2. Etapa 2. Elaborar el inventario e identificación de los activos
3. Etapa 3. Definir una metodología de análisis, evaluación y valoración de riesgos
4. Etapa 4. Identificar amenazas, vulnerabilidades para cada activo
5. Etapa 5. Definir plan de tratamiento de riesgo
6. Etapa 6. Definir la política con todos sus criterios

3. CAPITULO III DESARROLLO DEL PROYECTO

3.1. Alcance del proceso

Se definió el alcance del caso de estudio aplicando la metodología de las Elipses que "es un método que permite identificar los diferentes tipos de activos de información existentes dentro del alcance del modelo y se utiliza como herramienta de identificación de los componentes de cada proceso y las interacciones con otros procesos en la organización y con entidades externas la empresa" [15] al proceso de Gestión de requerimientos. En la figura 2, se visualizan tres elipses: la primera elipse (de adentro hacia afuera) encierra los 5 procedimientos principales que hacen parte del proceso, la segunda elipse encierra todos los procesos internos de SITIS SAS que intervienen en los procedimientos, y la tercera elipse encierra los procesos tercerizados al proceso de Gestión de Requerimientos.

Estructura de procesos:

1. Proceso misional: Gestión de Requerimientos
   - Planeación de producto
   - Diseño
   - Análisis
   - Seguimiento y control de iteración
   - Liberación
2. Procesos de soporte
   - Gestión comercial y de mercadeo

- Gestión de proyectos de operaciones
- Gestión financiera y administrativa
- Gestión humana
- Diseño de Arquitectura del sistema
- Construcción e integración del producto
- Aseguramiento de la calidad
- Gestión de mediciones
- Mejora de procesos

3. Procesos tercerizados
   - Infraestructura

Alcance del SGSI del proceso de Gestión de Requerimientos

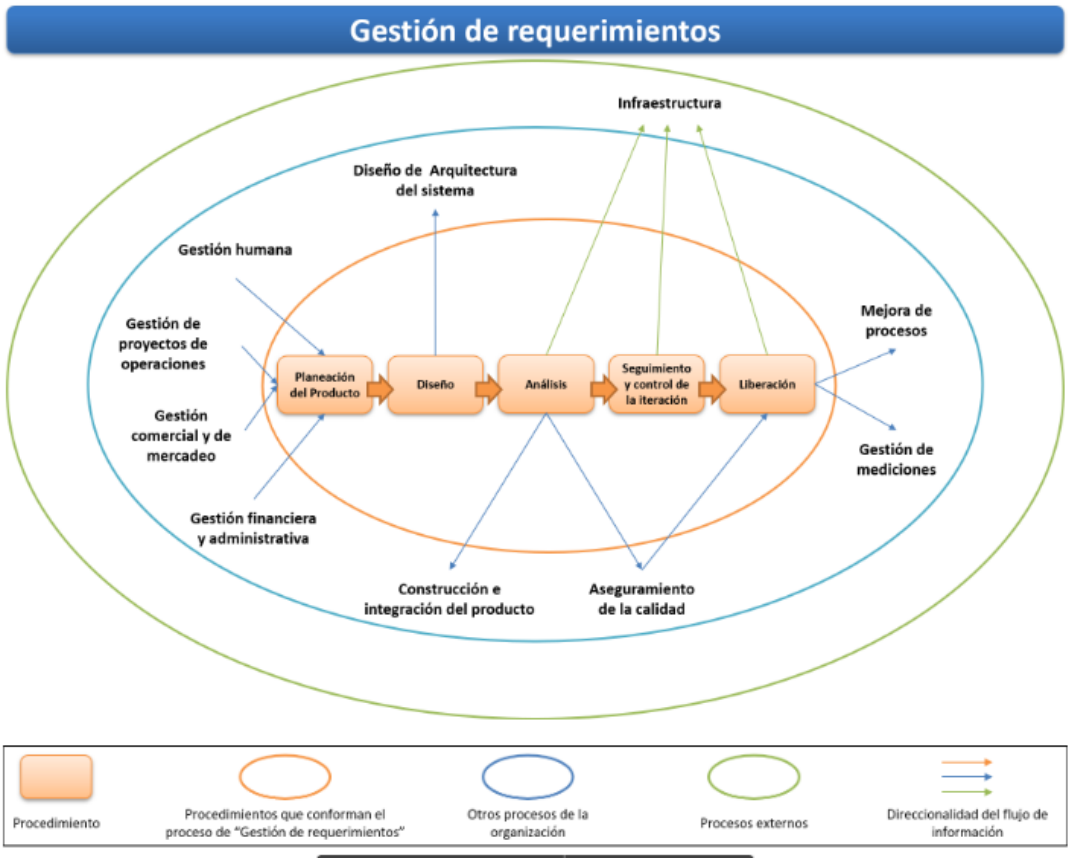

Figura 4. Alcance del proceso de Gestión de Requerimientos
Fuente propia basado en [15]

3.2. Metodología escogida

Una metodología es una guía que se debe seguir para alcanzar el objetivo propuesto, la metodología de tratamientos de riesgos nos permitirá identificar cada uno de los riesgos que se encuentran en el proceso de Gestión de Requerimientos de la empresa SITIS S.A y tendrá un enfoque para la protección de todos los activos identificados.

Para el desarrollo de la propuesta del diseño de la etapa de planificación de un sistema de gestión de seguridad de información del proceso de gestión de requerimientos de la empresa SITIS S.A.S. se utilizará la metodología *Magerit - versión 3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*, por las ventajas que se listan a continuación:

- Conoce de manera de profunda cada uno de los riesgos correspondientes a cada activo que hacen parte de la organización
- Brinda un método sistemático para el análisis de los riegos, que ayudaría a proteger un Sistema de Información.
- Ayuda planificar las medidas oportunas para mantener los riesgos bajo control aplicando la norma ISO 27001
- Ayuda a las Organización en evaluación, auditoría, certificación o acreditación y así se pueda resaltar con su competencia.
- Sensibiliza a los responsables de los sistemas de información de los posibles riesgos existentes aplicando la norma ISO 27001,
- Las salvaguardas permiten de manera oportuna enfrentar los riesgos que se presenten en el activo de la organización.
- Ayuda a proteger cada uno de los activos de las posibles amenazas existentes.
- Permite realizar un análisis y gestión del riesgo, para proteger los activos de vulnerabilidades y amenazas existentes.
- Da un valor asertivo para la representación de los activos de la organización

Actualmente, es importante realizar el análisis de riesgo de seguridad para cada uno de los procesos de la empresa SITIS SAS, para ello se recomienda escoger una metodología que se considere fácil y factible para cada uno de ellos, específicamente para este proyecto nos basamos en la Magerit V3 Libro II Catalogo de elementos para el proceso de *Gestión de Requerimientos*, debido a que esta metodología contiene como complemento un catálogo de SALVAGUARDAS que permiten reducir y proteger cada uno de los riesgos identificados.

3.3. Implementación de la metodología Magerit V3 Libro II Catalogo de elementos

A continuación, haciendo uso del catálogo de elementos de Magerit se describe la metodología de análisis y tratamientos de riesgos aplicado al caso de estudio del proceso de Gestión de Requerimientos de la empresa SITIS SAS, se analiza y se identifican los activos de información y a partir de ellos se procede a detectar las amenazas y vulnerabilidades para poder hacer la gestión de los riesgos encontrados.

3.3.1. Identificación de activos del proceso de Gestión de Requerimientos

Según el contexto de la norma ISO/IEC 27001:2013, un activo de información es “algo que una organización valora y por lo tanto debe proteger”. EL inventario de activos de información basados en la metodología Magerit, es la parte principal para poder empezar a realizar el proyecto de SGSI, debido a que nos permite identificar cada uno de los ellos con sus respetivas características para posteriormente brindar protección a cada uno de los activos por medio de la Gestión de Riesgo.

A continuación, en *Tabla 3. Activos de información* se realiza la identificación de 27 activos de información del proceso “Gestión de Requerimientos” en donde se listan y describen cada uno de los mismos.

