ANÁLISIS DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DE UN APLICATIVO DE GESTIÓN DOCUMENTAL LIDER EN EL MERCADO COLOMBIANO.

TRABAJO DE GRADO

CARMEN ELIZABETH FAJARDO DIAZ

Código: 1424000081

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO

FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS

ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

2017

ANÁLISIS DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DE UN APLICATIVO DE GESTIÓN DOCUMENTAL LIDER EN EL MERCADO COLOMBIANO.

TRABAJO DE GRADO

CARMEN ELIZABETH FAJARDO DIAZ

Código: 1424000081

ALEJANDRO CASTIBLANCO CARO

Asesor(es)

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO

FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS

ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

2017

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

_____

_____

Firmas de los jurados

Bogotá, 2 de Junio de 2017

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

INTRODUCCIÓN

En la actualidad las aplicaciones de gestión documental son muy utilizadas en el sector productivo debido a que les permite organizar, centralizar, gestionar y administrar de forma digital todos los procesos corporativos que adelantan las diversas empresas en nuestro país. Para cualquier organización, los documentos que procesan son la evidencia de las actividades que desarrollan al interior de la empresa así como con otras entidades, manejando acorde al tipo de documento información que puede ser sensible para la organización, motivo por el cual la seguridad de la información es un aspecto clave que debe se debe tener presente a la hora de implementar un sistema de gestión documental dentro de una entidad.

Este documento está enfocado a realizar un análisis de los riesgos de seguridad de la información de un aplicativo de gestión documental líder en el mercado Colombiano, determinando cuales son los riesgos de seguridad a los que se encuentra expuesta la información dentro del proceso y aplicativo de gestión documental, así como establecer el plan de tratamiento adecuado de dichos riesgos para controlarlos y reducirlos a niveles aceptables y asumibles para la entidad propietaria del software así como sus respectivos clientes.

1. RESUMEN EJECUTIVO

En la actualidad las aplicaciones de gestión documental son muy utilizadas en el sector productivo debido a que les permite optimizar la administración, gestión y control de la documentación e información de la compañía, de manera eficiente, eficaz y menos costosa de forma digital e involucra todos los procesos corporativos que adelantan las diversas empresas en nuestro país. Para cualquier organización, los documentos que procesan son la evidencia de las actividades que desarrollan al interior de la empresa así como con otras entidades, manejando acorde al tipo de documento información que puede ser sensible para la organización, motivo por el cual la seguridad de la información es un aspecto clave que tienen presente las organizaciones que desean implementar un sistema de gestión documental, entre otros aspectos como el aumento de la productividad, disminución de tiempo y costos en el procesamiento de la documentación, la optimización de los procesos entre otros aspectos.

El Sistema de Gestión Documental objeto del presente estudio, es una aplicación de software propietaria de una empresa Colombiana que incursiono en el mercado a mediados de los noventa con el objetivo de brindar a las diferentes organizaciones del sector productivo una herramienta que les permitirá automatizar y dinamizar los procesos documentales generados diariamente en el desarrollo de su objeto de negocio; posicionándose actualmente en el sector productivo como una aplicación de gestión documental líder en el territorio colombiano.

Debido a la importancia que tiene la información hoy en día para la continuidad del negocio y el cumplimiento de los objetivos organizacionales, la empresa propietaria del software de gestión documental ha detectado la necesidad de establecer acciones de mejora que le permitan identificar las debilidades y falencias que presenta su aplicativo de gestión documental en la protección de la seguridad de la información, debido a que han presentado situaciones que han conllevado a la perdida de confidencialidad y disponibilidad de la información de los clientes que se gestiona a través aplicativo de gestión documental, así como perdida de código fuente de mejoras del aplicativo por la ausencia de procesos y procedimientos que establezcan los lineamientos para la administración y almacenamiento de la información correspondiente al desarrollo de software asociados con el aplicativo de gestión documental objeto del presente estudio.

La empresa propietaria del software de gestión documental permitió realizar el respectivo estudio, sin embargo no autorizo a divulgar el nombre del aplicativo ni de la organización, ya que consideran podrían perder la credibilidad y confianza de sus clientes, así como afectar negativamente la continuidad y posicionamiento de su aplicación en el sector productivo.

Para brindar solución a la problemática mencionada se describe a continuación el alcance y los objetivos del proyecto.

Alcance del proyecto

El alcance del proyecto establece la identificación de los riesgos de seguridad del aplicativo de gestión documental objeto del presente estudio, diseñando el plan de tratamiento de riesgos que le permitan a la organización controlar y disminuir los riesgos de seguridad detectados en el aplicativo de gestión documental. Dentro de las limitaciones del alcance del proyecto está la ejecución, seguimiento y control del plan de tratamiento de riesgos diseñado para la aplicación de gestión documental, sugiriendo a las directivas y personal IT de la empresa propietaria del software implementar el plan de tratamiento de riesgos, para mitigar y controlar los riesgos existentes a los que se encuentran expuestos los activos de información que engloba la solución de gestión documental.

Objetivo General

Realizar el análisis de riesgos de seguridad de la información sobre la aplicación de gestión documental, proponiendo un plan de tratamiento orientado a mitigar y controlar los riesgos de seguridad detectados en el aplicativo de software objeto del presente estudio.

Objetivos Específicos

- Definir la metodología a emplear para identificar, valorar, clasificar y tratar los activos de información que apoyan la gestión del aplicativo de gestión documental.

- Realizar un inventario de los activos de información que engloba el aplicativo de gestión documental resultado de aplicar la metodología de identificación,

clasificación y valoración de los activos de información del software de gestión documental.

- Especificar la metodología para la identificación y valoración de los riesgos de seguridad que se encuentran presentes en el aplicativo de gestión documental.

- Identificar y valorar los riesgos de seguridad sobre los activos de información del aplicativo de gestión documental al interior de la empresa propietaria del software.

- Definir la política de seguridad de la información de la organización propietaria del software de gestión documental.

Con el desarrollo de la metodología propuesta para el presente trabajo de grado los entregables que harán parte de los resultados obtenidos son:

- Política de seguridad de la información enfocada a la organización propietaria del software de gestión documental.

- Inventario de activos asociados al sistema de gestión documental objeto del presente trabajo de grado.

- Informe del análisis de riesgos detectados sobre el aplicativo de gestión documental empleando la metodología MAGERIT.

- Informe de plan de tratamiento y gestión de riesgos de seguridad de la información detectados en el aplicativo de gestión documental enfocado a minimizar y controlar los riesgos de información descritos.

2. JUSTIFICACIÓN

En Colombia existe un amplio marco legal y jurídico, entre las que se encuentra la ley 594 de 2000 – Ley General de Archivos en la que define la gestión documental como un "conjunto de actividades administrativas y técnicas tendientes a la planificación, manejo y organización de la documentación producida y recibida por las entidades, desde su origen hasta su destino final, con el objeto de facilitar su utilización y conservación" (MinTIC, 2014, p. 4).

En la actualidad tanto entidades públicas como privadas han optado por implementar soluciones de gestión documental que les permita organizar, centralizar, gestionar y administrar digitalmente toda la documentación que manejan tanto al interior como al exterior de la organización, siendo la información que se encuentra contenida en estos documentos uno de los activos más importantes de las organizaciones, motivo por el cual hace necesario que las aplicaciones de gestión documental protejan la confidencialidad, integridad y disponibilidad de la información; cualidades que le permiten a las empresas mantener su buen nombre con sus clientes, proveedores y aliados estratégicos, así como posesionarse en el sector productivo.

El software de gestión documental objeto de este proyecto se encuentra implementado y operativo en alrededor de setenta y nueve (79) clientes entre entidades del sector público y privado, con aproximadamente veinticuatro mil seiscientos (24.600) usuarios en producción distribuidos a través del territorio Colombiano. En el año 2016 las áreas de consultoría y TI de la entidad propietaria del software diseñaron una prueba para evaluar diversos aspectos operativos y de seguridad del aplicativo de gestión documental siendo aplicada en una muestra de cuatro (4) clientes, la cual fue implementada por los diversos usuarios líderes de cada proyecto, los usuarios del sistema e interventores durante un (1) mes obteniendo los siguientes resultados.

ASPECTO A EVALUAR	DESCRIPCION DEL ASPECTO A EVALUAR	FORMULA	PORCENTAJE OBTENIDO
Integridad	Se refiere a que el criterio evaluado esté de acuerdo a los requerimientos establecidos.	(Cantidad de pruebas realizadas al sistema satisfactorias / total de pruebas al sistema) *100	74 %
Confiabilidad	La información o proceso que se relacione con el criterio debe estar completo y acorde con lo que se		43 %

ASPECTO A EVALUAR	DESCRIPCION DEL ASPECTO A EVALUAR	FORMULA	PORCENTAJE OBTENIDO
	espera que realice o represente.		
Exactitud	Es un cálculo numérico o de medición de los resultados de las variables y/o procesos relacionados con el criterio.		91%
Fiabilidad	Los resultados que se tienen están acordes con lo que se espera de acuerdo al criterio definido.		77 %
Autenticidad	Se debe medir la validez de la información que se encuentra en el sistema frente a la suministrada por la fuente.		74 %
Vulnerabilidad	Debilidades reales que han sido detectadas en el sistema.		80 %

Tabla 1 – Indicadores del estado actual del problema detectado.

Acorde a los indicadores descritos en la tabla 1 y obtenidos a través del muestreo implementado con clientes directos del aplicativo, es importante para la organización propietaria de la aplicación de gestión documental objeto de este proyecto; el contar con un estudio que le proporcione el análisis de los riesgos de seguridad de la información a los que se encuentra expuesta la información (esta puede ser de clientes o de la organización propietaria del software) que se gestiona a través del aplicativo de gestión documental que ofrecen a sus clientes, así como el plan tratamiento de riesgos diseñado y sugerido para reducir y controlar los riesgos de seguridad detectados sobre la aplicación de gestión documental llevándolos a niveles aceptables y asumibles para la entidad propietaria del software, lo que le permitirá a la organización tomar las acciones correctivas necesarias para fortalecer la seguridad como parte del desarrollo e implementación de sus aplicaciones de software, así como operativo para salvaguardar la información propia y de sus clientes aspectos enfocados a contribuir con la continuidad del negocio y el crecimiento de la organización a nivel nacional.

3. MARCO TEÓRICO Y REFERENTES

El marco teórico descrito a continuación referencia la conceptualización técnica que se puede encontrar en el presente documento y anexos asociados al desarrollo del proyecto.

3.1 SEGURIDAD DE LA INFORMACIÓN

A continuación se relacionan la definición de los términos relacionados con la seguridad de la información, aplicados en el proyecto objeto del presente documento.

- ✓ ***Activo:*** "Se considera un activo a aquello que es de alta validez y que contiene información vital la cual es importante proteger". (Institución Universitaria Politécnico GranColombiano, 2016, p. 7)

- ✓ ***Información:*** "Conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje". (Institución Universitaria Politécnico GranColombiano, 2016, p. 5)

- ✓ ***Triada CID:*** "Compuesta por la Confidencialidad, Integridad y Disponibilidad de la información, la cual, es considerada como una definición de los objetivos de la seguridad de la información". (Institución Universitaria Politécnico GranColombiano, 2016, p. 8)

- ✓ ***Confidencialidad:*** "Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados". (International Standar ISO/IEC 27000, 2016, p. 3)

- ✓ ***Integridad:*** "Propiedad de salvaguardar la exactitud y estado completo de los activos". (International Standar ISO/IEC 27000, 2016, p. 3)

- ✓ ***Disponibilidad:*** "Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada" (International Standar ISO/IEC 27000, 2016, p. 3)

- ✓ ***Autenticidad***: “Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.” (Gobierno de España, 2012, p. 9)

- ✓ ***Autenticación:*** “Proceso bajo el cual se verifica la identidad del usuario”. (Institución Universitaria Politecnico GranColombiano, 2016, p. 6)

- ✓ ***Trazabilidad:*** “Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento”. (Gobierno de España, 2012, p.9)

- ✓ ***Seguridad de la información:*** “Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad”. (International Standar ISO/IEC 27000, 2016, p. 6)

- ✓ ***Política de seguridad de la información:*** “Documento global ejecutivo que establece las obligaciones a tener en cuenta en cuanto a seguridad de la información (en virtud de la triada CID) dentro de una organización.” (Institución Universitaria Politécnico GranColombiano, 2016, p. 9)

- ✓ ***Vulnerabilidad:*** “Es una debilidad a nivel de software, hardware, procedimientos o error humano que permite a un atacante aprovecharla para causar daño. La vulnerabilidad se caracteriza por ausencia de controles de seguridad que permite ser explotada”. (Institución Universitaria Politécnico GranColombiano, 2016, p. 7)

- ✓ ***Amenaza:*** “Se define como un peligro potencial a la información del sistema. Se presente cuando un atacante identifica una vulnerabilidad sobre un activo y es usada para generar daños que afectan a la compañía”. (Institución Universitaria Politécnico GranColombiano, 2016, p. 7)

- ✓ ***Probabilidad:*** “Estimación de ocurrencia de un evento, el cual está relacionado a características de las vulnerabilidades presentadas y el origen de la amenaza”. (Institución Universitaria Politécnico GranColombiano, 2016, p. 7)

- ***Impacto:*** “Consecuencia generada a partir de la materialización de una amenaza. El impacto es clasificado de acuerdo al daño que produce sobre el activo la cual puede ser alta, media o baja”. (Institución Universitaria Politécnico GranColombiano, 2016, p. 7)

- ***Controles:*** “Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los bienes de la compañía”. (Institución Universitaria Politécnico GranColombiano, 2016, p. 7)

- ***Riesgo:*** “Grado de exposición de un activo que cual permite la materialización de una amenaza ocasionando daños a la compañía”. (Institución Universitaria Politécnico GranColombiano, 2016, p. 7)

- ***Riesgo residual:*** “Nivel restante de riesgo después del tratamiento del riesgo”. (International Standar ISO/IEC 27000, 2016, p. 10)

- ***Aceptación del riesgo:*** “Decisión de asumir un riesgo”. (International Standar ISO/IEC 27000, 2016, p. 10)

- ***Análisis de riesgo:*** “Uso sistemático de la información para identificar las fuentes y estimar el riesgo”. (International Standar ISO/IEC 27000, 2016, p. 11)

- ***Evaluación del riesgo:*** “Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo”. (International Standar ISO/IEC 27000, 2016, p. 11)

- ***Gestión del riesgo:*** “Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo”. (International Standar ISO/IEC 27000, 2016, p. 12)

- ***Tratamiento del riesgo***: “Proceso de selección e implementación de medidas para modificar el riesgo”. (International Standar ISO/IEC 27000, 2016, p. 12)

- ✓ ***Mapa de riesgos:*** “Relación de las amenazas a que están expuestos los activos”. (Gobierno de España, 2012, p. 8)

- ✓ ***Valoración del riesgo***: “Proceso global de análisis y evaluación del riesgo”. (International Standar ISO/IEC 27000, 2016, p. 11)

3.2 GESTIÓN DOCUMENTAL

La gestión documental consiste en la aplicación de tecnologías y procedimientos que permiten establecer un acceso unificado a la información generada en la organización, a través de actividades administrativas y técnicas que permiten coordinar y controlar la creación, recepción, organización, almacenamiento, preservación, acceso y difusión de documentos durante su ciclo de vida con el objeto de facilitar su utilización a través de los procesos en los cuales pueda intervenir dentro de la organización, así como su conservación.

Entre los beneficios que trae para una organización implementar un sistema de gestión documental se encuentran:

- ✓ Calidad en la gestión administrativa, la cual se ve reflejada en los siguientes aspectos:
    - Eficiencia en los procesos
    - Control de actividades
    - Información en línea
    - Ahorro de tiempo
    - Brinda apoyo en la toma de decisiones

- ✓ Reduce tiempo en el acceso a la información: debido a que brinda una mayor eficacia y eficiencia en los procesos de búsqueda y recuperación de información reduciendo los tiempos de respuesta.

- ✓ Reducción de volúmenes documentales, racionalizando el archivo y de esta forma obteniendo un volumen real del inventario documental y a su vez minimiza los

espacios donde se preserva la documentación, así como los costos asociados a su manipulación y almacenamiento y recuperación.

- ✓ Minimiza los riesgos de pérdida y deterioro.
- ✓ Refleja la modernización empresarial
- ✓ Reduce los costos de mantenimiento y apoyo en la gestión de la documentación.
- ✓ Asegura la óptima utilización de los recursos y el espacio físico, percibiendo a través del ROI (Retorno sobre la inversión) el beneficio obtenido en relación con la inversión realizada en la implementación del sistema de gestión documental.
- ✓ Permite agilizar los procesos, mejorando la productividad de la organización.

Dentro de los aspectos relevantes que tiene un sistema de gestión documental, se encuentra el ciclo de vida de los documentos, el cual se basa en una serie de etapas o fases sucesivas por las que pasan los documentos desde la producción o recepción del documento hasta su archivado permanente o eliminación. La figura 1 ilustra el ciclo de vida de los documentos.

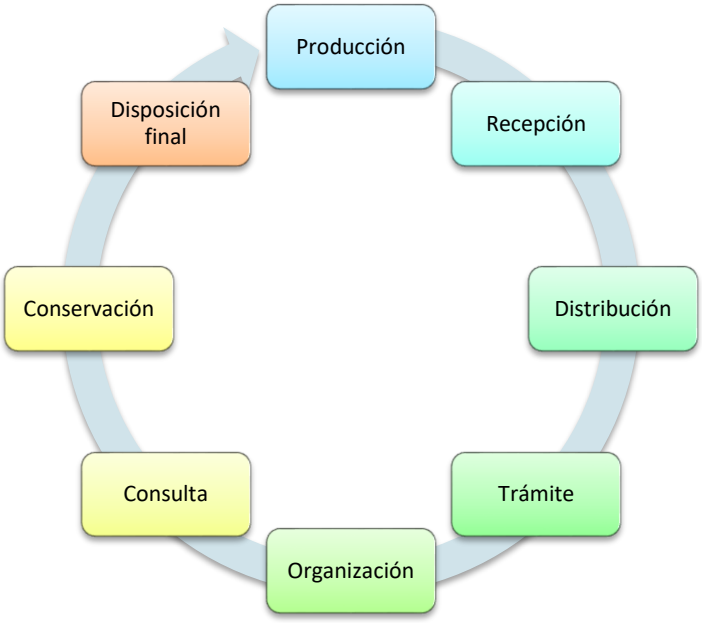

Figura 1 – Ciclo de vida de los documentos

La fase de producción documental hace relación a la generación de los documentos en las entidades en el ejercicio de su razón social. La recepción del documento involucra procesos de verificación y control que les permiten admitir los documentos que pueden ser remitidos por un cliente interno o externo de la entidad. En la fase de distribución de documentos se encuentra enfocado a garantizar que los documentos lleguen a su destinatario para su respectiva gestión y tramite.

La organización documental establece el conjunto de acciones orientadas a la clasificación, ordenación y descripción de los documentos como parte integral de los procesos archivísticos. La consulta de documentos permite establecer el acceso a un documento o grupo de documento con la finalidad de conocer la información que contienen. En la conservación de los documentos se toman las medidas preventivas o correctivas que permitan garantizar la integridad física y funcional de los documentos de archivo sin alterar su contenido.

La fase de disposición final determina el proceso final de documento el cual posterior a una valoración puede ser eliminado o archivado.

En todas las fases descritas en el ciclo de vida de la documentación se encuentra implícito la información, el cual es considerado el activo más valioso que posee una organización y que está ligado a la continuidad del negocio; de ahí la importancia de que el aplicativo de gestión documental permita salvaguardar la integridad, confidencialidad y disponibilidad de la información.

4. METODOLOGÍA

Para desarrollar el alcance y los objetivos propuestos en el proyecto, la metodología a implementar enmarca las fases de inicio, análisis y diseño, donde cada etapa establece una serie de actividades encaminadas a lograr los resultados del proyecto, las cuales se describen a continuación.

FASE 1 - INICIO

- Elaboración de la propuesta del análisis de riesgos de la información sobre la aplicación de gestión documental objeto del presente estudio.
- Revisión y aprobación de la propuesta por parte de la gerencia de la empresa propietaria del software.
- Revisión y aprobación de la propuesta por parte de la Universidad.

FASE 2 - ANÁLISIS

- Realizar el Levantamiento de información empleando las siguientes técnicas:

    - Entrevistas con los actores relevantes del aplicativo de gestión de documental (Gerencia y áreas involucras (Desarrollo, Soporte y Consultoría)).
    - Revisión de la infraestructura física existente donde se alberga el aplicativo de gestión documental.
    - Reconocimiento de la infraestructura existente de red bajo la cual se establece el acceso al aplicativo de gestión documental al personal de desarrollo, consultoría de la entidad y clientes externos.
    - Realización de pruebas con cuenta creada y valida con diversos roles para detectar las vulnerabilidades en cuanto a seguridad de la información del aplicativo de gestión documental.

FASE 3 - DISEÑO

- Definir la metodología a implementar para realizar el análisis de riesgos de seguridad de la información sobre el aplicativo de gestión documental.

    - Identificación y clasificación de los activos de información, empleando el modelo de clasificación de los activos descrito en la metodología MAGERIT.
    - Determinar las vulnerabilidades y amenazas de los activos de información correspondientes a la aplicación de gestión documental.

○ Definir los riesgos de seguridad de la información detectados en el aplicativo, empleando la metodología MAGERIT de análisis y gestión de riesgos de los sistemas de información. ○ Evaluar en términos de probabilidad de ocurrencia e impacto los riesgos de seguridad de la información detectados. ○ Definir con la dirección el nivel de aceptación de los riesgos de seguridad de la información. • Diseñar la política de seguridad de la información para la empresa propietaria del software de gestión documental. • Diseñar el plan de tratamiento y gestión de riesgos de seguridad de la información. • Socializar los resultados obtenidos ante la dirección de la empresa y/o Universidad.

Tabla 2 – Descripción de la metodología a emplear en el desarrollo del trabajo de grado.

El plan de trabajo propuesto se basa en el desarrollo de la metodología descrita, el cual se adjunta en el Anexo N.1 al presente documento, describiendo a continuación las actividades realizadas en cada una de las fases propuestas.

4.1 FASE DE INICIO

En esta fase se estableció los respectivos ajustes del anteproyecto acorde a las orientaciones recibidas por parte de la Universidad. Una vez obtenida la viabilidad para el desarrollo del proyecto se formalizo con el gerente general de la empresa propietaria del software de gestión documental la propuesta y el plan de trabajo a realizar para llevar a cabo el análisis de riesgos sobre dicho aplicativo, recibiendo la respectiva aprobación, apoyo y permiso para elaborar el análisis de riesgos de seguridad de la información del aplicativo objeto del presente estudio.

4.2 FASE DE ANALISIS

Las actividades asociadas a la fase de análisis se realizaron con el objetivo de identificar los lineamientos que se implementan en el desarrollo y mejoras del código fuente del aplicativo de gestión documental, características de funcionamiento y estado actual de la seguridad en la infraestructura tecnológica que alberga la información pertinente al aplicativo, su gestión y administración a través de la red corporativa de la organización.

Para identificar el estado actual de la seguridad de la información en el aplicativo de gestión documental se emplearon las siguientes técnicas.

- ✓ Entrevistas con los ingenieros líderes de las áreas de Desarrollo y Soporte IT, actores relevantes del aplicativo de gestión documental. Los respectivos soportes de las entrevistas se encuentran en los anexos 2 y 3. En septiembre de 2016 se entrevistó al consultor líder de procesos generando como resultado el planteamiento del presente proyecto.

- ✓ Inspección visual de las instalaciones administrativas de la empresa propietaria del software, empleando una lista de chequeo. Anexo 4.

- ✓ Ejecución de pruebas para identificar los aspectos que afectan la seguridad de la información en el aplicativo de gestión documental. Los resultados obtenidos permitieron identificar las vulnerabilidades descritas en la matriz de riesgos. No se genera un documento que evidencie el desarrollo de las pruebas debido a la reserva y confidencialidad que solicito el cliente.

4.3 FASE DE DISEÑO

Las actividades propuestas en esta fase permitieron realizar el análisis de los riesgos de seguridad de la información del aplicativo de gestión documental, estableciendo una propuesta de tratamiento y gestión de los riesgos de seguridad de la información que permita su mitigación y control, donde la empresa propietaria del software es autónoma en realizar o no su implementación.

Para lograr el desarrollo de los objetivos del proyecto se realizaron las siguientes acciones:

- Identificación, clasificación y valoración de los activos de tecnología asociados al diseño y funcionamiento del aplicativo de gestión documental, empleando el modelo de clasificación descrito en la metodología MAGERIT - versión 3.0 Libro II – Catalogo de elementos.

- La metodología a emplear para realizar el respectivo análisis de riesgos de seguridad de la información sobre el software de gestión documental, es la Metodología de Análisis y Gestión de Riesgos de los sistemas de información MAGERIT versión 3.0 descrita en el libro I – Método.

- Análisis de riesgos de seguridad de la información aplicando la metodología seleccionada.

- Valoración y evaluación de los riesgos de seguridad de la información en términos de probabilidad de ocurrencia e impacto.

- Diseño del plan de tratamiento de riesgos orientado a salvaguardar la seguridad de la información de los activos del aplicativo de gestión documental objeto del presente trabajo de grado.

- Establecimiento de la política de seguridad de la información para la organización.

A continuación se describen aspectos relevantes en el establecimiento de cada una de las actividades definidas en la fase de diseño.

4.3.1 IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS

La identificación de los activos relacionados con el sistema de información relacionados en el presente documento se enfoca en una aplicación de software de gestión documental, que se caracteriza por ser una de las líneas de negocio de la organización propietaria de la aplicación. La clasificación de los activos identificados se realizó gracias

al acompañamiento de los líderes del área de desarrollo y consultoría de la empresa propietaria del software, empleando la metodología MAGERIT, la cual propone el siguiente modelo de clasificación.