Tabla 3. Activos de información

ACTIVO	DESCRIPCION
Alcance funcional	Este documento escrito por el líder de producto y los expertos de dominio define a alto nivel (historias épicas) las necesidades de los interesados y que deberán apuntar a satisfacer una necesidad específica; también permiten al líder de producto evaluar que sean relevantes, alcanzables y finalmente priorizarlas para su implementación.
Casos de uso	Este documento escrito por los analistas funcionales, integra las historias de usuario, mockups, los criterios de aceptación y las reglas de negocio, describe el proceso de atención, los interesados, las condiciones previas que se deberán tener en cuenta y como estas

	apuntan estos requisitos a satisfacer las necesidades en cada paso del proceso. También indica la interacción entre las historias de un componente o con componentes de otros modulo del sistema.
Conceptos Generales (Basados en normas oficiales)	Este documento escrito por el líder de producto y los expertos de dominio definen las fronteras de comportamiento de un módulo del sistema, en aras de cumplir las necesidades funcionales y normativas expresadas por los interesados; describe también la interacción que este módulo y sus componentes tendrá con otros módulos del sistema y entre sus funciones
Conjunto Mínimo de datos básicos	Este documento escrito por el líder de producto y los expertos de dominio define el conjunto de información mínima y básica sobre cada episodio asistencial de cada paciente, en ella se representan las estructuras (tablas) y campos, el tipo, tamaño y obligatoriedad además de una breve descripción y la referencia a catálogos normativos o de operación definidos por el cliente. Son el insumo inicial entregado al proceso de base de datos para el diseño del modelo de datos y en últimas de la base.
Criterios de aceptación	Escritos en conjunto por los expertos de dominio y los analistas funcionales, describen los requisitos funcionales y las condiciones por las cuales se puede dar por hecho la implementación de una historia de usuario. Sirven como insumo inicial para el proceso de testing (pruebas) para la construcción de los casos de prueba. Describen además el comportamiento de algunos elementos del Front END y de algunas validaciones y restricciones que se aplicaran en los formularios sin que sea necesario realizar consultas a la base de datos, por ejemplo, resaltar los campos obligatorios.

Historias de usuario	Escritas en lenguaje natural (común) por los expertos de dominio, representan una necesidad del negocio y cuyo objetivo es la de satisfacer una necesidad expresada por los interesados (requisito); estas historias son escritas siguiendo la estructura definida para representar un escenario del proceso de atención clínica. Constituyen el insumo inicial para la construcción del Backlog del producto.
Plan de Liberación	Es una relación de las versiones que se espera liberar con unas fechas y un alcance funcional propuesto
Prototipos (mockups)	Los Mockups permiten al equipo de Producto representar la arquitectura de la información, su disposición y orden para el registro de los datos en los formularios de captura, además de hacerse una idea muy clara de qué apariencia visual va a tener el producto, y permite a su vez presentar a los interesados y al equipo de desarrollo tener una representación visual de los elementos del formulario y definir patrones de diseño como el color, la tipografía, las sombras, etc.
Reglas de negocio	Escritos en conjunto por los expertos de dominio y los analistas funcionales, describen las validaciones que se implementaran en el BACK END y los mensajes que el sistema presentara para informar, alertar, confirmar alguna acción del sistema. Estas están relacionadas directamente con los criterios de aceptación y las historias de usuario.
Roadmap	Es una planificación del desarrollo de un software con los objetivos a corto y largo plazo.
BIZAGI	Es una suite ofimática con dos productos complementarios, un Modelador de Procesos Bizagi Process Modeler y una Suite de BPM. 2. [22]

KIMAI	Es una aplicación para el registro de tareas y tiempos de código abierto y gratuito. Realiza un seguimiento del tiempo de trabajo e imprime un resumen de sus actividades a pedido. Anual, mensual, diario, por cliente, por proyecto.
Manejador de BD	Un SGBD o DataBase Management System (DBMS) es una recopilación de software orientado al manejo de base de datos, cuya función es servir de interfaz entre la base de datos, el usuario y las distintas aplicaciones utilizadas. [23]
Ofimática	Este es el conjunto de aplicaciones y herramientas informáticas que se utilizan para construir los diferentes artefactos y documentos que se generan en el proceso de Gestión de requerimientos; tales como el paquete de Microsoft Office.
SAR (Sistema de administración de requerimientos)	Es el sistema de Administración de Requerimientos como JIRA o Mantis en el cual reportan cada uno de los requisitos que han sido solicitados por el cliente y que van a ser implementados por el área de desarrollo
Sistema operativo W10	Es la versión del sistema operativo instalado en los equipos de cada uno de los miembros del equipo de producto y análisis.
Laptop de Analista Funcional	Computador ubicado en el área de Producto en el cual es utilizado por el analista funcional
Laptop de Coordinador del área	Computador ubicado en el área de Producto en el cual es utilizado por el coordinador.
Laptop del Experto en dominio	Computador ubicado en el área de Producto en el cual es utilizado por el analista funcional
Router	Dispositivo de hardware que permite la interconexión de los computadores en red.
LAN	Red LAN es utilizada para el uso de la comunicación entre los computadores de la empresa
Analista Funcional	Genera los documentos que permiten detallar los requerimientos solicitados por el cliente.
Coordinador Producto	Prioriza los requerimientos a implementarse.

	Consulta y se asesora para la implementación de requerimientos con equipo consultor. Dirige al equipo de trabajo encargado de documentar la propuesta para dar una solución al requerimiento del cliente.
Experto de dominio	Es un usuario que es especialista y que conoce los procesos de negocio y ayuda a delimitar el alcance funcional de la solución propuesta
Infraestructura	Es el área encargada de la gestión y administración de la comunicación e infraestructura, verificando el correcto funcionamiento de las instalaciones y equipos de la empresa SITIS S.A. Esta área esta tercerizada.
Oficina	Es el lugar destinado al trabajo. En donde se encuentran todos los funcionarios que trabajan en el área de producto y análisis.
Energía Eléctrica	Energía Eléctrica permite tener toda la oficina con iluminación y sus distintos puntos poder conectarlos a los computadores para así poder trabajar

Fuente propia

3.3.2. Clasificación de activos según Magerit

Los tipos de activos se clasifican de acuerdo a la especificación de la *Tabla 4. Clasificación de activos* dada por Magerit:

Tabla 4. Clasificación de activos

[D]	Datos / Información	Los datos son la parte importante en una organización y la información es un activo abstracto que será almacenado en equipos o soportes de información.
[K]	Claves Criptográficas	La criptografía se emplea para proteger el secreto o autenticar a las partes. Las claves criptográficas, combinando secretos e información pública, son esenciales para

		garantizar el funcionamiento de los mecanismos criptográficos
[S]	Servicios	Función que satisface una necesidad de los usuarios (del servicio). Esta sección contempla servicios prestados por el sistema
[SW]	Software- Aplicaciones Informáticas	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.
[HW]	Hardware – Equipamiento Informático	Dícese de 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.
[COM]	Redes de Comunicación	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.
[MEDIA]	Soportes de Información	Se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.
[AUX]	Equipamiento auxiliar	Se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
[L]	Instalaciones	Los lugares donde se hospedan los sistemas de información y comunicaciones.
[P]	Personal	Aparecen las personas relacionadas con los sistemas de información

Fuente Magerit V3 – Catalogo de elementos [6]

3.3.3. Clasificación de activos a partir de Magerit

La tipificación de los activos según la metodología Magerit permite distinguir la importancia de cada activo de información que tiene la empresa SITIS S.A en su proceso Gestión de Requerimientos, para obtener un criterio de identificación de las vulnerabilidades, amenazas y salvaguardas que puede tener cada uno. En Tabla 5. *Clasificación del Inventario de Activos* se discrimina el activo y su ubicación dentro de la empresa.