CATEGORÍA DEL ACTIVO	DESCRIPCIÓN DE LOS POSIBLES ACTIVOS
Datos e información	La información se caracteriza por ser el activo más importante que le permite a la organización prestar sus servicios. Su forma de almacenamiento puede ser digital o físico y se puede ver representada en ficheros, copias de respaldo, datos de gestión interna, credenciales, datos de validación de credenciales, datos de control de acceso, registro de actividad, códigos fuente, código ejecutable, etc.
Servicios	Contempla los servicios prestados por el sistema que satisfacen la necesidad de los usuarios. Dentro de los cuales se pueden encontrar correo electrónico, almacenamiento de ficheros, gestión de identidades, gestión de privilegios, acceso remoto, etc.
Software - Aplicaciones Informáticas	Se caracterizan porque gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios. Dentro de la clasificación se puede relacionar desarrollo propio, desarrollo a medida, aplicaciones ofimáticas, sistemas operativos, antivirus, etc.
Equipamiento Informático	Brindan soporte directo o indirectamente a los servicios que presta la organización, siendo repositorios temporales o permanentes de datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesamiento o transmisión de datos. Dentro de esta clasificación se relaciona todo el hardware de la red como dispositivos de red, servidores, host y periféricos.
Redes de comunicaciones	Se centran en los medios de transporte que llevan datos de un sitio a otro. Las redes pueden ser propias o contratadas a terceros. Se relacionan las redes LAN, Internet, redes inalámbricas, etc.
Soportes de información	Se consideran dispositivos físicos que permiten almacenar información de forma permanente o durante periodos de tiempo como discos físicos y virtuales, memorias USB, CD-DVD, etc.
Equipamiento auxiliar	Infraestructura que sirve de soporte a los sistemas de información, sin estar directamente relacionados con los datos como fuentes de alimentación, UPS, equipos de climatización, cableado, mobiliario, equipos de destrucción de soportes de información, suministros esenciales, etc.
Instalaciones	Relaciona los lugares donde se hospedan los sistemas de información y comunicaciones. Ej. Edificios, oficinas, instalaciones de respaldo.
Personal	Involucra el personal relacionado con los sistemas de información como pueden ser los usuarios internos, externos, operadores, administradores del sistema, desarrolladores, etc.

Tabla 3 – Clasificación de los activos definida en la metodología MAGERIT. (Gobierno de España, 2012, p8)

A continuación se describen los activos relacionados con el sistema de información identificados y clasificados acorde a la metodología descrita.

N. ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCION DEL ACTIVO	CATEGORIA DEL ACTIVO	UBICACIÓN (CONTENEDOR) DEL ACTIVO DE INFORMACIÓN
GD - A1	Software de control de versiones (Subversión y GIT)	Aplicación de administración para el control en el versionamiento del software.	Datos e información	• Servidor de aplicación
GD - A2	Metodología de desarrollo	Documento que establece la metodología de desarrollo de software	Datos e información	• Servidor de aplicación • Computadores de los desarrolladores
GD - A3	Código fuente	Código fuente del aplicativo de gestión documental	Datos e información	• Servidor de aplicación • Código fuente de nuevas funcionalidades puede estar ubicado localmente en el computador de un desarrollador.
GD - A4	Servidor de aplicaciones	Servidor de aplicación que soporta el aplicativo de gestión documental a través de ambiente web.	Equipamiento Informático	• Cuarto de equipos de la sede principal
GD - A5	Servidor de bases de datos	Servidor de bases de datos que soporta la información de los usuarios de sistema de gestión documental.	Equipamiento Informático	• Cuarto de equipos de la sede principal
GD - A6	Servidor de imágenes	Servidor de archivos que almacena las imágenes indexadas al sistema de gestión documental.	Equipamiento Informático	• Cuarto de equipos de la sede principal
GD - A7	Portátiles	Computadoras portátiles de la entidad asignados a desarrolladores.	Equipamiento Informático	• Espacio administrativo asignado al área de desarrollo.
GD - A8	Computadores de escritorio desarrolladores	Computadores de escritorio asignados a los desarrolladores de software	Equipamiento Informático	• Espacio administrativo asignado al área de desarrollo. • Instalaciones de los clientes que utilizan la aplicación de gestión documental. • En la ubicación donde se encuentre el responsable del activo (Empleado). Ej.: Lugar de residencia.
GD - A9	Dispositivos de red	Dispositivos encargados de la conectividad de la red. La organización cuenta con switch no administrables, router y dispositivos inalámbricos.	Equipamiento Informático	• Cuarto de equipos, el cual cumple también la función del cuarto de telecomunicaciones en las instalaciones de la organización.

N. ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCION DEL ACTIVO	CATEGORIA DEL ACTIVO	UBICACIÓN (CONTENEDOR) DEL ACTIVO DE INFORMACIÓN
GD - A10	Cuarto de equipos	Instalación física donde residen los dispositivos de red y servidores	Instalaciones	• Instalación física de la organización (Casa de dos plantas)
GD - A11	Desarrolladores	El personal que conforma el área de desarrollo de la organización	Personal	• Talento humano del área de desarrollo
GD - A12	Red de área local - LAN	Red LAN corporativa de la entidad	Redes de comunicaciones	• Instalación física de la organización (Casa de dos plantas)
GD - A13	Red Inalámbrica - WLAN	Red Wifi utilizada por dispositivos móviles para acceder a los servicios y recursos de la red corporativa.	Redes de comunicaciones	• Instalación física de la organización (Casa de dos plantas)
GD - A14	Servicio de File Systems	Almacenamiento de la información concerniente al desarrollo de la aplicación.	Servicios	• Carpeta compartida en el servidor de aplicación
GD - A15	Interfaz de desarrollo (Netbeans con lenguaje de programación Java)	Plataforma de desarrollo de código abierto para aplicaciones desarrolladas en Java.	Software - Aplicaciones Informáticas	• Computadores de los desarrolladores
GD - A16	Sistemas operativos	Software que permite la administración del hardware de los equipos de cómputo (Escritorio, portátiles, servidores)	Software - Aplicaciones Informáticas	• Equipos de cómputo (Portátiles y de escritorio) • Servidores
GD - A17	Antivirus	Software orientado a proteger la red de código malicioso (Malware)	Software - Aplicaciones Informáticas	• Equipos de cómputo (Portátiles y de escritorio) • Servidores
GD - A18	Aplicativo de gestión documental - Ejecutable	Aplicativo de gestión documental	Software - Aplicaciones Informáticas	• Servidor de aplicación
GD - A19	Sistemas de gestión de bases de datos	Aplicación para la gestión y administración de la base de datos	Software - Aplicaciones Informáticas	• Servidor de base de datos
GD - A20	Medios de almacenamiento electrónico (USB, Discos duros externos)	Unidades de almacenamiento externo de información	Soportes de información	• Espacio administrativo asignado al área de desarrollo. • Instalaciones de los clientes que utilizan la aplicación de gestión documental. • En la ubicación donde se encuentre el responsable del activo (Empleado). Ej.: Lugar de residencia.

Tabla 4 - Inventario de activos relacionados con el aplicativo de gestión documental

Ya identificados los activos relacionados con el sistema de información se estableció su valoración en términos de confidencialidad, integridad y disponibilidad teniendo presente la importancia del activo para la continuidad del negocio, así como el impacto que puede causar para la organización a nivel financiero, jurídico y de imagen corporativa la perdida de alguna de las características de la seguridad de la información relacionada con el aplicativo de gestión documental debido a la materialización de una amenaza.

La identificación de la perdida de confidencialidad, integridad y/o disponibilidad se realizó teniendo en cuenta las siguientes preguntas en cada uno de los aspectos descritos.

DIMENSION DE SEGURIDAD	ASPECTO AFECTADO	PREGUNTA FORMULADA
Confidencialidad	Financiero	¿La divulgación no autorizada de un activo de información sensible afecta la estrategia del negocio y el estado financiero de la organización?
	Jurídico	¿La divulgación no autorizada de un activo de información sensible ocasiona el incumplimiento de la normatividad y/o puede generar demandas de terceros?
	Imagen Corporativa	¿La divulgación no autorizada de un activo de información afecta credibilidad y buen nombre de la organización?
Integridad	Financiero	¿La modificación no autorizada de un activo de información genera costos en reprocesos, afectación de estrategias de negocio y posibles costos por procesos jurídicos?
	Jurídico	La modificación no autorizada de un activo de información incurre en aplicación de sanciones legales y jurídicas.
	Imagen Corporativa	La alteración no autorizada de un activo de información afecta negativamente la imagen institucional.
Disponibilidad	Financiero	¿La indisponibilidad de los activos de información afecta los ingresos económicos de la organización y las estrategias del negocio?
	Jurídico	¿La indisponibilidad de los activos de información genera sanciones legales y jurídicas?
	Imagen Corporativa	¿La no disponibilidad del activo de información afecta la operación y la imagen corporativa ante terceros?

Tabla 5 - Consulta para determinar la criticidad del activo

Las dimensiones de seguridad serán valoradas teniendo presente los siguientes aspectos y criterios de valoración.

ASPECTO	CONSECUENCIAS DE LA PERDIDA DEL ACTIVO	CRITERIO DE VALORACIÓN	VALOR ASIGNADO
Financiero	Pérdida de recursos económicos que pueden afectar la continuidad del negocio. (Porcentaje definido sobre la utilidad operacional de la línea de negocio)	Entre 0% y 0.9%	**1**
		Entre 1% y 10%	**2**
		Entre 11% y 20%	**3**
		Superior al 20%	**4**
Jurídicos	Incumplimiento de la ley de protección de datos o del contrato ocasionando demandas legales por parte de sus clientes.	No se presenta una afectación al interior de la organización.	**1**
		Genera procesos de auditoria y/o control interno para determinar las acciones correctivas y preventivas según aplique.	**2**
		Cancelación del contrato del personal que afecto el activo de información.	**3**
		Inicio de un proceso penal por afectación de la confidencialidad, integridad y/o disponibilidad de la información.	**4**
Imagen Corporativa	Pérdida de prestigio y buen nombre de la organización ante sus clientes, proveedores y terceros.	No hay una afectación en la imagen de la organización.	**1**
		Es conocido de manera interna solo por el área de desarrollo.	**2**
		Afectación de la imagen al interior de la organización, sin ser de dominio público.	**3**
		Desprestigio de la organización ante terceros (Clientes, Proveedores y demás).	**4**

Tabla 6 - Criterios de valoración de los activos de información

Valorando la afectación que puede tener la pérdida parcial y/o total de confidencialidad, integridad y /o disponibilidad a nivel financiero, jurídico y de imagen corporativa se determina el nivel de criticidad del activo relacionado con el sistema de información aplicando la siguiente ponderación.

ASPECTO	VALOR DE CRITICIDAD DEL ACTIVO	NIVEL DE CRITICIDAD
Cuando el promedio de valoración del activo en términos de confidencialidad, integridad y disponibilidad es igual a 1	Muy bajo	**Es igual a 1**
Cuando el promedio de valoración del activo en términos de confidencialidad, integridad y disponibilidad es mayor a 1 y menor a 2	Bajo	**> 1 y <=2**

ASPECTO	VALOR DE CRITICIDAD DEL ACTIVO	NIVEL DE CRITICIDAD
Cuando el promedio de valoración del activo en términos de confidencialidad, integridad y disponibilidad es mayor a 2 y menor a 3	Medio	**>2 y <= 3**
Cuando el promedio de valoración del activo en términos de confidencialidad, integridad y disponibilidad es mayor a 3 y menor a 4	Alto	**> 3 y <= 4**

Tabla 7 - Nivel de criticidad del activo de información

Acorde al procedimiento descrito para clasificación y valoración de los activos relacionados con el sistema de información se visualiza en la siguiente tabla el nivel de criticidad de los activos.

IDENTIFICACIÓN DEL ACTIVO DE INFORMACIÓN		CONFIDENCIALI-DAD			INTEGRIDAD			DISPONIBILIDAD			CONSOLIDADO DE VALORACIÓN			
N. ACTIVO	NOMBRE DEL ACTIVO	FINANCIERO	JURIDICO	IMAGEN	FINANCIERO	JURIDICO	IMAGEN	FINANCIERO	JURIDICO	IMAGEN	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBLIDAD	CRITICIDAD DEL ACTIVO
GD - A1	Software de control de versiones (Subversión y GIT)	4	1	4	4	2	1	4	4	3	4	4	4	Alto
GD - A2	Metodología de desarrollo	1	1	2	1	1	2	1	1	1	2	2	1	Bajo
GD - A3	Código fuente	4	4	4	4	4	4	4	4	4	4	4	4	Alto
GD - A4	Servidor de aplicaciones	3	2	3	3	2	3	4	2	3	3	3	4	Alto
GD - A5	Servidor de bases de datos	4	4	4	4	4	4	4	4	4	4	4	4	Alto
GD - A6	Servidor de imágenes	4	4	4	4	4	4	4	4	4	4	4	4	Alto
GD - A7	Portátiles	2	2	2	1	2	2	1	2	2	2	2	2	Bajo
GD - A8	Computadores de escritorio desarrolladores	2	2	2	1	2	2	1	2	2	2	2	2	Bajo
GD - A9	Dispositivos de red	4	4	3	4	2	3	4	2	3	4	4	4	Alto
GD - A10	Cuarto de equipos	4	2	3	2	2	3	3	2	3	4	3	3	Alto
GD - A11	Desarrolladores	3	4	4	2	3	2	1	2	2	4	3	2	Medio
GD - A12	Red de área local - LAN	4	4	3	4	2	3	4	2	3	4	4	4	Alto
GD - A13	Red Inalámbrica - WLAN	4	4	3	4	2	3	4	2	3	4	4	4	Alto
GD - A14	Servicio de File Systems	4	4	4	4	4	4	4	4	4	4	4	4	Alto

IDENTIFICACIÓN DEL ACTIVO DE INFORMACIÓN		CONFIDENCIALI-DAD			INTEGRIDAD			DISPONIBILIDAD			CONSOLIDADO DE VALORACIÓN			
N. ACTIVO	NOMBRE DEL ACTIVO	FINANCIERO	JURIDICO	IMAGEN	FINANCIERO	JURIDICO	IMAGEN	FINANCIERO	JURIDICO	IMAGEN	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBLIDAD	CRITICIDAD DEL ACTIVO
GD - A15	Interfaz de desarrollo (Netbeans con lenguaje de programación Java)	4	4	4	4	4	4	4	4	4	4	4	4	Alto
GD - A16	Sistemas operativos	1	1	1	1	2	2	1	2	2	1	2	2	Bajo
GD - A17	Antivirus	4	2	4	2	2	3	4	4	4	4	3	4	Alto
GD - A18	Aplicativo de gestión documental	4	4	4	4	4	4	3	2	4	4	4	4	Alto
GD - A19	Sistemas de gestión de bases de datos	4	4	4	4	4	4	4	4	4	4	4	4	Alto
GD - A20	Medios de almacenamiento electrónico (USB, Discos duros externos)	2	4	4	1	2	2	1	1	1	4	2	1	Medio

Tabla 8 - Valoración de activos relacionados con el sistema de información del aplicativo de gestión documental

Los activos asociados con el sistema de información del software de gestión documental a seleccionar para el análisis de riesgos son aquellos que tienen nivel de criticidad medio y alto. A continuación se agrupan los activos de acuerdo a su relación funcional.

IDENTIFICACIÓN DEL ACTIVO DE INFORMACIÓN			
N. ACTIVO	NOMBRE DEL ACTIVO	CRITICIDAD DEL ACTIVO	CONTENEDOR Y/O ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANALISIS DE RIESGOS
GD - A1	Software de control de versiones (Subversión y GIT)	Alto	Código fuente
GD - A3	Código fuente	Alto	
GD - A15	Interfaz de desarrollo (Netbeans con lenguaje de programación Java)	Alto	
GD - A18	Aplicativo de gestión documental	Alto	Aplicación de gestión documental
GD - A4	Servidor de aplicaciones	Alto	Servidores
GD - A5	Servidor de bases de datos	Alto	
GD - A19	Sistemas de gestión de bases de datos	Alto	

IDENTIFICACIÓN DEL ACTIVO DE INFORMACIÓN			
N. ACTIVO	NOMBRE DEL ACTIVO	CRITICIDAD DEL ACTIVO	CONTENEDOR Y/O ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANALISIS DE RIESGOS
GD - A6	Servidor de imágenes	Alto	
GD - A14	Servicio de File Systems	Alto	
GD - A9	Dispositivos de red	Alto	Cuarto de infraestructura tecnológica (Cuarto de Equipos)
GD - A10	Cuarto de equipos	Alto	
GD - A12	Red de área local - LAN	Alto	Red LAN corporativa
GD - A13	Red Inalámbrica - WLAN	Alto	
GD - A17	Antivirus	Alto	Antivirus
GD - A20	Medios de almacenamiento electrónico (USB, Discos duros externos)	Medio	Unidades de almacenamiento de información
GD - A11	Desarrolladores	Medio	Talento humano

Tabla 9 - Activos objeto de análisis de riesgos

4.3.2 METODOLOGÍA A EMPLEAR PARA EL ANÁLISIS DE RIESGOS

Teniendo presente el objeto organizacional de la empresa propietaria del software, se describe a continuación la metodología a emplear como guía para realizar el análisis de riesgos de seguridad de la información a los cuales se encuentra expuesto el software de gestión documental. Las actividades descritas a continuación se establecieron teniendo como referencia la Metodología de análisis y gestión de riesgos de los sistemas de información MAGERIT.

Las actividades que comprende la metodología son:

- ✓ Identificación de vulnerabilidades y amenazas sobre los activos asociados a la información así como su respectivo impacto.
- ✓ Definición de los riesgos de seguridad.
- ✓ Establecer la cuantificación de la probabilidad de ocurrencia del riesgo y el impacto que puede generar para la organización la materialización del riesgo.
- ✓ Construir la matriz de riesgos inherente.
- ✓ Diseñar el plan de tratamiento y gestión de riesgos de seguridad de la información

A continuación se evidencia el desarrollo de las actividades descritas.

4.3.2.1 Identificación de vulnerabilidades y amenazas

Acorde a los activos seleccionados para realizar el análisis de riesgos definidos en la tabla N.9, se realizó la identificación de vulnerabilidades, amenazas y posibles consecuencias de la materialización de una amenaza sobre alguna vulnerabilidad a partir de la información recopilada en la fase de análisis.

CONTENEDOR Y/O ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANALISIS DE RIESGOS	CAUSAS		CONSECUENCIAS (IMPACTO)
	VULNERABILIDADES	AMENAZAS	
Código fuente	• Ausencia de una metodología de desarrollo de software seguro. • El desarrollo de nuevas funcionalidades del software de gestión documental no quedan documentadas y/o actualizadas en el aplicativo de control de versiones, permaneciendo de manera local en el equipo del desarrollador. • No se encuentra documentado los lineamientos de seguridad implementados en el desarrollo de software de gestión documental. • No hay definido un plan detallado de pruebas de seguridad a efectuar en las etapas del desarrollo de software. • No se realizan pruebas de seguridad sobre el software que permitan detectar vulnerabilidades de seguridad. • El aplicativo no encripta la información para su transmisión a través de la red. • Ausencia de un plan de tratamiento de incidentes de seguridad.	• Manipulación intencionada interna o externa de las fuentes de información ocasionando pérdida parcial y/o total del código fuente del aplicativo de gestión documental. • Hurto o pérdida de información causada por parte de un empleado descontento de la entidad. • Indisponibilidad de acceso a los repositorios o contenedores de información como la subversión o el GIF. • Secuestro de la información relacionada con el código fuente efectuado por un tercero a través de un malware.	• Eliminación de información clave para el negocio afectando la disponibilidad de la misma para el desarrollo de las actividades concernientes al negocio. • Manipulación no autorizada de la información que puede conllevar a la afectación del negocio y pérdida de clientes y negocios importantes para la entidad. • Afectación de la operación de la organización debido a la indisponibilidad de la información. • Divulgación de información no autorizada por terceros por asignación excesiva de permisos sobre un rol. • Divulgación de información no autorizada por terceros, que favorezcan a la competencia, afectando la imagen corporativa de la entidad.
Aplicativo de gestión documental	• Cuando el aplicativo funciona bajo cliente servidor, la instalación del aplicativo en los equipos clientes genera un archivo de configuración que puede modificar el comportamiento de la aplicación. • El entorno web del aplicativo de gestión documental funciona bajo http, donde la transferencia de información se encuentra en texto claro. • Ausencia de configuraciones de seguridad en el aplicativo que permita solicitar el cambio de la contraseña con el aprovisionamiento del servicio de un usuario nuevo. • El aplicativo maneja un nivel de complejidad débil en el	• Ataques internos y/o externos al aplicativo de gestión documental capturando usuarios y contraseñas de acceso válidos. • Suplantación de identidad ocasionando perdida de información contenida en el sistema de gestión documental. • Alteración por terceros no autorizados del archivo de configuración en la estructura cliente servidor que modifica el comportamiento de la aplicación.	• Pérdida de clientes debido a la sustracción y divulgación no autorizada de información confidencial alojada en el aplicativo de gestión documental. • Desprestigio de la organización en el sector productivo debido a la explotación de las debilidades existentes por un tercero sobre el aplicativo de gestión documental. • Afectación en los ingresos económicos debido a la divulgación de las vulnerabilidades de seguridad del aplicativo

CONTENEDOR Y/O ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANALISIS DE RIESGOS	CAUSAS		CONSECUENCIAS (IMPACTO)
	VULNERABILIDADES	AMENAZAS	
	establecimiento de las contraseñas de usuario debido a: No hay restricción mínima de la cantidad de caracteres que debe poseer la contraseña, el historial de contraseñas almacena solo las dos últimas contraseñas establecidas, no solicita la combinación de caracteres alfanuméricos en la contraseña. • El software no cuenta con lineamientos de seguridad que establezca una frecuencia de renovación y cambio del password por parte del usuario. • Visualización del código fuente de la aplicación de gestión documental por medio del navegador web, situación que puede provocar la pérdida de confidencialidad del código fuente produciendo fugas de información que pueden afectar la exclusividad de funcionalidades en el aplicativo de gestión documental ya que estas pueden ser integradas en software de la competencia.		de gestión documental por personal interno y/o externo de la organización.
Servidores	• El sistema operativo de red instalado en algunos servidores no se encuentra licenciado ni actualizado. • Ausencia de configuraciones de seguridad en los servidores. • No se realiza un monitoreo constante de los eventos y registro de logs que permitan detectar posibles intrusiones y/o debilidades de seguridad. • El respaldo de backup se encuentra ubicado en los mismos servidores a los cuales les establecen las copias de respaldo. • La configuración y administración de los servidores no se encuentra centralizada. • El antivirus instalado en los servidores no se encuentra activo ni actualizado. • Ausencia de sistemas de control ambiental que permitan controlar variables como temperatura y humedad relativa en	• Manipulación intencionada interna o externa sobre los servidores ocasionando pérdida parcial y/o total de la información alojada en los equipos. • Presentación de condiciones inadecuadas de temperatura y humedad que generan daños sobre la infraestructura física. • Indisponibilidad temporal en el acceso la información contenida en los servidores generada por un tercero no autorizado. • Modificación y/o alteración de la información y los servicios alojados en los servidores por un empleado con exceso de privilegios. • Fallos no intencionales causado por un empleado de la organización.	• Eliminación de información clave para el negocio afectando la disponibilidad de la misma para el desarrollo de las actividades concernientes al negocio. • Manipulación no autorizada de las configuraciones de los servicios de red, afectando la disponibilidad del servicio a los empleados de la organización. • Perdida de información que puede conllevar a la afectación del negocio y pérdida de clientes y negocios importantes para la entidad. • Afectación de la operación de la organización debido a la indisponibilidad de la información. • Divulgación de información no autorizada

CONTENEDOR Y/O ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANALISIS DE RIESGOS	CAUSAS		CONSECUENCIAS (IMPACTO)
	VULNERABILIDADES	AMENAZAS	
	el área donde se encuentran instalados los servidores. • Deficiencia en la programación de actividades de mantenimiento preventivo sobre la infraestructura de red que permita prologar el funcionamiento de los equipos y salvaguardar la información. • No existen configuraciones de seguridad establecidas en los servidores ni en los servicios de red que han sido implementados a través de la red corporativa.		por terceros por asignación excesiva de permisos sobre los servidores.
Cuarto de infraestructura tecnológica (Cuarto de Equipos)	• Ausencia de un sistema de control de acceso. • No existen procedimientos establecidos para la restricción de acceso a la infraestructura física de la organización. • Ausencia de sistemas de control ambiental que permitan controlar variables como temperatura y humedad relativa en cuarto de equipos (Centro de cómputo). • No poseen un sistema de detección de humo, fuego y/o humedad instalado en el centro de cómputo.	• Hurto o pérdida de información causada por parte de un empleado descontento de la entidad. • Afectación temporal de la disponibilidad de la información y/o aplicativos alojados en los servidores causados por una falla no intencionada de un empleado de la organización. • Fuego – Posibilidad de que un incendio destruya los recursos y activos de la organización. • Daños causados por Agua – Escape, fuga o inundación que ocasione el daño de los recursos de la organización. • Presentación de condiciones inadecuadas de temperatura y humedad que generan daños sobre la infraestructura física.	• Eliminación de información clave para el negocio afectando la disponibilidad de la misma para el desarrollo de las actividades concernientes al negocio. • Perdida de información que puede conllevar a la afectación del negocio y pérdida de clientes y negocios importantes para la entidad. • Afectación de la operación de la organización debido a la indisponibilidad de la información por deterioro de los contenedores de información (Servidores). • Divulgación de información no autorizada por terceros por asignación ausencia de controles de acceso a los contenedores de información. • Hurto de infraestructura física que pueda contener activos de información que puedan colocar en riesgo la continuidad del negocio. • Hurto y/o daño de la infraestructura tecnológica (Servidores, Dispositivos de red, etc.) que se encuentra alojada en el cuarto de equipos debido a la ausencia de controles de acceso.