Tabla 5. Clasificación del Inventario de Activos

Tipo de Activo	Activo	Ubicación
Datos / Información	**[D]** Alcance funcional	Servidor
	[D] casos de uso	Servidor
	[D] Conceptos Generales (Basados en normas oficiales)	Servidor
	[D] Conjunto Mínimo de datos básicos	Servidor
	[D] Criterios de aceptación	Servidor
	[D] Historias de usuario	Servidor
	[D] Plan de Liberación	Servidor
	[D] Prototipos (mockups)	Servidor
	[D] reglas de negocio	Servidor
	[D] Roadmap	Servidor
Software - Aplicaciones informáticas	**[SW]** BIZAGI	PC
	[SW] KIMAI	Servidor
	[SW] Manejador de BD	PC
	[SW] Ofimática	Área de producto
	[SW] SAR (Sistema de administración de requerimientos)	Servidor
	[SW] Sistema operativo W10	Área de producto
Hardware - Equipamiento Informático	**[HW]** Laptop (3)	Área de producto
	[HW] Router	Área de producto
Redes de comunicaciones	**[COM]** LAN	Infraestructura

Equipamiento Auxiliar	**[AUX]** Energía Eléctrica	Empresa
Instalaciones	**[L]** Oficina	Empresa
	[L] Infraestructura	Empresa
Personal	**[P]** Coordinador Producto	Área de producto
	[P] Analista Funcional	Área de producto
	[P] Experto de dominio	Área de producto

Fuente propia

3.3.4. Dimensiones de Valoración

Son las características o atributos que hacen valioso un activo. Una dimensión es una faceta o aspecto de un activo, independiente de otras facetas. Pueden hacerse análisis de riesgos centrados en una única faceta, independientemente de lo que ocurra con otros aspectos. Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión [6]. En la *Tabla 6. Definiciones de Confidencialidad, Integridad y Disponibilidad* se especifican cada una de las dimensiones que se evaluaran.

Tabla 6. Definiciones de Confidencialidad, Integridad y Disponibilidad

(C)	**Confidencialidad**	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]
(I)	**Integridad**	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]
(D)	**Disponibilidad**	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]

Fuente Magerit V3 – Catalogo de elementos [6]

En la *Tabla 7. Criterios para valoración de activos* se describen los valores y criterios que se tendrán en cuenta para la evaluación.

Tabla 7. Criterios para valoración de activos

Valor			Criterio
10	Muy alto	MA	Daño muy grave a la organización
7-9	Alto	A	Daño grave a la organización
4-6	Medio	M	Daño importante a la organización
1-3	Bajo	B	Daño menor a la organización
0	Despreciable	D	Irrelevante a efectos prácticos

Fuente Magerit V3 – Catalogo de elementos [6]

La Tabla 8. Dimensiones de seguridad presenta para este caso las dimensiones que se evaluaran por parte del líder del equipo de producto.

Tabla 8. Dimensiones de seguridad

Dimensiones de seguridad	
[D]	Disponibilidad
[I]	Integridad de los datos
[C]	Confidencialidad de los datos

Fuente Magerit V3 – Catalogo de elementos [6]

3.3.5. Valoración de activos dependencia de información

A continuación, en la *Tabla 9. Valoración de dependencias activos de información*, se realiza la valoración por parte del líder de área de producto de las dimensiones de cada uno de los activos de información del proceso de Gestión de Requerimientos de acuerdo a la confidencialidad, la integridad y la disponibilidad.

Tabla 9. Valoración de dependencias activos de información

		Dimensiones de Seguridad		
Tipo de Activo	**Activo**	**C**	**I**	**D**
Datos / Información	**[D]** Conceptos Generales	5	6	5
	[D] Alcance funcional	5	6	5
	[D] Prototipos (mockups)	10	10	8
	[D] Conjunto Mínimo de datos básicos	9	7	7
	[D] Historias de usuario	10	10	8
	[D] Criterios de aceptación	6	6	6
	[D] reglas de negocio	6	6	6
	[D] casos de uso	10	10	8
	[D] Roadmap	6	4	6
	[D] Plan de Liberación	3	2	3
Software - Aplicaciones informáticas	**[SW]** Sistema operativo W10	5	5	5
	[SW] Ofimática	5	5	5
	[SW] KIMAI	0	0	0
	[SW] MANTIZ	0	0	0
	[SW] BIZAGI	3	2	2
	[SW] Manejador de BD	3	2	3
Hardware - Equipamiento Informático	**[HW]** Laptop	0	0	0
	[HW] Laptop	0	0	0
	[HW] Router	0	0	0
Redes de comunicaciones	**[COM]** LAN	0	0	0
Equipamiento Auxiliar	**[AUX]** Energía Eléctrica	0	0	0
Instalaciones	**[L]** Oficina	5	5	4
	[L] Infraestructura	5	5	4
Personal	**[P]** Coordinador Producto	3	3	3
	[P] Analista Funcional	6	4	6
	[P] Experto de dominio	6	4	6

Fuente propia

3.4. Identificación de amenazas

Las amenazas son toda acción que se beneficia de una vulnerabilidad para violentar contra la seguridad de un sistema de información, estos incidentes pueden generar daño a la organización causando pérdidas materiales, por lo cual es importante identificarlas para hallar un posible tratamiento y evitar los riesgos que puedan ocurrir.

A continuación, se presentan las descripciones en la *Tabla 10. Categorización de las amenazas* del catálogo de amenazas de Magerit sobre los activos de un sistema de información, que son el grupo de diferentes tipos de amenazas que se encuentran en la vida cotidiana, cada uno de ellos los podemos encontrar en la metodología de Magerit Versión 3, Libro 2 Catalogo de elementos.

Tabla 10. Categorización de las amenazas

Código	Nombre	Descripción	Origen
[N]	Desastres Naturales	Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.	Natural (accidental)
[I]	Origen Industrial	Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.	Industrial
[E]	Errores y fallos no intencionados	Fallos no intencionales causados por las personas. La numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto	Humano (accidental)
[A]	Ataques Intencionados	Fallos deliberados causados por las personas. La numeración no es consecutiva para coordinarla con los errores no intencionados, muchas veces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto	Humano (deliberado)

Fuente Magerit V3 – Catalogo de elementos [6]

Teniendo en cuenta la descripción anterior, se relaciona continuación el grupo de amenazas mencionados en cada categorización.

- **[N] Desastres naturales**
  - [N.1] Fuego
  - [N.2] Daños por agua
  - [N.*] Desastres naturales

- **[I] Origen industrial**
  - [I.1] Fuego
  - [I.2] Daños por agua
  - [I.*] Desastres industriales
  - [I.3] Contaminación mecánica
  - [I.4] Contaminación electromagnética
  - [I.5] Avería de origen físico o lógico
  - [I.6] Corte del suministro eléctrico
  - [I.7] Condiciones inadecuadas de temperatura o humedad
  - [I.8] Fallo de servicios de comunicaciones
  - [I.9] Interrupción de otros servicios y suministros esenciales
  - [I.10] Degradación de los soportes de almacenamiento de la información
  - [I.11] Emanaciones electromagnéticas

- **[E] Errores y fallos no intencionados**
  - [E.1] Errores de los usuarios
  - [E.2] Errores del administrador
  - [E.3] Errores de monitorización (log)
  - [E.4] Errores de configuración
  - [E.7] Deficiencias en la organización
  - [E.8] Difusión de software dañino
  - [E.9] Errores de [re-]encaminamiento
  - [E.10] Errores de secuencia
  - [E.14] Escapes de información
  - [E.15] Alteración accidental de la información
  - [E.18] Destrucción de información
  - [E.19] Fugas de información
  - [E.20] Vulnerabilidades de los programas (software)

- [E.21] Errores de mantenimiento / actualización de programas (software)
- [E.23] Errores de mantenimiento / actualización de equipos (hardware)
- [E.24] Caída del sistema por agotamiento de recursos
- [E.25] Pérdida de equipos
- [E.28] Indisponibilidad del personal

❖ **[A] Ataques intencionados**

- [A.3] Manipulación de los registros de actividad (log)
- [A.4] Manipulación de la configuración
- [A.5] Suplantación de la identidad del usuario
- [A.6] Abuso de privilegios de acceso
- [A.7] Uso no previsto
- [A.8] Difusión de software dañino
- [A.9] [Re-]encaminamiento de mensajes
- [A.10] Alteración de secuencia
- [A.11] Acceso no autorizado
- [A.12] Análisis de tráfico
- [A.13] Repudio
- [A.14] Interceptación de información (escucha)
- [A.15] Modificación deliberada de la información
- [A.18] Destrucción de información
- [A.19] Divulgación de información
- [A.22] Manipulación de programas
- [A.23] Manipulación de los equipos
- [A.24] Denegación de servicio
- [A.25] Robo
- [A.26] Ataque destructivo
- [A.27] Ocupación enemiga
- [A.28] Indisponibilidad del personal
- [A.29] Extorsión
- [A.30] Ingeniería social (picaresca)

Teniendo en cuenta esta lista de amenazas se deben documentar las que se consideran pueden afectar a cualquier activo identificado en el proceso de Gestión de Requerimientos.