CONTENEDOR Y/O ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANALISIS DE RIESGOS	CAUSAS		CONSECUENCIAS (IMPACTO)
	VULNERABILIDADES	AMENAZAS	
Red LAN corporativa	• No hay un proceso establecido para la administración y gestión de identidades al interior de la organización. • Ausencia de procesos que establezcan los procedimientos para habilitar o deshabilitar las cuentas de usuario. • No existe un registro actualizado de los usuarios que tienen acceso a los aplicativos y servicios corporativos ni se identifica su estado (Activo, Bloqueado, Deshabilitado). • Deficiencias en las configuraciones de seguridad de la red inalámbrica, empleando un cifrado débil. • Ausencia de un administrador de red que configure, administre y gestione la red bajo criterios de seguridad de la información. • No existe una política de seguridad de la información. • Perdida de confidencialidad de información que puede ser sensible para la entidad debido a que es compartida a través de la infraestructura de red de la organización, permitiendo su visualización a personas no autorizadas.	• Fuga de información debido al acceso de usuarios no autorizados a la infraestructura de red de la organización. • Indisponibilidad del servicio de la red inalámbrica debido a ataques de denegación de servicios (DoS). • Terceros realizan procesos de suplantación de identidad para acceder a los aplicativos tecnológicos de la entidad que se encuentran disponibles a través de la red de datos corporativa. • Empleados descontentos pueden hacer uso de usuarios y contraseñas de personal que ya no labora en la entidad para visualizar y/o sustraer información confidencial de la entidad.	• Perdida de disponibilidad, integridad y confidencialidad de la información de la entidad, generando un impacto negativo en la continuidad del negocio. • Afectación en los ingresos económicos de la organización debido a la pérdida de clientes a causa de la divulgación no autorizada de información a la competencia. • Indisponibilidad de los servicios que se brindan a través de la red ocasionando tiempos no productivos del equipo de desarrollo de la organización. • Desprestigio de la imagen corporativa debido a la divulgación no autorizada de información confidencial por parte del personal interno y/o externo de la entidad.
Antivirus	• No se encuentran activos ante la firma propietaria del software, ni actualizados.	• Fuga y/o pérdida de información generada por código malicioso. • Divulgación no autorizada de información debido a acceso de terceros a través del uso de malware. • Indisponibilidad de la información generado por virus informáticos. • Secuestro de información generado por una aplicación ramsomware. • Daño de hardware ocasionado por código	• Afectación de la continuidad del negocio debido al secuestro de la información ocasionado por código malicioso. • Afectación de los ingresos económicos de lo entidad, generados por la indisponibilidad parcial y/o total del código fuente del aplicativo de gestión documental. • Sustracción no autorizada de información confidencial de la organización, afectando la continuidad del negocio. • Daño de hardware ocasionado por código

CONTENEDOR Y/O ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANALISIS DE RIESGOS	CAUSAS		CONSECUENCIAS (IMPACTO)
	VULNERABILIDADES	AMENAZAS	
		malicioso.	malicioso, provocando a la organización la asignación de presupuesto extra para la reposición del hardware.
Unidades de almacenamiento de información	• No se establece ningún proceso de cifrado de información en unidades de almacenamiento externas como USB, discos duros (Internos y/o externos). • Ausencia de niveles de protección física sobre los dispositivos de almacenamiento externo. • No se realizan procesos de borrado seguro de la información contenida en las unidades de almacenamiento de información.	• Pérdida y/o fuga de información confidencial de la organización por hurto de unidades de almacenamiento de información externos.	• Divulgación por terceros de información confidencial de la organización generando problemas de índole legal y reputacional a la entidad. • Perdida de información ocasionada accidentalmente, generando pérdida de imagen corporativa ante terceros.
Talento humano	• Ausencia de capacitación al personal en temas relacionados con desarrollo de software seguro. • Ausencia de un programa de sensibilización al personal sobre la importancia de su rol en la seguridad de la información. • No se establecen acuerdos de confidencialidad y protección de la propiedad intelectual y corporativa entre la empresa y sus empleados directos, contratistas, etc. • Algunos desarrolladores no realizan la actualización en la subversión de nuevas funcionalidades del aplicativo de gestión documental, generando retrocesos en las actividades del área de desarrollo. • Exceso de confianza de los empleados con su entorno (Dentro y fuera de las instalaciones de la entidad). • No hay lineamientos claros de seguridad orientados al personal debido a la ausencia de una política de seguridad de la información.	• Empleado descontento de la organización. • Ex-empleado de la organización aun con accesos y privilegios habilitados para acceder a la infraestructura física y lógica de la organización. • Terceros interesados en generar ataques que provoquen la indisponibilidad del servicio y/o producto que brinda la empresa.	• Fuga de información que puede llegar a manos de la competencia, quien la utiliza en beneficio propio para brindar mejores propuestas de valor a los clientes de la empresa que fue víctima de la sustracción de información. • Divulgación no autorizada de terceros de información confidencial de clientes, generándole a la entidad problemas de índole legal por divulgación de información no autorizada y confidencial. • Desprestigio de la organización por divulgación de información confidencial de los clientes de la organización.

Tabla 10 – Determinación de vulnerabilidades y amenazas sobre los activos objeto de análisis de riesgos.

4.3.2.2 Definición de riesgos de seguridad

Acorde a la identificación de vulnerabilidades y amenazas sobre los activos seleccionados objeto del análisis de riesgos, se establecen los riesgos de seguridad a los cuales se encuentra expuesta los activos y/o contenedores de información asociados al software de gestión documental objeto del presente documento de grado.

CONTENEDOR Y/O ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANALISIS DE RIESGOS	RIESGOS DE SEGURIDAD
Código fuente	**R1** - Pérdida parcial de información asociada a nuevas funcionalidades y/o actualizaciones del aplicativo de gestión documental provocado por la falta de actualización de la subversión por parte de los desarrolladores.
	R2 - Alteración y/o pérdida de información por deficiencias en los controles de acceso físicos y lógicos a los repositorios de información de la organización.
	R3 - Indisponibilidad de la información provocado por deficiencias en los controles de acceso lógicos a los repositorios de información que contienen el software de gestión documental.
	R4 - Deterioro de la imagen corporativa de la entidad por la divulgación no autorizada de las falencias existentes en el aplicativo de gestión documental.
Aplicativo de gestión documental	**R5** - Sustracción y/o pérdida de información contenida en el aplicativo de gestión documental, debido al uso de protocolos inseguros utilizados en la publicación del entorno web del software.
	R6 - Perdida de confidencialidad de la información contenida en el aplicativo de gestión documental por la ausencia de lineamientos de seguridad en el software que soliciten el cambio de contraseña a nuevos usuarios que han sido aprovisionados por el administrador del aplicativo.
	R7 - Sustracción y/o perdida de información contenida en el aplicativo de gestión documental causada por la ausencia de lineamientos de seguridad en el software que definan una frecuencia de renovación y un nivel de complejidad en el establecimiento de los password por parte de los usuarios del aplicativo.
	R8 - Incumplimiento de acuerdos de servicio con clientes debido a la indisponibilidad del aplicativo de gestión documental a causa de la explotación de las debilidades existentes por un tercero sobre el software de gestión documental.
	R9 - Divulgación y/o pérdida de información no autorizada por terceros a causa de asignación excesiva de permisos sobre un rol.
Servidores	**R10** - Perdida de información de la organización debido a la ausencia de procedimientos que establezcan los lineamientos y buenas prácticas de seguridad para realizar backup de la información.

CONTENEDOR Y/O ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANALISIS DE RIESGOS	RIESGOS DE SEGURIDAD
	R11 - Afectación de la confidencialidad e integridad de la información a causa de una inadecuada gestión de identidades y control de acceso a los recursos y repositorios de información de la organización.
	R12 - Perdida de información y afectación del servicio por desactualización de sistemas operativos y antivirus en los servidores.
	R13 - Indisponibilidad de la información alojada en los servidores por deterioro físico causado por la ausencia de planes de mantenimiento preventivo sobre el hardware.
	R14 - Tiempos laborales muertos causados por la indisponibilidad de la información y servicios debido a la ausencia de configuraciones de seguridad en los servidores.
Cuarto de infraestructura tecnológica (Cuarto de Equipos)	**R15** - Daño o hurto de infraestructura tecnológica afectando la operatividad de la organización por inadecuados controles de acceso físico al centro de cómputo.
	R16 - Indisponibilidad de la información causado por el deterioro del equipamiento informático debido a la ausencia de sistemas de control de condiciones ambientales como temperatura y humedad.
	R17 - Tiempos de inactividad en las operaciones de la organización, debido al daño o ausencia de sistemas de respaldo eléctrico a la infraestructura de red de la organización.
	R18 - Deterioro parcial y/o total de la infraestructura tecnológica del centro de cómputo causada por la presencia de fuego en el recinto.
Red LAN corporativa	**R19** - Sustracción y/o pérdida de información sensible de la organización debido a la ausencia de políticas y controles en el establecimiento de contraseñas de acceso a los dispositivos tecnológicos de la entidad.
	R20 - Indisponibilidad de la información y/o servicios que se acceden a través de la red corporativa por deficiencias en su diseño e implementación.
Antivirus	**R21** - Pérdida parcial y/o total de información provocado por la desactualización y/o ausencia de antivirus.
	R22 - Daño de hardware provocado por código malicioso debido a la desactualización de los antivirus.
	R23 - Afectación de la operatividad de la red corporativa debido a la presencia de malware.
Unidades de almacenamiento de información	**R24** - Pérdida de clientes por divulgación no autorizada de información debido a la ausencia de mecanismos de cifrado de información sobre unidades de almacenamiento electrónico.
Talento humano	**R25** - Sustracción y/o pérdida de la información sensible de la organización debido a la ausencia de acuerdos de confidencialidad y protección de la propiedad intelectual entre la empresa y sus empleados directos, aprendices, practicantes y aliados estratégicos.

Tabla 11 - Riesgos de seguridad de la información

4.3.2.3 Cuantificación de la probabilidad e impacto a emplear en la valoración de los riesgos.

Para efectuar la valoración de los riesgos es importante realizar previamente el respectivo análisis de los hallazgos detectados en cada una de las situaciones descritas que afectan la seguridad de la información, teniendo presente la probabilidad de ocurrencia del riesgo y el impacto que puede generar para la organización la materialización del riesgo. En conjunto con la organización se establecieron las escalas a emplear para realizar la respectiva valoración de los riesgos descritos en el tabla 11.

PROBABILIDAD	FRECUENCIA DE OCURRENCIA	VALOR
Muy Bajo	Por lo menos una vez cada año	1
Bajo	Por lo menos una vez cada semestre	2
Medio	Por lo menos una vez cada trimestre	3
Alto	Por lo menos una vez cada mes	4
Muy Alto	Por lo menos una vez cada quince días	5

Tabla 12 – Valoración de la probabilidad en términos de ocurrencia a través del tiempo.

La valoración del impacto se realizó teniendo en cuenta la afectación a nivel económico y operativo al interior de la organización.

IMPACTO	DESCRIPCION DEL IMPACTO	IMPACTO CUALITATIVO	VALOR
Muy Bajo	Pérdida económica de entre el 0.1 y 0.4 % del presupuesto anual. Disminución en la prestación del servicio entre un 0.1% y 4.9%	• No afecta la seguridad de la información de la entidad. • No hay afectación de la imagen de la entidad ante los clientes y terceros. • Se puede recuperar la información con la misma calidad. • Se presentan reprocesos que no tienen mayor importancia.	1
Bajo	Pérdida económica de entre el 0.5 y 0.9 % del presupuesto anual. Disminución en la prestación del servicio entre un 5% y 9.9%	• No afecta la seguridad de la información de la entidad. • Se presenta una leve afectación a la imagen de la entidad ante los clientes y terceros. • Se puede recuperar la información con la misma calidad en un tiempo moderado. • Se presentan reprocesos menores en las actividades de la entidad.	2

IMPACTO	DESCRIPCION DEL IMPACTO	IMPACTO CUALITATIVO	VALOR
Medio	Pérdida económica de entre el 1 y 10% del presupuesto anual. Disminución en la prestación del servicio entre un 10% y 20%	• Hay una afectación en menor grado de la seguridad de la información de la entidad. • Afecta medianamente la imagen corporativa de la entidad ante sus clientes y terceros. • Se presentan retrocesos moderados en las actividades. • La información se puede recuperar pero no con la misma calidad.	3
Alto	Pérdida económica de entre el 11 y 20% del presupuesto anual. Disminución en la prestación del servicio entre un 21% y 29.9%	• Se genera una afectación importante en la seguridad de la información de la entidad. • Afecta altamente la imagen corporativa de la entidad. • Se generan mayores retrocesos en las actividades. • Es difícil de recuperar la información.	4
Muy Alto	Pérdida económica superior al 20% del presupuesto anual. Disminución en la prestación del servicio hasta en un 50%	• Se presenta una afectación crítica a la seguridad de la información. • Se afecta negativamente y en gran proporción la imagen corporativa de la entidad ante terceros. • Es difícil realizar la recuperación de la información. • Puede afectar las decisiones estratégicas de la organización y la continuidad del negocio.	5

Tabla 13 – Valoración del impacto en términos económicos y operativos para la organización.

La valoración de los riesgos en términos de probabilidad e impacto de ocurrencia se obtiene de aplicar la siguiente ecuación.

$$Riesgo\ Inherente = \text{Probabilidad} * \text{Impacto} \qquad \textit{(Ecuación 1)}$$

PROBABILIDAD	IMPACTO				
	Muy Bajo	Bajo	Medio	Alto	Muy Alto
Muy Bajo	Muy bajo	Muy bajo	Bajo	Bajo	Medio
Bajo	Muy bajo	Bajo	Medio	Medio	Alto
Medio	Bajo	Medio	Medio	Alto	Alto
Alto	Bajo	Medio	Alto	Critico	Critico
Muy Alto	Medio	Alto	Alto	Critico	Critico

PROBABILIDAD	IMPACTO				
	Muy Bajo (1)	Bajo (2)	Medio (3)	Alto (4)	Muy Alto (5)
Muy Bajo (1)	1	2	3	4	5
Bajo (2)	2	4	6	8	10
Medio (3)	3	6	9	12	15
Alto (4)	4	8	12	16	20
Muy Alto (5)	5	10	15	20	25

Tabla 14 – Valoración del riesgo en términos de probabilidad e impacto.

VALORACIÓN DEL RIESGO	CALIFICACIÓN
Muy bajo	1 – 2
Bajo	3 - 4
Medio	5 - 9
Alto	10 - 15
Critico	16 - 25

Tabla 15 – Ponderación de la valoración del riesgo.

Acorde a la valoración establecida para el riesgo inherente en términos de probabilidad de ocurrencia e impacto se obtienen los siguientes resultados:

CONTENEDOR Y/O ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANALISIS DE RIESGOS	RIESGOS DE SEGURIDAD	VALORACIÓN DEL RIESGO			
		PROBABILIDAD	IMPACTO	CALIFICACIÓN	NIVEL DEL RIESGO
Código fuente	**R1** - Pérdida parcial de información asociada a nuevas funcionalidades y/o actualizaciones del aplicativo de gestión documental provocado por la falta de actualización de la subversión por parte de los desarrolladores.	4	3	12	Alto
	R2 - Alteración y/o pérdida de información por deficiencias en los controles de acceso físicos y lógicos a los repositorios de información de la organización.	2	5	10	Alto
	R3 - Indisponibilidad de la información provocado por deficiencias en los controles de acceso lógicos a los repositorios de información que contienen el software de gestión documental.	2	3	6	Medio
	R4 - Deterioro de la imagen corporativa de la entidad por la divulgación no autorizada de las falencias existentes en el aplicativo de gestión documental.	2	5	10	Alto

CONTENEDOR Y/O ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANALISIS DE RIESGOS	RIESGOS DE SEGURIDAD	VALORACIÓN DEL RIESGO			
		PROBABILIDAD	IMPACTO	CALIFICACIÓN	NIVEL DEL RIESGO
Aplicativo de gestión documental	**R5** - Sustracción y/o pérdida de información contenida en el aplicativo de gestión documental, debido al uso de protocolos inseguros utilizados en la publicación del entorno web del software.	2	4	8	Medio
	R6 - Perdida de confidencialidad de la información contenida en el aplicativo de gestión documental por la ausencia de lineamientos de seguridad en el software que soliciten el cambio de contraseña a nuevos usuarios que han sido aprovisionados por el administrador del aplicativo.	2	4	8	Medio
	R7 - Sustracción y/o perdida de información contenida en el aplicativo de gestión documental causada por la ausencia de lineamientos de seguridad en el software que definan una frecuencia de renovación y un nivel de complejidad en el establecimiento de los password por parte de los usuarios del aplicativo.	2	4	8	Medio
	R8 - Incumplimiento de acuerdos de servicio con clientes debido a la indisponibilidad del aplicativo de gestión documental a causa de la explotación de las debilidades existentes por un tercero sobre el software de gestión documental.	2	4	8	Medio
	R9 - Divulgación y/o pérdida de información no autorizada por terceros a causa de asignación excesiva de permisos sobre un rol.	4	3	12	Alto
Servidores	**R10** - Perdida de información de la organización debido a la ausencia de procedimientos que establezcan los lineamientos y buenas prácticas de seguridad para realizar backup de la información.	3	4	12	Alto
	R11 - Afectación de la confidencialidad e integridad de la información a causa de una inadecuada gestión de identidades y control de acceso a los recursos y repositorios de información de la organización.	3	4	12	Alto
	R12 - Perdida de información y afectación de los servicios por desactualización de sistemas operativos y antivirus en los servidores.	3	4	12	Alto
	R13 - Indisponibilidad de la información alojada en los servidores por deterioro físico causado por la ausencia de planes de mantenimiento preventivo sobre el hardware.	2	4	8	Medio
	R14 - Tiempos laborales muertos causados por la indisponibilidad de la información y servicios debido a la ausencia de configuraciones de seguridad en los servidores.	1	2	2	Muy bajo

CONTENEDOR Y/O ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANALISIS DE RIESGOS	RIESGOS DE SEGURIDAD	VALORACIÓN DEL RIESGO			
		PROBABILIDAD	IMPACTO	CALIFICACIÓN	NIVEL DEL RIESGO
Cuarto de infraestructura tecnológica (Cuarto de Equipos)	**R15** - Daño o hurto de infraestructura tecnológica afectando la operatividad de la organización por inadecuados controles de acceso físico al centro de cómputo.	2	3	6	Medio
	R16 - Indisponibilidad de la información causado por el deterioro del equipamiento informático debido a la ausencia de sistemas de control de condiciones ambientales como temperatura y humedad.	2	3	6	Medio
	R17 - Tiempos de inactividad en las operaciones de la organización, debido al daño o ausencia de sistemas de respaldo eléctrico a la infraestructura de red de la organización.	3	3	9	Medio
	R18 - Deterioro parcial y/o total de la infraestructura tecnológica del centro de cómputo causada por la presencia de fuego en el recinto.	2	5	10	Alto
Red LAN corporativa	**R19** - Sustracción y/o pérdida de información sensible de la organización debido a la ausencia de políticas y controles en el establecimiento de contraseñas de acceso a los dispositivos tecnológicos de la entidad.	2	5	10	Alto
	R20 - Indisponibilidad de la información y/o servicios que se acceden a través de la red corporativa por deficiencias en su diseño e implementación.	2	3	6	Medio
Antivirus	**R21** - Pérdida parcial y/o total de información provocado por la desactualización y/o ausencia de antivirus.	3	4	12	Alto
	R22 - Daño de hardware provocado por código malicioso debido a la desactualización de los antivirus.	2	3	6	Medio
	R23 - Afectación de la operatividad de la red corporativa debido a la presencia de malware.	2	4	8	Medio
Unidades de almacenamiento de información	**R24** - Pérdida de clientes por divulgación no autorizada de información debido a la ausencia de mecanismos de cifrado de información sobre unidades de almacenamiento electrónico.	3	5	15	Alto
Talento humano	**R25** - Sustracción y/o pérdida de la información sensible de la organización debido a la ausencia de acuerdos de confidencialidad y protección de la propiedad intelectual entre la empresa y sus empleados directos, aprendices, practicantes y aliados estratégicos.	3	5	15	Alto

Tabla 16 – Valoración de los riesgos de seguridad asociados a los activos de información

La valoración de los riesgos en términos de probabilidad e impacto para la organización, permitió establecer el mapa de calor de los riesgos de seguridad de la información contemplados en el presente análisis, obteniendo el siguiente consolidado.

PROBABILIDAD	IMPACTO				
	Muy Bajo (1)	Bajo (2)	Medio (3)	Alto (4)	Muy Alto (5)
Muy Bajo (1)		2			
Bajo (2)			6	8	10
Medio (3)			9	12	15
Alto (4)			12		
Muy Alto (5)					

PROBABILIDAD	IMPACTO				
	Muy Bajo (1)	Bajo (2)	Medio (3)	Alto (4)	Muy Alto (5)
Muy Bajo (1)		R14			
Bajo (2)			R3, R15 R16 R20, R22	R5, R6 R7, R8 R13, R23	R2, R4, R18, R19
Medio (3)			R17	R10, R11 R12, R21	R24, R25
Alto (4)			R1, R9		
Muy Alto (5)					

Tabla 17 – Mapa de calor con la ubicación de los riesgos inherentes.

4.3.3 PLAN DE TRATAMIENTO Y GESTIÓN DE LOS RIESGOS

Dando continuidad a la metodología establecida se describe a continuación el procedimiento a emplear para definir el plan de tratamiento y gestión de los riesgos asociados a los activos de información, el cual tendrá como alcance diseñar y documentar las acciones de mejora que permitan controlar y disminuir los riesgos de seguridad a los que están expuestos los activos de información.

Es importante resaltar que la organización propietaria del software de gestión documental actualmente no tiene implementado controles existentes que mitiguen los riesgos de seguridad de la información descritos en el presente documento. Acorde a esto se plantea la estrategia de plan de tratamiento del riesgo descrita a continuación.

4.3.3.1 Estrategia de tratamiento del Riesgo

Con la valoración de los riesgos de seguridad identificados y descritos en la tabla N.16, se define la estrategia del tratamiento de riesgo acorde a los objetivos organizacionales y la importancia de la aplicación de gestión documental para la continuidad del negocio, permitiendo así determinar las acciones a realizar en cada uno de los riesgos identificados. A continuación se describe los parámetros a tener presentes en la estrategia de tratamiento del riesgo.

ÍTEM	ESTRATEGIA DE TRATAMIENTO DEL RIESGO	DESCRIPCIÓN
1	Evitar el riesgo	Está asociado a la suspensión de las actividades que causan el riesgo.
2	Reducir el riesgo	Se establecen los controles y salvaguardas necesarios para reducir el riesgo sobre el activo de información
3	Transferir el riesgo	Se transfiere el riesgo a terceros (Subcontratación) y/o se evalúa la opción de contar con seguros que cubran los gastos en caso de la materialización del riesgo.
4	Aceptar el riesgo	Se decide aceptar el riesgo, sin implementar controles adicionales para la protección del activo. En esta estrategia se emplean labores de monitorización continua del riesgo.

Tabla 18 – Descripción de la estrategia de tratamiento

Para establecer adecuadamente la estrategia de tratamiento del riesgo es fundamental evaluar el costo beneficio que tendrá para la organización el establecimiento de medidas de control que permitan salvaguardar los activos de información que se encuentran en riesgo. En la siguiente tabla se relaciona los aspectos de costo beneficio con la estrategia de tratamiento propuesta en la tabla 18.

ÍTEM	ESTRATEGIA DE TRATAMIENTO DEL RIESGO	COSTO - BENEFICIO
1	Evitar el riesgo	El costo de implementación de los controles es elevado en comparación con los beneficios obtenidos.
2	Reducir el riesgo	El costo de tratamiento e implementación de los controles es adecuado a los beneficios obtenidos.
3	Transferir el riesgo	El costo de tratamiento del riesgo es más económico y beneficioso para la organización que lo realice terceros, que si se realiza el tratamiento directo la empresa propietaria del riesgo.
4	Aceptar el riesgo	Se asume el riesgo, sin implementar nuevos controles que generen otro costo a la organización y el beneficio obtenido no sea proporcional. El costo asociado de aceptar el riesgo está enfocado a labores de monitoreo continuo del riesgo.

Tabla 19 – Descripción de la estrategia de tratamiento vs. Costo beneficio

De acuerdo a la descripción de la estrategia de tratamiento de los riesgos vs. Costo beneficio se analizó en cada uno de los riesgos el impacto que podría causar su materialización en la continuidad del negocio, estableciendo como estrategia de tratamiento en los riesgos de nivel medio y alto la reducción del riesgo; y en los riesgos valorados como “muy bajo” estos serán aceptados por la organización. A continuación se observa la estrategia de tratamiento seleccionada para cada riesgo identificado.

RIESGOS DE SEGURIDAD	NIVEL DEL RIESGO	ESTRATEGIA DE TRATAMIENTO DEL RIESGO
R1 - Pérdida parcial de información asociada a nuevas funcionalidades y/o actualizaciones del aplicativo de gestión documental provocado por la falta de actualización de la subversión por parte de los desarrolladores.	Alto	Reducir el riesgo
R2 - Alteración y/o pérdida de información por deficiencias en los controles de acceso físicos y lógicos a los repositorios de información de la organización.	Alto	Reducir el riesgo
R3 - Indisponibilidad de la información provocado por deficiencias en los controles de acceso lógicos a los repositorios de información que contienen el software de gestión documental.	Medio	Reducir el riesgo
R4 - Deterioro de la imagen corporativa de la entidad por la divulgación no autorizada de las falencias existentes en el aplicativo de gestión documental.	Alto	Reducir el riesgo
R5 - Sustracción y/o pérdida de información contenida en el aplicativo de gestión documental, debido al uso de protocolos inseguros utilizados en la publicación del entorno web del software.	Medio	Reducir el riesgo

RIESGOS DE SEGURIDAD	NIVEL DEL RIESGO	ESTRATEGIA DE TRATAMIENTO DEL RIESGO
R6 - Perdida de confidencialidad de la información contenida en el aplicativo de gestión documental por la ausencia de lineamientos de seguridad en el software que soliciten el cambio de contraseña a nuevos usuarios que han sido aprovisionados por el administrador del aplicativo.	Medio	Reducir el riesgo
R7 - Sustracción y/o perdida de información contenida en el aplicativo de gestión documental causada por la ausencia de lineamientos de seguridad en el software que definan una frecuencia de renovación y un nivel de complejidad en el establecimiento de los password por parte de los usuarios del aplicativo.	Medio	Reducir el riesgo
R8 - Incumplimiento de acuerdos de servicio con clientes debido a la indisponibilidad del aplicativo de gestión documental a causa de la explotación de las debilidades existentes por un tercero sobre el software de gestión documental.	Medio	Reducir el riesgo
R9 - Divulgación y/o pérdida de información no autorizada por terceros a causa de asignación excesiva de permisos sobre un rol.	Alto	Reducir el riesgo
R10 - Perdida de información de la organización debido a la ausencia de procedimientos que establezcan los lineamientos y buenas prácticas de seguridad para realizar backup de la información.	Alto	Reducir el riesgo
R11 - Afectación de la confidencialidad e integridad de la información a causa de una inadecuada gestión de identidades y control de acceso a los recursos y repositorios de información de la organización.	Alto	Reducir el riesgo
R12 - Perdida de información y afectación de los servicios por desactualización de sistemas operativos y antivirus en los servidores.	Alto	Reducir el riesgo
R13 - Indisponibilidad de la información alojada en los servidores por deterioro físico causado por la ausencia de planes de mantenimiento preventivo sobre el hardware.	Medio	Reducir el riesgo
R14 - Tiempos laborales muertos causados por la indisponibilidad de la información y servicios debido a la ausencia de configuraciones de seguridad en los servidores.	Muy bajo	Aceptar el riesgo
R15 - Daño o hurto de infraestructura tecnológica afectando la operatividad de la organización por inadecuados controles de acceso físico al centro de cómputo.	Medio	Reducir el riesgo
R16 - Indisponibilidad de la información causado por el deterioro del equipamiento informático debido a la ausencia de sistemas de control de condiciones ambientales como temperatura y humedad.	Medio	Reducir el riesgo
R17 - Tiempos de inactividad en las operaciones de la organización, debido al daño o ausencia de sistemas de respaldo eléctrico a la infraestructura de red de la organización.	Medio	Reducir el riesgo
R18 - Deterioro parcial y/o total de la infraestructura tecnológica del centro de cómputo causada por la presencia de fuego en el recinto.	Alto	Reducir el riesgo
R19 - Sustracción y/o pérdida de información sensible de la organización	Alto	Reducir el riesgo

RIESGOS DE SEGURIDAD	NIVEL DEL RIESGO	ESTRATEGIA DE TRATAMIENTO DEL RIESGO
debido a la ausencia de políticas y controles en el establecimiento de contraseñas de acceso a los dispositivos tecnológicos de la entidad.		
R20 - Indisponibilidad de la información y/o servicios que se acceden a través de la red corporativa por deficiencias en su diseño e implementación.	Medio	Reducir el riesgo
R21 - Pérdida parcial y/o total de información provocado por la desactualización y/o ausencia de antivirus.	Alto	Reducir el riesgo
R22 - Daño de hardware provocado por código malicioso debido a la desactualización de los antivirus.	Medio	Reducir el riesgo
R23 - Afectación de la operatividad de la red corporativa debido a la presencia de malware.	Medio	Reducir el riesgo
R24 - Pérdida de clientes por divulgación no autorizada de información debido a la ausencia de mecanismos de cifrado de información sobre unidades de almacenamiento electrónico.	Alto	Reducir el riesgo
R25 - Sustracción y/o pérdida de la información sensible de la organización debido a la ausencia de acuerdos de confidencialidad y protección de la propiedad intelectual entre la empresa y sus empleados directos, aprendices, practicantes y aliados estratégicos.	Alto	Reducir el riesgo

Tabla 20 – Estrategia de tratamiento seleccionada por riesgo identificado

4.3.3.2 Descripción del plan de acción

De acuerdo con la estrategia de tratamiento seleccionada en cada riesgo, se plantean los siguientes controles enfocados a reducir, mitigar y controlar los riesgos inherentes que se encuentran presentes en la herramienta de gestión documental objeto del presente trabajo de grado.