3.4.1. Identificación de amenazas del proceso de Gestión de Requerimientos

Teniendo en cuenta la identificación de los activos del proceso de Gestión de Requerimiento, es importante analizar cada uno de ellos y poder determinar las amenazas que pueden ocurrir y causar algún tipo de daño, que pueda perjudicar el entorno laboral.

Por medio de la presente *Tabla 11. Identificación de amenazas*, se realiza la identificación de amenazas para el activo *Casos de uso*, según lo expresado por el libro II del catálogo de amenazas posibles de la metodología MAGERIT. Para ver las amenazas de los otros activos ver el Anexo 02 - Identificación de Amenazas

Tabla 11. Identificación de amenazas

ACTIVO	**Amenazas**			
	[N] Desastres naturales	**De origen industrial [I]**	**Errores y fallos no intencionados [E]**	**[A] Ataques intencionados**
Casos de uso			[E.15] Alteración accidental de la información [E.18] Destrucción de información [E.19] Fugas de información	[A.5] Suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado [A.15] Modificación deliberada de la información [A.18] Destrucción de información [A.19] Divulgación de información

Fuente propia

3.5. Análisis de riesgos

Una vez los activos de información han sido clasificados y se ha identificado las respectivas amenazas que los pueden afectar, se debe establecer que vulnerabilidades pueden impactar al activo mediante la materialización de una amenaza. Posteriormente se realiza la evaluación del riesgo cuantitativa y cualitativamente, teniendo en cuenta el

impacto por la probabilidad de suceso y finalmente se realiza la identificación de las salvaguardas para los activos.

3.6. Identificación de vulnerabilidades y riesgos por amenaza

Posteriormente a la identificación de amenazas por activos, se realiza identifican las vulnerabilidades que son las “debilidades de un activo o control que puede ser explotada por una o más amenazas” [24], estas debilidades son las que pueden causar que las amenazas tengan altas probabilidades de ocurrencia e impacto que provoquen incidentes de seguridad; de igual manera se describen los riesgos que son el “efecto en la incertidumbre del objetivo” [24]. A continuación, se describen en la *Tabla 12. la Identificación de vulnerabilidades y riesgos por amenaza* específicamente para el activo “Caso de uso”.
Para ver las valoraciones y riesgos de los demás activos de información ver el Anexo 03 - Identificación de vulnerabilidades y riesgos por amenaza

Tabla 12. Identificación de vulnerabilidades y riesgos por amenaza – Casos de uso

Tipo	Activo	Descripción	Vulnerabilidad	Amenaza	Riesgo
Datos / Información	Casos de uso	Este documento escrito por los analistas funcionales, integra las historias de usuario, mockups, los criterios de aceptación y las reglas de negocio, describe el proceso de atención, los interesados, las condiciones previas que se deberán tener en	[E.15] Carencia en el ingreso y modificaciones en la información	[E.15] Alteración accidental de la información	Perdida de información desarrollada durante la actividad del funcionario
			[E.18] Falta de herramientas lógicas para la protección de hardware y software de la empresa	[E.18] Destrucción de información	Información errónea y accidental lo cual puede ocasionar confusión y malos entendidos en el proceso, pérdida de confianza con la documentación
			[E.19] Inseguridad en la información con fácil acceso	[E.19] Fugas de información	Daño o Perdida de la información confidencial dentro del proceso
			[A.5] Falta de control en la asignación de usuarios	[A.5] Suplantación de la identidad del usuario	Modificaciones injustificadas a información confidencial de la empresa

		cuenta y como estas apuntan estos requisitos a satisfacer las necesidades en cada paso del proceso. También indica la interacción entre las historias de un componente o con componentes de otros modulo del sistema.	[A.6] Falta de control de los privilegios otorgados	[A.6] Abuso de privilegios de acceso	Modificaciones injustificadas a información confidencial de la empresa con beneficio propio
			[A.11] Fácil acceso, usuario sin contraseña	[A.11] Acceso no autorizado	Perdida de información confidencial, alteración en interfaz del usuario y base de datos, y destrucción de documentos.
			[A.15] Información inseguridad con fácil acceso	[A.15] Modificación deliberada de la información	Alteración en la interfaz del usuario, caída constante por manipulación, caída, virus con facilidad de acceso y daño de la información
			[A.18] Falta de backups en la información	[A.18] Destrucción de información	Retraso en las actividades laborales. Perdida de información confidencial, daños en la documentación
			[A.19] Información insegura con fácil acceso	[A.19] Divulgación de información	Destrucción de la información y perdida de documentación confidencial

Fuente propia

3.7. Evaluación y valoración de riesgo

3.7.1. Identificación del riesgo potencial

Este proceso se realiza para encontrar, enumerar y caracterizar los elementos de riesgo de cada uno de los activos de información del proceso de Gestión de Riesgos, para esto es necesario conocer los niveles de impacto y probabilidad de ocurrencia de una vulnerabilidad.

3.7.2. Escala de valoración del impacto

El impacto según la norma ISO 27001 es el “Cambio adverso en el nivel de los objetivos del negocio logrados” [24] o es la consecuencia de la materialización de una amenaza que se da cuando un activo tiene un estado y posterior a la ejecución de la amenaza cambia ese estado. En la *Tabla 13. Nivel de Impacto*, presenta la nomenclatura, la categoría y la valoración que será utilizada para evaluar más adelante el nivel de riesgo.

Tabla 13. Nivel de Impacto

IMPACTO		
Nomenclatura	**Categoría**	**Valoración**
MA	Muy Alto	5
A	Alto	4
M	Medio	3
B	Bajo	2
MB	Muy Bajo	1

Fuente propia

3.7.3. Escala de valoración de probabilidad

Teniendo en cuenta que la probabilidad es la “posibilidad de que algo suceda, frecuencia o factibilidad de ocurrencia del riesgo” [24], la *Tabla 14. Nivel de Probabilidad* contiene la nomenclatura, categoría y valoración que se utilizara para calcular el nivel del riesgo.

Tabla 14. Nivel de Probabilidad

PROBABILIDAD		
Nomenclatura	**Categoría**	**Valoración**
MA	Prácticamente seguro	5
A	Probable	4
M	Posible	3
B	Poco probable	2
MB	Muy raro	1

Fuente propia

3.7.4. Valoración del riesgo potencial con la relación Impacto – Probabilidad

Teniendo en cuenta las escalas de valoración del Impacto y la Probabilidad para conocer el valor del riesgo, se realiza mediante la siguiente formula:

Riesgo = Impacto * probabilidad

El riesgo es la valoración del Impacto de la ejecución de una amenaza y la probabilidad de ocurrencia de dicha amenaza producto de la explotación de una vulnerabilidad.

3.7.5. Matriz de riesgo potencial (Mapa de Calor)

Por medio de esta herramienta de visualización de datos se comunica la valoración y priorizan los riesgos a los que está expuesta la organización, generado del producto entre el nivel de probabilidad y el nivel de impacto, obteniendo al final la matriz denominada "Matriz de riesgo potencial" que se puede visualizar en la *Tabla 15. Matriz de riesgo potencial*, la cual se utiliza para dar el valor del riesgo.

Tabla 15. Matriz de riesgo potencial

Impacto	**MA**	5	10	15	20	25
	A	4	8	12	16	20
	M	3	6	9	12	15
	B	2	4	6	8	10
	MB	1	2	3	4	5
RIESGO		**MB**	**B**	**M**	**A**	**MA**
		Probabilidad				

Fuente propia

En la *Tabla 16. Nivel de riesgo* se da la categoría y nomenclatura dependiendo del rango sobre el cual está el valor del riesgo.