CONTENEDOR Y/O ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANALISIS DE RIESGOS	CARACTERIZACIÓN DEL RIESGO		QUE AFECTA			PLAN DE TRATAMIENTO DE RIESGOS			
	RIESGOS DE SEGURIDAD	NIVEL DEL RIESGO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBLIDAD	ESTRATEGIA DE TRATAMIENTO DEL RIESGO	IDENTIFICACIÓN DEL CONTROL	DESCRIPCION DEL PLAN DE ACCIÓN (CONTROLES)	RESPONSABLE
Código fuente	R1 - Pérdida parcial de información asociada a nuevas funcionalidades y/o actualizaciones del aplicativo de gestión documental provocado por la falta de actualización de la subversión por parte de los desarrolladores.	Alto			D	Reducir el riesgo	C1	Definir los procesos para documentación y actualización de las nuevas funcionalidades del aplicativo de gestión documental en la subversión, teniendo presente la política de seguridad de la información de la organización.	Líder de desarrollo
							C2	Estandarizar la versión del software utilizada por los desarrolladores en sus equipos de cómputo asignados.	Líder de desarrollo
							C3	Documentar el software de control de cambios, previa aprobación del líder de desarrollo.	Desarrolladores
	R2 - Alteración y/o pérdida de información por deficiencias en los controles de acceso físicos y lógicos a los repositorios de información de la organización.	Alto	C	I	D	Reducir el riesgo	C4	Realizar un inventario de los activos asociados a la información, estableciendo el responsable de la custodia de los activos.	Responsable del proceso y líder TI especialista en seguridad de la información
							C5	Clasificar la información de la organización, definiendo si es pública, privada o confidencial.	Responsable del proceso y líder TI especialista en seguridad de la información
							C6	Implementar controles de acceso físico y lógico que restrinjan los accesos no autorizados a los repositorios de información.	Líder TI especialista en seguridad de la información
	R3 - Indisponibilidad de la información provocado por deficiencias en los controles de acceso lógicos a los repositorios de información que contienen el software de	Medio			D	Reducir el riesgo	C7	Realizar monitoreo periódico que permita corroborar la efectividad de los controles lógicos implementados, aplicando las acciones correctivas necesarias para salvaguardar la información de la organización.	Líder TI especialista en seguridad de la información

CONTENEDOR Y/O ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANALISIS DE RIESGOS	CARACTERIZACIÓN DEL RIESGO		QUE AFECTA			PLAN DE TRATAMIENTO DE RIESGOS			
	RIESGOS DE SEGURIDAD	NIVEL DEL RIESGO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBLIDAD	ESTRATEGIA DE TRATAMIENTO DEL RIESGO	IDENTIFICACIÓN DEL CONTROL	DESCRIPCION DEL PLAN DE ACCIÓN (CONTROLES)	RESPONSABLE
	gestión documental.						C8	Realizar periódicamente pruebas de penetración que permitan identificar el nivel de protección de la infraestructura TI de la organización.	Líder TI especialista en seguridad de la información
	R4 - Deterioro de la imagen corporativa de la entidad por la divulgación no autorizada de las falencias existentes en el aplicativo de gestión documental.	Alto	C			Reducir el riesgo	C9	Actualizar y depurar los directorios existentes, identificando las cuentas de usuario que no cumplan con las políticas de seguridad, así como las cuentas huérfanas, en desuso y cuentas que carezcan de atributos que pueden ser relevantes para la gestión de identidades dentro de la organización.	Líder TI especialista en seguridad de la información
							C10	Establecer programas de capacitación y sensibilización al personal de la organización en temas relacionados con la seguridad de la información.	Líder TI especialista en seguridad de la información
Aplicativo de gestión documental	R5 - Sustracción y/o pérdida de información contenida en el aplicativo de gestión documental, debido al uso de protocolos inseguros utilizados en la publicación del entorno web del software.	Medio	C			Reducir el riesgo	C11	Crear y documentar una metodología de desarrollo de software seguro.	Líder de desarrollo y Líder TI especialista en seguridad de la información
							C12	Implementar la metodología de desarrollo de software seguro en el aplicativo de gestión documental.	Líder de desarrollo
							C13	Adquirir un certificado SSL con una entidad de certificación autorizada en el país.	CEO de la organización (Asignación del recurso), Líder de desarrollo y Líder TI especialista en seguridad de la información

CONTENEDOR Y/O ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANALISIS DE RIESGOS	CARACTERIZACIÓN DEL RIESGO		QUE AFECTA			PLAN DE TRATAMIENTO DE RIESGOS			
	RIESGOS DE SEGURIDAD	NIVEL DEL RIESGO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBLIDAD	ESTRATEGIA DE TRATAMIENTO DEL RIESGO	IDENTIFICACIÓN DEL CONTROL	DESCRIPCION DEL PLAN DE ACCIÓN (CONTROLES)	RESPONSABLE
							C14	Instalar y configurar adecuadamente el certificado SSL para la publicación del aplicativo de gestión documental a través del entorno web.	Líder de desarrollo y Líder TI especialista en seguridad de la información
							C15	Implementar pruebas de penetración sobre el software previa salida de producción para detectar posibles vulnerabilidades de seguridad.	Líder de desarrollo y Líder TI especialista en seguridad de la información
	R6 - Perdida de confidencialidad de la información contenida en el aplicativo de gestión documental por la ausencia de lineamientos de seguridad en el software que soliciten el cambio de contraseña a nuevos usuarios que han sido aprovisionados por el administrador del aplicativo.	Medio	C			Reducir el riesgo	C12	Implementar la metodología de desarrollo de software seguro en el aplicativo de gestión documental.	Líder de desarrollo
							C15	Implementar pruebas de penetración sobre el software previa salida de producción para detectar posibles vulnerabilidades de seguridad.	Líder de desarrollo y Líder TI especialista en seguridad de la información
							C16	Capacitar al personal del área de desarrollo en temas relacionados a la seguridad de la información y software seguro.	CEO de la organización (Asignación del recurso), Líder de desarrollo y Líder TI especialista en seguridad de la información
	R7 - Sustracción y/o perdida de información contenida en el aplicativo de gestión documental causada por la ausencia de lineamientos de seguridad en el software que definan una frecuencia de renovación y un nivel de	Medio			D	Reducir el riesgo	C12	Implementar la metodología de desarrollo de software seguro en el aplicativo de gestión documental.	Líder de desarrollo
							C15	Implementar pruebas de penetración sobre el software previa salida de producción para detectar posibles vulnerabilidades de seguridad.	Líder de desarrollo y Líder TI especialista en seguridad de la información

CONTENEDOR Y/O ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANALISIS DE RIESGOS	CARACTERIZACIÓN DEL RIESGO		QUE AFECTA			PLAN DE TRATAMIENTO DE RIESGOS			
	RIESGOS DE SEGURIDAD	NIVEL DEL RIESGO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBLIDAD	ESTRATEGIA DE TRATAMIENTO DEL RIESGO	IDENTIFICACIÓN DEL CONTROL	DESCRIPCION DEL PLAN DE ACCIÓN (CONTROLES)	RESPONSABLE
	complejidad en el establecimiento de los password por parte de los usuarios del aplicativo.						C16	Capacitar al personal del área de desarrollo en temas relacionados a la seguridad de la información y software seguro.	CEO de la organización (Asignación del recurso), Líder de desarrollo y Líder TI especialista en seguridad de la información
	R8 - Incumplimiento de acuerdos de servicio con clientes debido a la indisponibilidad del aplicativo de gestión documental a causa de la explotación de las debilidades existentes por un tercero sobre el software de gestión documental.	Medio			D	Reducir el riesgo	C12	Implementar la metodología de desarrollo de software seguro en el aplicativo de gestión documental.	Líder de desarrollo
							C15	Implementar pruebas de penetración sobre el software previa salida de producción para detectar posibles vulnerabilidades de seguridad.	Líder de desarrollo y Líder TI especialista en seguridad de la información
							C16	Capacitar al personal del área de desarrollo en temas relacionados a la seguridad de la información y software seguro.	CEO de la organización (Asignación del recurso), Líder de desarrollo y Líder TI especialista en seguridad de la información
	R9 - Divulgación y/o pérdida de información no autorizada por terceros a causa de asignación excesiva de permisos sobre un rol.	Alto	C		D	Reducir el riesgo	C12	Implementar la metodología de desarrollo de software seguro en el aplicativo de gestión documental.	Líder de desarrollo
							C17	Realizar el aprovisionamiento de usuarios en la aplicación de gestión documental con un enfoque de privilegios mínimos.	Líder de desarrollo

CONTENEDOR Y/O ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANALISIS DE RIESGOS	CARACTERIZACIÓN DEL RIESGO		QUE AFECTA			PLAN DE TRATAMIENTO DE RIESGOS			
	RIESGOS DE SEGURIDAD	NIVEL DEL RIESGO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBLIDAD	ESTRATEGIA DE TRATAMIENTO DEL RIESGO	IDENTIFICACIÓN DEL CONTROL	DESCRIPCION DEL PLAN DE ACCIÓN (CONTROLES)	RESPONSABLE
Servidores	R10 - Perdida de información de la organización debido a la ausencia de procedimientos que establezcan los lineamientos y buenas prácticas de seguridad para realizar backup de la información.	Alto			D	Reducir el riesgo	C18	Diseñar y/o actualizar la política de seguridad de la información de la organización.	Líder TI especialista en seguridad de la información
							C19	Definir un plan de tratamiento de incidentes de seguridad de la información.	Líder TI especialista en seguridad de la información
							C20	Establecer el procedimiento para el backup de la información, el cual debe estar en un contenedor de información diferente al cual le están realizando el backup.	Líder TI especialista en seguridad de la información
	R11 - Afectación de la confidencialidad e integridad de la información a causa de una inadecuada gestión de identidades y control de acceso a los recursos y repositorios de información de la organización.	Alto	C	I		Reducir el riesgo	C21	Implementar la gestión de identidades a través de un modelo basado en roles que permita proveer los procesos de autenticación de las identidades, autorización de privilegios y permisos sobre los servicios e infraestructura de la organización.	Líder de Recursos Humanos y Líder TI especialista en seguridad de la información
							C9	Actualizar y depurar los directorios existentes, identificando las cuentas de usuario que no cumplan con las políticas de seguridad, así como las cuentas huérfanas, en desuso y cuentas que carezcan de atributos que pueden ser relevantes para la gestión de identidades dentro de la organización.	Líder TI especialista en seguridad de la información
	R12 - Perdida de información y afectación de los servicios por desactualización de sistemas operativos y antivirus en los servidores.	Alto	C		D	Reducir el riesgo	C22	Emplear software (Sistemas Operativos, Antivirus, etc.) licenciado y actualizado en los servidores de la organización.	Líder TI especialista en seguridad de la información

CONTENEDOR Y/O ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANALISIS DE RIESGOS	CARACTERIZACIÓN DEL RIESGO		QUE AFECTA			PLAN DE TRATAMIENTO DE RIESGOS			
	RIESGOS DE SEGURIDAD	NIVEL DEL RIESGO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBLIDAD	ESTRATEGIA DE TRATAMIENTO DEL RIESGO	IDENTIFICACIÓN DEL CONTROL	DESCRIPCION DEL PLAN DE ACCIÓN (CONTROLES)	RESPONSABLE
							C23	Realizar revisiones periódicas en los equipos de cómputo para prevenir desactualizaciones en el software instalado (Sistema operativo, Antivirus y aplicaciones).	Líder TI especialista en seguridad de la información
	R13 - Indisponibilidad de la información alojada en los servidores por deterioro físico causado por la ausencia de planes de mantenimiento preventivo sobre el hardware.	Medio			D	Reducir el riesgo	C24	Diseñar un plan de mantenimiento de hardware y software que permita prolongar el funcionamiento de la infraestructura de red (Dispositivos activos, servidores, equipos de cómputo, cableado), brindando una continuidad de los servicios a través de la red.	Líder TI especialista en seguridad de la información
							C25	Programar y documentar las actividades de mantenimiento realizadas en los equipos de cómputo (Servidores, computadores de escritorio, portátiles) para establecer su respectiva trazabilidad y garantía según aplique.	Líder TI especialista en seguridad de la información
	R14 - Tiempos laborales muertos causados por la indisponibilidad de la información y servicios debido a la ausencia de configuraciones de seguridad en los servidores.	Muy bajo			D	Aceptar el riesgo	C26	No se aplican controles ya que la organización ha decidido aceptar el riesgo	No aplica
Cuarto de infraestructura tecnológica (Cuarto de Equipos)	R15 - Daño o hurto de infraestructura tecnológica afectando la operatividad de la organización por	Medio			D	Reducir el riesgo	C6	Implementar controles de acceso físico y lógico que restrinjan los accesos no autorizados a los repositorios de información.	Líder TI especialista en seguridad de la información