Tabla 16. Nivel de riesgo

Nivel del Riesgo		
Nomenclatura	**Categoría**	**Valoración**
MA	Critico	21 – 25
A	Importante	16 – 20
M	Apreciable	10 – 15
B	Bajo	5 – 9
MB	Despreciable	1 – 4

Fuente propia

3.7.6. Valoración de riesgos sobre los activos

En esta etapa se realiza la valoración de la probabilidad y el impacto de cada riesgo por parte del líder del área de producto con cada activo de información del proceso de Gestión de Requerimientos, en la *Tabla 17. Valoración de riesgo del activo Casos de Uso* se evidencia como ejemplo el resultado la valoración y el nivel de riesgo, para ver la valoración de los otros activos ver el Anexo 04 - Valoración de riesgos

Tabla 17. Valoración de riesgo del activo Casos de Uso

					VALORACION DEL RIESGO			
Tipo	**Activo**	**Vulnerabilidad**	**Amenaza**	**Riesgo**	**Probabilidad**	**Impacto**	**Valoración**	**Nivel de Riesgo**
Datos / Información	Casos de uso	[E.15] Carencia en el ingreso y modificaciones en la información	[E.15] Alteración accidental de la información	Perdida de información desarrollada durante la actividad del funcionario	**2**	**2**	**4**	**MB**
		[E.18] Falta de herramientas lógicas para la protección de hardware y software de la empresa	[E.18] Destrucción de información	Información errónea y accidental lo cual puede ocasionar confusión y malos entendidos en el proceso, pérdida de	**2**	**4**	**8**	**B**

				confianza con la documentación				
		[E.19] Inseguridad en la información con fácil acceso	[E.19] Fugas de informaci ón	Daño o Perdida de la información confidencial dentro del proceso	**4**	**4**	**16**	**A**
		[A.5] Falta de control en la asignación de usuarios	[A.5] Suplantac ión de la identidad del usuario	Modificaciones injustificadas a información confidencial de la empresa	1	1	1	**MB**
		[A.6] Falta de control de los privilegios otorgados	[A.6] Abuso de privilegios de acceso	Modificaciones injustificadas a información confidencial de la empresa con beneficio propio	1	1	1	**MB**
		[A.11] Fácil acceso, usuario sin contraseña	[A.11] Acceso no autorizad o	Perdida de información confidencial, alteración en interfaz del usuario y base de datos, y destrucción de documentos.	1	1	1	**MB**
		[A.15] Información inseguridad con fácil acceso	[A.15] Modificaci ón deliberad a de la informaci ón	Alteración en la interfaz del usuario, caída constante por manipulación, caída, virus con facilidad de acceso y daño de la información	1	1	1	**MB**
		[A.18] Falta de backups en la información	[A.18] Destrucci ón de informaci ón	Retraso en las actividades laborales. Perdida de información confidencial, daños en la documentación	3	4	12	**M**
		[A.19] Información insegura con fácil acceso	[A.19] Divulgaci ón de informaci ón	Destrucción de la información y perdida de documentación confidencial	5	5	25	**MA**

Fuente propia

3.7.7. Gráfica de categorización de los activos

Los resultados obtenidos en la *Figura 5. Activos de información por categoría* indican la valoración del riesgo en base a los activos de la empresa, en donde contamos con 3 activos (Prototipos Mockups, Historias de Usuario, Casos de Uso) con una alta probabilidad de riesgo **CRÍTICO**, 1 activo (Conjunto mínimo de datos básicos) con una probabilidad de riesgo **IMPORTANTE**, y 14 activos (Conceptos Generales (Basados en normas oficiales), Alcance Funcional, Criterios de Aceptación, Reglas de Negocio, Roadmap, Sistema Operativo W10, Ofimática, Bizagi, Laptop de Coordinador del área , Laptop del Experto en dominio, Laptop de Analista Funcional, Oficina e Infraestructura, Infraestructura, Energía Eléctrica) que se encuentran en una probabilidad de riesgos **APRECIABLE**, dejando un alto impacto en la empresa, en el cual se deben tomar acciones apropiadas para poder mitigar cada riesgo que perjudique la funcionalidad de la empresa, y también contamos con 4 activos (Plan de liberación, SAR (Sistema de administración de requerimientos), Manejador de Base de datos, Coordinador de producto) con una probabilidad BAJA y 5 activos (KMAI, Router, LAN, Analista Funcional, Experto en Dominio) con un probabilidad de un nivel muy **DESPRECIABLES**, que a pesar que no se consideran un algo de riesgo, deben tener la protección adecuada con toda la información confidencial, íntegro y disponible tanto para los usuarios como para los que operan dentro de la empresa.

Categorización de los activos

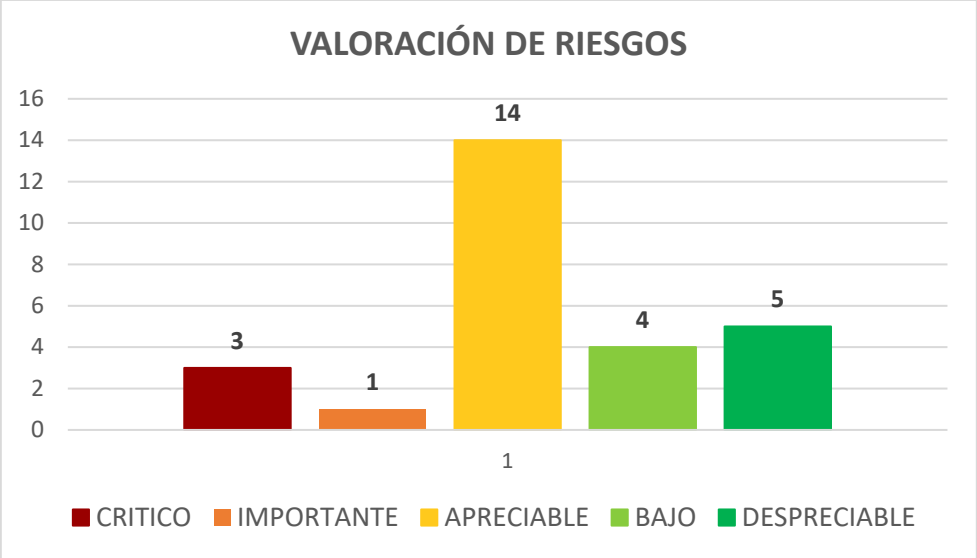

Figura 5. Activos de información por categoría
Fuente propia

3.8. Salvaguardas

Las salvaguardas permiten enfrentar amenazas que se encuentran en cada activo del proceso estudiado, en el cual Magerit nos presenta un catálogo de Salvaguardas que nos ayudan como guía en la implementación de los sistemas de información.

Basados en la metodología Magerit, encontramos la categorización de las Salvaguardas, que serán aplicadas en el proyecto con el fin de reducir y proteger cada uno de los activos de los riesgos encontrados y por ende nos ayudara a tener una continuidad en el negocio.

Categorización de salvaguardas

1. **Protecciones generales u horizontales**
   - H Protecciones Generales
2. **Protección de los datos / información**
   - D Protección de la Información
3. **Protección de las claves criptográficas**
   - K Gestión de claves criptográficas
4. **Protección de los servicios**
   - S Protección de los Servicios
5. **Protección de las aplicaciones (software)**
   - SW Protección de las Aplicaciones Informáticas
6. **Protección de los equipos (hardware)**
   - HW Protección de los Equipos Informáticos
7. **Protección de las comunicaciones**
   - COM Protección de las Comunicaciones
8. **Protección en los puntos de interconexión con otros sistemas**
   - IP Puntos de interconexión: conexiones entre zonas de confianza
9. **Protección de los soportes de información**
   - MP Protección de los Soportes de Información
10. **Protección de los elementos auxiliares**
    - AUX Elementos Auxiliares
11. **Seguridad física**
    - L Protección de las instalaciones Protección de las Instalaciones
12. **Salvaguardas relativas al personal**

Son aquellas que se refieren a las personas que tienen relación con el sistema de información.

- PS Gestión del Personal

13. Salvaguardas de tipo organizativo

Son aquellas que se refieren al buen gobierno de la seguridad.

- G Organización

14. Continuidad de operaciones

Prevención y reacción frente a desastres.

- BC Continuidad del negocio

15. Externalización

Es cada vez más flexible la frontera entre los servicios de seguridad prestados internamente y los servicios contratados a terceras partes.

- E Relaciones Externas

16. Adquisición y desarrollo

- NEW Adquisición / desarrollo

3.8.1. Identificación de salvaguardas

Según la metodología Magerit libro II, Catalogo de elementos, las salvaguardas están definidas para reducir el riesgo y proteger los activos de información de las amenazas existentes, teniendo en cuenta la identificación de las amenazas que son las que explotan una vulnerabilidad y se consideran como la debilidad del activo, se realiza la identificación en la *Tabla 18. Salvaguarda – Casos de uso* de la protección que se aplicara para disminuir el riesgo.

Para ver las salvaguardas de cada activo, revisar el Anexo 05 – Salvaguardas.

Tabla 18. Salvaguarda – Casos de uso

Tipo	Activo	Descripción	Vulnerabilidad	Amenaza	Riesgo	Salvaguarda
Datos / Información	Casos de uso	Este documento escrito por los analistas funcionales, integra las historias de usuario, mockups, los	[E.15] Carencia en el ingreso y modificaciones en la información	[E.15] Alteración accidental de la información	Perdida de información desarrollada durante la actividad del funcionario	D Protección de la Información D.A Copias de seguridad de los datos (backup)

		criterios de aceptación y las reglas de negocio, describe el proceso de atención, los interesados, las condiciones previas que se deberán tener en cuenta y como estas apuntan estos requisitos a satisfacer las necesidades en cada paso del proceso. También indica la interacción entre las historias de un componente o con componentes de otros modulo del sistema.				D.I Aseguramiento de la integridad D.C Cifrado de la información
			[E.18] Falta de herramientas lógicas para la protección de hardware y software de la empresa	[E.18] Destrucción de información	Información errónea y accidental lo cual puede ocasionar confusión y malos entendidos en el proceso, pérdida de confianza con la documentación	D Protección de la Información D.A Copias de seguridad de los datos (backup) D.I Aseguramiento de la integridad D.C Cifrado de la información
			[E.19] Inseguridad en la información con fácil acceso	[E.19] Fugas de información	Daño o Perdida de la información confidencial dentro del proceso	D Protección de la Información D.A Copias de seguridad de los datos (backup) D.I Aseguramiento de la integridad D.C Cifrado de la información
			[A.5] Falta de control en la asignación de usuarios	[A.5] Suplantación de la identidad del usuario	Modificaciones injustificadas a información confidencial de la empresa	D Protección de la Información D.A Copias de seguridad de los datos (backup) D.I Aseguramient

						o de la integridad D.C Cifrado de la información
			[A.6] Falta de control de los privilegios otorgados	[A.6] Abuso de privilegios de acceso	Modificaciones injustificadas a información confidencial de la empresa con beneficio propio	D Protección de la Información D.A Copias de seguridad de los datos (backup) D.I Aseguramiento de la integridad D.C Cifrado de la información
			[A.11] Fácil acceso, usuario sin contraseña	[A.11] Acceso no autorizado	Perdida de información confidencial, alteración en interfaz del usuario y base de datos, y destrucción de documentos.	D Protección de la Información D.A Copias de seguridad de los datos (backup) D.I Aseguramiento de la integridad D.C Cifrado de la información
			[A.15] Información inseguridad con fácil acceso	[A.15] Modificación deliberada de la información	Alteración en la interfaz del usuario, caída constante por manipulación, caída, virus con facilidad de acceso y daño de la información	D Protección de la Información D.A Copias de seguridad de los datos (backup) D.I Aseguramiento de la integridad

						D.C Cifrado de la información
			[A.18] Falta de backups en la información	[A.18] Destrucción de información	Retraso en las actividades laborales. Perdida de información confidencial, daños en la documentación	D.A Copias de seguridad de los datos (backup) D.C Cifrado de la información
			[A.19] Información insegura con fácil acceso	[A.19] Divulgación de información	Destrucción de la información y perdida de documentación confidencial	D Protección de la Información D.I Aseguramiento de la integridad

Fuente propia

3.9. Plan de tratamiento de riesgo

Previo al desarrollo del plan de tratamiento se diligencia la Declaración de Aplicabilidad (SoA por las siglas en inglés de Statement of Applicability), este es un requisito del estándar ISO/IEC 27001, que se realiza para llevar el registro de los controles que son aplicados en la organización para mantener la seguridad de la información.

En el Anexo 06 - SOA Declaración de aplicabilidad, se desarrolla la validación que se realiza junto con los encargados del área asignados por la empresa, se evidencia la aplicación a media de políticas como copias de seguridad y de controles que son de importancia para la protección de la información del proceso. A partir de este documento se inicia con el desarrollo del plan de tratamiento.

El objetivo del Plan de Tratamiento de Riesgos es mitigar los riesgos detectados en el análisis de riesgos, ya sea en la perdida de la Confidencialidad, Integridad o de Disponibilidad de los activos de información evitando la presencia de incidencias que afecten los logros de los objetivos de la organización. Existen 4 opciones para tratar el riesgo las cuales son:

- **Aceptar**: La organización decide no realizar acciones para mitigar los riesgos y se aceptan.
- **Mitigar**: Implementar Controles Anexo A para reducir el riesgo.
- **Evitar o Eliminar**: Identificar la condición que genera el riesgo y dejar de hacerla.
- **Transferir**: Se delega la acción para mitigar a través de pólizas o de terceros.

A continuación, se visualiza en la *Tabla 19. Plan de tratamiento – Casos de uso* donde se propone el tratamiento de los riesgos en el cual se evalúan las posibles acciones que se pueden adoptar para mitigar por cada riesgo detectado, en este activo específicamente. Para ver el tratamiento de los riesgos de los demás activos de información ver el Anexo 07 - Plan de Tratamiento de Riesgo.

Los siguientes controles de la norma ISO/EIC 27001:2013 se definen a partir de la información arrojada por el análisis de riesgos, el cual brindó información acerca de las necesidades del Proceso de Gestión de requerimientos en cuanto a la seguridad de la información y las actividades que debe desarrollar la empresa para dar tratamiento a los riesgos de nivel Apreciable, Importante y Crítico.

Tabla 19. Plan de tratamiento – Casos de uso

					VALORACION DE RIESGO				PLAN DE TRATAMIENTO DE RIESGO			
Tipo	**Activo**	**Vulnerabilidad**	**Amenaza**	**Riesgo**	**Probabilidad**	**Impacto**	**Valoración**	**Nivel de riesgo**	**Tratamiento**	**Control ISO 27002:2013**	**Justificación**	**Actividades**
Datos / Información	Casos de uso	[E.15] Carencia en el ingreso y modificaciones en la información	[E.15] Alteración accidental de la información	Pérdida de información desarrollada durante las actividades del funcionario	**2**	**2**	**4**	**MB**	**Mitigar**	**A.12.3.1**	Se deben hacer copias de respaldo de la documentación, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada, de esta manera evitar perdida de información confidencial	

		[E.18] Falta de herramientas lógicas para la protección de hardware y software de la empresa	[E.18] Destrucción de información	Información errónea y accidental lo cual puede ocasionar confusión y malos entendidos en el proceso, pérdida de confianza con la documentación	**2**	**4**	**8**	**B**	**Mitigar**	**A.12.3.1**	Se deben hacer copias de respaldo de la documentación, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada, de esta manera evitar perdida de información confidencial	

		[E.19] Inseguridad en la información con fácil acceso	[E.19] Fugas de información	Daño o Perdida de la información confidencial dentro del proceso	**4**	**4**	**16**	**A**	**Mitigar**	**A.8.3.1**	Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización	1. Se debe generar y documentar el procedimiento específico para el manejo adecuado de los medios removibles 2. Si se tiene acceso a medios removibles se debe garantizar que el empleado conozca el manejo de la información según la clasificación de la información 3. Garantizar que la información almacenada en el medio removible cuente con los backups necesarios para evitar la pérdida de la información 4. si la información de almacenada es confidencial debe tener protección criptográfica
									Mitigar	**A.8.3.3**	Previo a la transferencia de un medio, exigir la protección acorde con la clasificación de la información que esta almacenada en el dispositivo. Si la información es confidencial se debe proteger la información con algún medio de encriptación	1. Al momento de transportar la información por parte de algún empleado, se debe garantizar el embalaje correcto para la protección del medio físico 2. Llevar el registro con la identificación del contenido de los medios, la protección que se aplica y responsables
									Mitigar	**A.12.6.2**	Se debe implementar una política para el control de la instalación de software por parte de los usuarios. De esta manera se vigila el ingreso de vulnerabilidades que conlleven a incidentes de la seguridad de la información	1, Definir una política estricta que establezca las reglas de instalación del software por parte de los empleados 2. Validar los privilegios que tienen los usuarios 3. hacer cumplir la política por medio de revisiones y capacitaciones al personal

		[A.5] Falta de control en la asignación de usuarios	[A.5] Suplantación de la identidad del usuario	Modificaciones injustificadas a información confidencial de la empresa	**1**	**1**	**1**	**MB**	**Mitigar**	**A.12.3.1**	Se deberían hacer copias de respaldo de la documentación, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada, de esta manera evitar perdida de información confidencial	
									Mitigar	**A.13.2.1**	Se debe implementar una política, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación	
		[A.6] Falta de control de los privilegios otorgados	[A.6] Abuso de privilegios de acceso	Modificaciones injustificadas a información confidencial de la empresa con beneficio propio	**1**	**1**	**1**	**MB**	**Mitigar**	**A.9.1.1**	Se debe realizar la implementación de la política para control de acceso con base en los requisitos del negocio y de seguridad de la información	
									Mitigar	**A.9.2.5**	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios periódicamente	

		[A.11] Fácil acceso, usuario sin contraseña	[A.11] Acceso no autorizado	Perdida de información confidencial, alteración en interfaz del usuario y base de datos, y destrucción de documentos.	**4**	**4**	**4**	**4**	**Mitigar**	**A.11.2.9**	Una política de escritorio limpio y pantalla limpia teniendo en cuenta las clasificaciones de información, reduce los riesgos de acceso no autorizado, y pérdida y daño de información durante y por fuera de las horas laborales normales	1. Implementación de la política de escritorio limpio y pantalla limpia 2. Discriminar información sensible o crítica del negocio tanto en el escritorio, como en el puesto de trabajo 3. cuando están desatendidos, los computadores y terminales se deberían dejar fuera del sistema o proteger con un sistema de bloqueo de la pantalla y el teclado
									Mitigar	**A.6.2.2**	Implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo	En caso de que la organización adopte la modalidad de Teletrabajo o siga con modalidad de trabajo en casa se debe tener en cuenta la política de seguridad, por ejemplo: 1. Seguridad física en el sitio de teletrabajo tanto seguridad de la edificación como del entorno local 2. requisitos de seguridad de las comunicaciones 3. suministro de acceso al escritorio virtual, que impide el procesamiento y almacenamiento de información en equipo de propiedad privada 4. protección de amenaza de acceso no autorizado a información o a recursos, por parte de otras personas que usan el mismo alojamiento, por ejemplo, familia y amigos 5. uso de redes domésticas y requisitos o restricciones sobre la configuración de servicios de red inalámbrica 6. requisitos de firewall y de protección contra software malicioso

		[A.15] Información inseguridad con fácil acceso	[A.15] Modificación deliberada de la información	Alteración en la interfaz del usuario, caída constante por manipulación, caída, virus con facilidad de acceso y daño de la información	**1**	**1**	**1**	**MB**	**Mitigar**	**A.12.3.1**	Se deben hacer copias de respaldo de la documentación, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada, de esta manera evitar perdida de información confidencial	
		[A.18] Falta de backups en la información	[A.18] Destrucción de información	Retraso en las actividades laborales. Perdida de información	**3**	**4**	**12**	**M**	**Mitigar**	**A.12.3.1**	Se deben hacer copias de respaldo de la documentación, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada, de esta manera evitar perdida de información confidencial	Para este caso la organización tiene implementada la política para copias de seguridad, pero se recomienda hacer la respectiva validación de ellas y verificar su correcto funcionamiento, ya que hasta el momento de hacer el análisis no se encuentra registro de esta actividad

				confidencial, daños en la documentación					**Mitigar**	**A.13.2.1**	Se debe implementar una política, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación. los procedimientos deben ser diseñados para proteger la información transferida contra interceptación, copiado, modificación, enrutado y destrucción	1. Diseñar e implementar la política de procedimientos de transferencia de información a través de la cual se busca la definición de reglas que protejan la información transferida contra interceptación, copiado, modificación, enrutado y destrucción, mediante el uso de varios tipos diferentes de instalaciones de comunicación, incluido el correo electrónico, voz, fax y video 2. Brindar asesoría al personal para que tome las precauciones apropiadas acerca de no revelar información confidencial
		[A.19] Información insegura con fácil acceso	[A.19] Divulgación de información	Destrucción de la información y perdida de documentación confidencial	**5**	**5**	**25**	MA	**Mitigar**	**A.8.2.1**	La clasificación brinda a las personas que tratan con información, una indicación concisa de cómo manejarla y protegerla	1. Realizar la clasificación de la información de pendiendo de las necesidades del negocio dependiendo del intercambio, restricción o requisitos legales 2. Dar un nombre a cada nivel que tenga sentido en el contexto de la aplicación del esquema de clasificación, por ejemplo: * Confidencial: acceso restringido a la alta dirección. * Restringido: Coordinadores de área y empleados que tienen clave de acceso. * Interno: Información accesible solo a los miembros de la organización, pero en cualquier nivel. * Público: Todas las personas, dentro y fuera de la organización pueden tener acceso.

									Mitigar	**A.13.2.1**	Se debe implementar una política, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación	1. Diseñar e implementar la política de procedimientos de transferencia de información a través de la cual se busca la definición de reglas que protejan la información transferida contra interceptación, copiado, modificación, enrutado y destrucción, mediante el uso de varios tipos diferentes de instalaciones de comunicación, incluido el correo electrónico, voz, fax y video 2. Brindar asesoría al personal para que tome las precauciones apropiadas acerca de no revelar información confidencial
									Mitigar	**A.13.2.4**	Se deben implementar acuerdos de confidencialidad y de no divulgación para proteger la información de la Organización. Estos informan a los firmantes acerca de su responsabilidad para proteger, usar y divulgar información de una manera autorizada y responsable	1. a pesar de que la organización cuenta con la firma de acuerdos de confidencialidad, se debe garantizar de que los empleados lean y entiendan lo consignado en los documentos, de esta manera se concientiza de la gravedad del cumplimiento de las misma.

Fuente propia

3.10. Resultado: política de seguridad

Como resultado de todo el análisis de riesgo que se realizó al proceso de Gestión de Requerimientos de la empresa SITIS S.A, se propone una política de Escritorio y Pantalla Limpia con el fin de prevenir y reducir riesgos encontrados y de muy fácil aplicabilidad, en el cual aplica para la protección de los activos de información identificados.

Ver Anexo 08 – Política de seguridad de escritorio y pantalla limpia

Esta política se establece con el fin de prevenir el acceso no autorizado, daño o pérdida de información que se encuentra en los puestos de trabajo, computadores, medios removibles y demás dispositivos asignados por la empresa, durante y fuera del horario laboral de los empleados del proceso de Gestión de Requerimientos.

Adicional se realiza la entrega de la Política general de seguridad de la información SITIS SAS que tiene como objetivo Proponer directrices para la implementación de un sistema de gestión de seguridad de la información que le permita al proceso de Gestión de requerimientos de la empresa SITIS, para proteger la información (datos, procesos y personas) de posibles amenazas, que puedan perjudicar el funcionamiento del proceso, con el fin de garantizar la continuidad de los sistemas de información, minimizando los riesgos de daño y asegurando el eficiente cumplimiento de sus objetivos.

Ver Anexo 09 - Política general de seguridad de la información SITIS SAS

3.11. Entregables

Se realizó el entregable de los siguientes artefactos a SITIS SAS:

1. Anexo 01 - Identificación de Amenazas
2. Anexo 02 - Identificación de vulnerabilidades y riesgos por amenaza
3. Anexo 03 - Valoración de riesgos
4. Anexo 04 - Salvaguardas
5. Anexo 05 - SOA Declaración de aplicabilidad
6. Anexo 06 - Plan de Tratamiento de Riesgo
7. Encuesta sobre conocimientos de Seguridad de la información
8. Inventario y clasificación de activos
9. Política de escritorio y pantalla limpia
10. Política general de seguridad de la información SITIS SAS

A conformidad se entrega los documentos y se recibe en formato PDF la firma, esta se puede visualizar en el Anexo 10 - Carta de aceptación

RECOMENDACIONES

Una vez terminado el análisis del proceso de Gestión de Requerimientos, se realizan las siguientes sugerencias que ayudaran a reducir el índice de amenazas y riesgos en los activos:

- Se recomienda la implementación del sistema de gestión de seguridad de la norma ISO 27001 no a un proceso, sino a la empresa en general, para que se adopte la estrategia de protección de activos de información de toda la organización y se pueda implementar la Política general de seguridad de la información generada a partir de este proyecto.

- Implementar y ejecutar la política propuesta de escritorio y pantalla limpia y en lo posible desarrollar más políticas dadas en la norma ISO 270001 para la protección de la información. Una vez se realice la implementación, mantener revisiones periódicas para comprobar el cumplimiento de la misma.

- Capacitar a los empleados en temas la seguridad de la información para que formen parte del resguardo del insumo vital de la empresa como es la información.

- De acuerdo a la evidencia que pudimos revisar de la política de seguridad de copias de seguridad, se sugiere que se revisen las bitácoras para validar efectivamente se esté llevando de acuerdo a lo estipulado, ya que en este momento el proceso está tercerizado y es necesario probarlas las copias.

- Establecer una cultura organizacional frente a la seguridad de la información para tomar acciones correctivas frente a la aparición de nuevas vulnerabilidades, amenazas o riesgos que se puedan presentar; de esta manera se permite tomar decisiones y acciones preventivas.

CONCLUSIONES

- Se realiza el inventario de los activos de información y se identifica cada una de las amenazas presentes en el proceso de gestión de requerimientos aplicando el catálogo de amenazas de la metodología Magerit.

- MAGERIT v3 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos se alinea con las directrices de la norma ISO 27001, permitiendo realizar el análisis de riesgos del proceso de Gestión de Requerimientos de la empresa SITIS SAS

- De igual manera se puede concluir que el proceso de Gestión de Requerimientos está expuesto a múltiples amenazas que pueden conducir a la perdida de la confidencialidad, integridad o disponibilidad y que causa de esta problemática parte del desconocimiento del personal sobre el manejo de la seguridad de la información y la falta de políticas que contribuyan al uso adecuado de cada activo de información.

- Las salvaguardas propuestas conducen a la disminución significativa del nivel de riesgo de cada uno de los activos de información, queda a cargo de la organización la implementación para evitar el reporte de incidencias de seguridad que conlleven a eventos de perdida para la empresa.

- Mediante el análisis de riesgo de la seguridad de la información en el proceso de Gestión de Requerimientos basado en la metodología Magerit, se define el plan tratamiento de riesgos en donde se especifican los controles y actividades para realizar el tratamiento de riesgo, dando como resultado una política de seguridad.

REFERENCIAS

[1] J. R. S. Agustín López Neira, «ISO27000.es,» 2005. [En línea]. Available: https://www.iso27000.es/glosario.html. [Último acceso: 15 09 2020].

[2] O. I. p. l. Normalización, «ISO,» [En línea]. Available: https://www.iso.org/isoiec-27001-information-security.html. [Último acceso: 04 02 2020].

[3] O. I. d. Normalización, «ISO 31000:2018(es) Gestión del riesgo — Directrices,» ISO, 2018. [En línea]. Available: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es. [Último acceso: 20 08 2020].

[4] O. I. d. Normalización, «ISO/IEC 27005:2018,» 07 2018. [En línea]. Available: https://www.iso.org/standard/75281.html. [Último acceso: 23 07 2020].

[5] C. J. B. S. G. P. R. D. W. W. R. Alberts, «Defense Technical Information Center - Octave,» 01 06 1999. [En línea]. Available: https://apps.dtic.mil/sti/citations/ADA367718. [Último acceso: 23 07 2020].

[6] P. e. I. d. l. A. E. Dirección General de Modernización Administrativa, «Portal Administración Electrónica,» 29 10 2020. [En línea]. Available: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.

[7] J. C. Miguel Angel Amutio Gómez, «Portal Administración Electrónica,» 10 2012. [En línea]. Available: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html. [Último acceso: 20 03 2020].

[8] F. Pacheco, «Welivesecurity,» ESET, 10 09 2010. [En línea]. Available: https://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/. [Último acceso: 15 07 2020].

[9] M. Cantalapiedra, «Think Big / Empresas,» 25 11 2019. [En línea]. Available: https://empresas.blogthinkbig.com/empresa-de-base-tecnologica/. [Último acceso: 09 10 2020].

[10] SigneBlock, «SIGNE Block,» 17 12 2020. [En línea]. Available: https://www.signeblock.com/iso-27001-sistemas-de-seguridad-de-la-informacion/. [Último acceso: 31 03 2021].

[11] C. H. T. T., «Amenazas informáticas y seguridad de la información,» *Poral de revistas - Universidad Externado de Colombia,* 2018.

[12] M. rockcontent, «Blogs de la IBERO,» 10 06 2010. [En línea]. Available: https://blog.posgrados.ibero.mx/seguridad-de-la-informacion/. [Último acceso: 06 11 2020].

[13] M. L. H. Cruz, «Gestión de riesgo metodologías Octave y Magerit,» [En línea]. Available: http://polux.unipiloto.edu.co:8080/00004420.pdf. [Último acceso: 20 07 2020].

[14] J. P. Pedro Guerrero, «Guía de sistema de gestión de seguridad de la información (SGSI) para entidades de Contact Center,» 2018. [En línea]. Available: https://repository.udistrital.edu.co/bitstream/handle/11349/14199/GuerreroRodriguezPedroAlejandro2018.pdf?sequence=1&isAllowed=y. [Último acceso: 15 09 2020].

[15] A. Siler, «Universidad Internacional de la Rioja,» 14 12 2014. [En línea]. Available: https://reunir.unir.net/bitstream/handle/123456789/4737/AMADOR%20DONADO%2c%20SILER.pdf?sequence=1&isAllowed=y. [Último acceso: 15 07 2020].

[16] O. I. d. Normalización, ISO/IEC 27001:2013, Bogotá: ICONTEC, 2013.

[17] ICONTEC, «COMPENDIO: Sistema de gestión de la seguridad de la información (SGSI),» 2006. [En línea]. Available: www.Icontec.org.co. [Último acceso: 12 05 2020].

[18] I. -. I. O. f. Standardization, «ISO/IEC 27002:2013,» 10 2013. [En línea]. Available: https://www.iso.org/standard/54533.html. [Último acceso: 04 09 2020].

[19] J. M. Poveda, «Análisis y valoración de los riesgos Metodologías,» [En línea]. Available: https://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-8.pdf. [Último acceso: 10 06 2020].

[20] C. G. Amaya, «Welivesecurity,» Eset, 14 05 2013. [En línea]. Available: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/. [Último acceso: 20 05 2020].

[21] F. N. S. Solarte, «Sistema de gestión de seguridad informática - SGSI,» 04 07 2016. [En línea]. Available: http://blogsgsi.blogspot.com/2016/07/v-behaviorurldefaultvmlo.html. [Último acceso: 07 11 2020].

[22] Bizagi, «Bizagi,» 2021. [En línea]. Available: https://www.bizagi.com/es. [Último acceso: 15 03 2020].

[23] R. PowerData, «PowerData,» 17 08 2015. [En línea]. Available: https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/bid/406549/qu-es-el-sistema-manejador-de-bases-de-datos#:~:text=Un%20sistema%20manejador%20de%20bases,y%20las%20distintas%20aplicaciones%20utilizadas. [Último acceso: 15 03 2020].

[24] O. I. p. l. Estandarización, ISO/IEC 27000, 2018.

[26] I. Excellence, «Blog especializado en Sistemas de Gestión,» 28 01 2015. [En línea]. Available: https://www.pmg-ssi.com/2015/01/iso-27001-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/. [Último acceso: 07 11 2020].

[27] U. Libre, «Seguridad de la Información,» 10 06 2015. [En línea]. Available: http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/152-seguridad-de-la-informacion. [Último acceso: 10 09 2020].

[28] U. -. U. I. d. L. Rioja, «¿Qué es la certificación ISO 27001 y para qué sirve?,» 11 12 2019. [En línea]. Available: https://www.unir.net/ingenieria/revista/iso-27001/. [Último acceso: 15 09 2020].

[29] J. Rodriguez, «Diseño de un SGSI (sistema de gestión de seguridad de la información) basado en iso27001 para laboratorios servicios farmacéuticos de calidad SFC LTDA,» 2017. [En línea]. Available: https://repository.unad.edu.co/bitstream/handle/10596/12598/1097035128.pdf?sequence=1&isAllowed=y. [Último acceso: 15 09 2020].

ANEXOS

1. Anexo 01 - Encuesta sobre conocimientos de Seguridad de la información
2. Anexo 02 - Identificación de Amenazas
3. Anexo 03 - Identificación de vulnerabilidades y riesgos por amenaza
4. Anexo 04 - Valoración de riesgos
5. Anexo 05 - Salvaguardas
6. Anexo 06 - SOA Declaración de aplicabilidad
7. Anexo 07 - Plan de Tratamiento de Riesgo
8. Anexo 08 - Política de seguridad de escritorio y pantalla limpia
9. Anexo 09 - Política general de seguridad de la información SITIS SAS
10. Anexo 10 - Carta de aceptación