CONTENEDOR Y/O ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANALISIS DE RIESGOS	CARACTERIZACIÓN DEL RIESGO		QUE AFECTA			PLAN DE TRATAMIENTO DE RIESGOS			
	RIESGOS DE SEGURIDAD	NIVEL DEL RIESGO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBLIDAD	ESTRATEGIA DE TRATAMIENTO DEL RIESGO	IDENTIFICACIÓN DEL CONTROL	DESCRIPCION DEL PLAN DE ACCIÓN (CONTROLES)	RESPONSABLE
	inadecuados controles de acceso físico al centro de cómputo.						C27	Realizar monitoreo periódico que permita corroborar la efectividad de los controles físicos implementados, aplicando las acciones correctivas necesarias para salvaguardar los activos asociados a la información de la organización.	Líder TI especialista en seguridad de la información
							C28	Revisar periódicamente la bitácora de control de acceso del personal a las instalaciones de la organización y centro de datos.	Líder TI especialista en seguridad de la información
	R16 - Indisponibilidad de la información causado por el deterioro del equipamiento informático debido a la ausencia de sistemas de control de condiciones ambientales como temperatura y humedad.	Medio			D	Reducir el riesgo	C29	Implementar un sistema de aire acondicionado de precisión que le permita controlar variables como temperatura y humedad en el centro de cómputo.	CEO de la organización (Asignación del recurso) y Líder TI especialista en seguridad de la información
							C30	Realizar una adecuada distribución de los rack de comunicaciones y servidores en el centro de cómputo que permita crear corredores de aire frio y aire caliente mejorando la eficiencia del sistema de refrigeración empleado.	Líder TI especialista en seguridad de la información
	R17 - Tiempos de inactividad en las operaciones de la organización, debido al daño o ausencia de sistemas de respaldo eléctrico a la infraestructura de red de la organización.	Medio			D	Reducir el riesgo	C31	Programar actividades de mantenimiento preventivo sobre la UPS para prolongar su funcionamiento.	Líder TI especialista en seguridad de la información
							C32	Implementar el monitoreo de la UPS online a través del software del fabricante de la UPS.	Líder TI especialista en seguridad de la información

CONTENEDOR Y/O ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANALISIS DE RIESGOS	CARACTERIZACIÓN DEL RIESGO		QUE AFECTA			PLAN DE TRATAMIENTO DE RIESGOS			
	RIESGOS DE SEGURIDAD	NIVEL DEL RIESGO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBLIDAD	ESTRATEGIA DE TRATAMIENTO DEL RIESGO	IDENTIFICACIÓN DEL CONTROL	DESCRIPCION DEL PLAN DE ACCIÓN (CONTROLES)	RESPONSABLE
	R18 - Deterioro parcial y/o total de la infraestructura tecnológica del centro de cómputo causada por la presencia de fuego en el recinto.	Alto			D	Reducir el riesgo	C33	Instalar sistemas de detección y extinción de incendios en el centro de cómputo.	CEO de la organización (Asignación del recurso) y Líder TI especialista en seguridad de la información
							C34	Realizar periódicamente actividades de mantenimiento sobre los sistemas de detección y extinción para garantizar su efectividad ante cualquier incidente.	CEO de la organización (Asignación del recurso) y Líder TI especialista en seguridad de la información
Red LAN corporativa	R19 - Sustracción y/o pérdida de información sensible de la organización debido a la ausencia de políticas y controles en el establecimiento de contraseñas de acceso a los dispositivos tecnológicos de la entidad.	Alto	C		D	Reducir el riesgo	C18	Diseñar y/o actualizar la política de seguridad de la información de la organización.	Líder TI especialista en seguridad de la información
							C6	Implementar controles de acceso físico y lógico que restrinjan los accesos no autorizados a los repositorios de información.	Líder TI especialista en seguridad de la información
							C35	Implementar configuraciones de seguridad orientadas a salvaguardar la información e infraestructura de red de la organización (Router, Switch, Servidores, redes inalámbricas).	Líder TI especialista en seguridad de la información
	R20 - Indisponibilidad de la información y/o servicios que se acceden a través de la red corporativa por deficiencias en su diseño e	Medio			D	Reducir el riesgo	C35	Implementar configuraciones de seguridad orientadas a salvaguardar la información e infraestructura de red de la organización (Router, Switch, Servidores, redes inalámbricas).	Líder TI especialista en seguridad de la información

CONTENEDOR Y/O ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANALISIS DE RIESGOS	CARACTERIZACIÓN DEL RIESGO		QUE AFECTA			PLAN DE TRATAMIENTO DE RIESGOS			
	RIESGOS DE SEGURIDAD	NIVEL DEL RIESGO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBLIDAD	ESTRATEGIA DE TRATAMIENTO DEL RIESGO	IDENTIFICACIÓN DEL CONTROL	DESCRIPCION DEL PLAN DE ACCIÓN (CONTROLES)	RESPONSABLE
	implementación.						C36	Efectuar periódicamente pruebas de hacking ético para detectar posibles vulnerabilidades en la seguridad de la infraestructura de red corporativa, incluido los servicios publicados en internet.	Líder TI especialista en seguridad de la información
							C37	Adquirir infraestructura de red (Firewall de nueva generación NGFW) que permita implementar lineamientos y políticas de seguridad para acceder a los recursos y servicios de la organización.	CEO de la organización (Asignación del recurso) y Líder TI especialista en seguridad de la información
							C38	Realizar monitoreo y seguimiento al registro de logs para evidenciar posibles intrusiones no autorizadas.	Líder TI especialista en seguridad de la información
Antivirus	R21 - Pérdida parcial y/o total de información provocado por la desactualización y/o ausencia de antivirus.	Alto	C		D	Reducir el riesgo	C22	Emplear software (Sistemas Operativos, Antivirus, etc.) licenciado y actualizado en los servidores de la organización.	Líder TI especialista en seguridad de la información
							C23	Realizar revisiones periódicas en los equipos de cómputo para prevenir desactualizaciones en el software instalado (Sistema operativo, Antivirus y aplicaciones).	Líder TI especialista en seguridad de la información
	R22 - Daño de hardware provocado por código malicioso debido a la desactualización de los	Medio			D	Reducir el riesgo	C22	Emplear software (Sistemas Operativos, Antivirus, etc.) licenciado y actualizado en los servidores de la organización.	Líder TI especialista en seguridad de la información

CONTENEDOR Y/O ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANALISIS DE RIESGOS	CARACTERIZACIÓN DEL RIESGO		QUE AFECTA			PLAN DE TRATAMIENTO DE RIESGOS			
	RIESGOS DE SEGURIDAD	NIVEL DEL RIESGO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBLIDAD	ESTRATEGIA DE TRATAMIENTO DEL RIESGO	IDENTIFICACIÓN DEL CONTROL	DESCRIPCION DEL PLAN DE ACCIÓN (CONTROLES)	RESPONSABLE
	antivirus.						C23	Realizar revisiones periódicas en los equipos de cómputo para prevenir desactualizaciones en el software instalado (Sistema operativo, Antivirus y aplicaciones).	Líder TI especialista en seguridad de la información
	R23 - Afectación de la operatividad de la red corporativa debido a la presencia de malware.	Medio	C		D	Reducir el riesgo	C22	Emplear software (Sistemas Operativos, Antivirus, etc.) licenciado y actualizado en los servidores de la organización.	Líder TI especialista en seguridad de la información
							C23	Realizar revisiones periódicas en los equipos de cómputo para prevenir desactualizaciones en el software instalado (Sistema operativo, Antivirus y aplicaciones).	Líder TI especialista en seguridad de la información
Unidades de almacenamiento de información	R24 - Pérdida de clientes por divulgación no autorizada de información debido a la ausencia de mecanismos de cifrado de información sobre unidades de almacenamiento electrónico.	Alto	C			Reducir el riesgo	C5	Clasificar la información de la organización, definiendo si es pública, privada o confidencial.	Responsable del proceso y líder TI especialista en seguridad de la información
							C39	Implementar mecanismos de cifrado de información en unidades de almacenamiento (Discos duros, USB, portátiles y dispositivos móviles).	Líder TI especialista en seguridad de la información
Talento humano	R25 - Sustracción y/o pérdida de la información sensible de la organización debido a la ausencia de acuerdos de confidencialidad y protección de la propiedad intelectual entre la empresa y sus empleados directos,	Alto	C		D	Reducir el riesgo	C18	Diseñar y/o actualizar la política de seguridad de la información de la organización.	Líder TI especialista en seguridad de la información
							C40	Establecer programas de capacitación y sensibilización al personal de la organización en temas relacionados con la seguridad de la información.	Líder TI especialista en seguridad de la información

CONTENEDOR Y/O ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANALISIS DE RIESGOS	CARACTERIZACIÓN DEL RIESGO		QUE AFECTA			PLAN DE TRATAMIENTO DE RIESGOS			
	RIESGOS DE SEGURIDAD	NIVEL DEL RIESGO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBLIDAD	ESTRATEGIA DE TRATAMIENTO DEL RIESGO	IDENTIFICACIÓN DEL CONTROL	DESCRIPCION DEL PLAN DE ACCIÓN (CONTROLES)	RESPONSABLE
	aprendices, practicantes y aliados estratégicos.						C41	Establecer acuerdos de confidencialidad con los empleados, proveedores y terceros para el manejo de la información institucional.	Líder de Recursos Humanos y Líder TI especialista en seguridad de la información

Tabla 21 - Plan de tratamiento de riesgos propuesto para mitigar y controlar los riesgos existentes.

Los controles de seguridad propuestos para reducir los riesgos detectados en los activos asociados a la información del aplicativo de gestión documental se clasifican en preventivos, detectivos y correctivos. A continuación se brinda una descripción de la clasificación descrita.

TIPO DE CONTROL	DESCRIPCIÓN DEL CONTROL
Preventivos	Están enfocados a evitar que se produzcan incidentes o riesgos de seguridad. Dentro de los controles preventivos se pueden encontrar el establecimiento de políticas de seguridad, metodologías de software seguro, definición de procesos que permitan implementar buenas prácticas de seguridad de la información, así como los planes de concientización y sensibilización del personal, la implementación de Firewalls, entre otros.
Detectivos	Se encargan de detectar los incidentes de seguridad en el momento que están ocurriendo, sin establecer acciones correctivas. Se clasifican dentro de los controles detectivos los sistemas de monitoreo, antivirus, alarmas, sistemas de detección de intrusos, etc.
Correctivos	Controles enfocados a corregir los incidentes y riesgos de seguridad ocurridos.

Tabla 22 – Descripción de la clasificación de los controles sugeridos

Teniendo en cuenta el alcance del presente proyecto, se deja a consideración de la organización la implementación, seguimiento y control del plan de tratamiento de riesgos descrito enfocado a reducir, mitigar y controlar los riesgos existentes a los que se encuentran expuestos actualmente los activos de información que engloba el software de gestión documental de la cual es propietaria.

4.3.4 POLITICA DE SEGURIDAD DE LA INFORMACIÓN

La organización propietaria del software de gestión documental, objeto del presente trabajo de grado no cuenta actualmente con una política de seguridad de la información que le brinde al personal de la entidad los lineamientos y recomendaciones que debe aplicar para salvaguardar la integridad, confidencialidad y disponibilidad de la información que manipula a diario para cumplir con el desarrollo de su objeto de contrato; motivo por el cual uno de los objetivos propuestos en el anteproyecto es la creación de la política de seguridad de la información para la entidad, estando proyectada a lograr el cumplimiento de la misión y visión institucional así como de contribuir al fortalecimiento de la seguridad de la información que le permita a la entidad continuar manteniendo su buen nombre y la confianza de sus clientes en los procesos de gestión documental, custodia de documentos y demás líneas de negocio que ofrece actualmente.

En el anexo 8 se encuentra la política de seguridad de la información diseñada y estructurada acorde a la importancia que reconoce la alta dirección de la entidad de definir lineamientos que deben ser aplicados por sus empleados directos, trabajadores ocasionales, contratistas, practicantes y terceros para proteger y asegurar la confidencialidad, integridad, disponibilidad y autenticidad de la información en sus diferentes medios de almacenamiento, procesamiento y transporte de información.

Como guía para la elaboración de la política de seguridad de la entidad se aplicaron las recomendaciones que brinda el documento de: “Políticas de Seguridad de la Información” de la Institución Universitaria Politécnico GranColombiano, correspondiente al módulo de Teoría de seguridad de la especialización en seguridad de la información a la cual me encuentro inscrita actualmente (Institución Universitaria Politecnico GranColombiano, 2016).

5. RESULTADOS Y DISCUSIÓN

Los resultados obtenidos en el presente documento se generaron gracias a la aplicación del plan de trabajo propuesto para el desarrollo del proyecto en el cual se identifican las fases descritas a continuación que permitieron dar cumplimiento a los objetivos del proyecto.

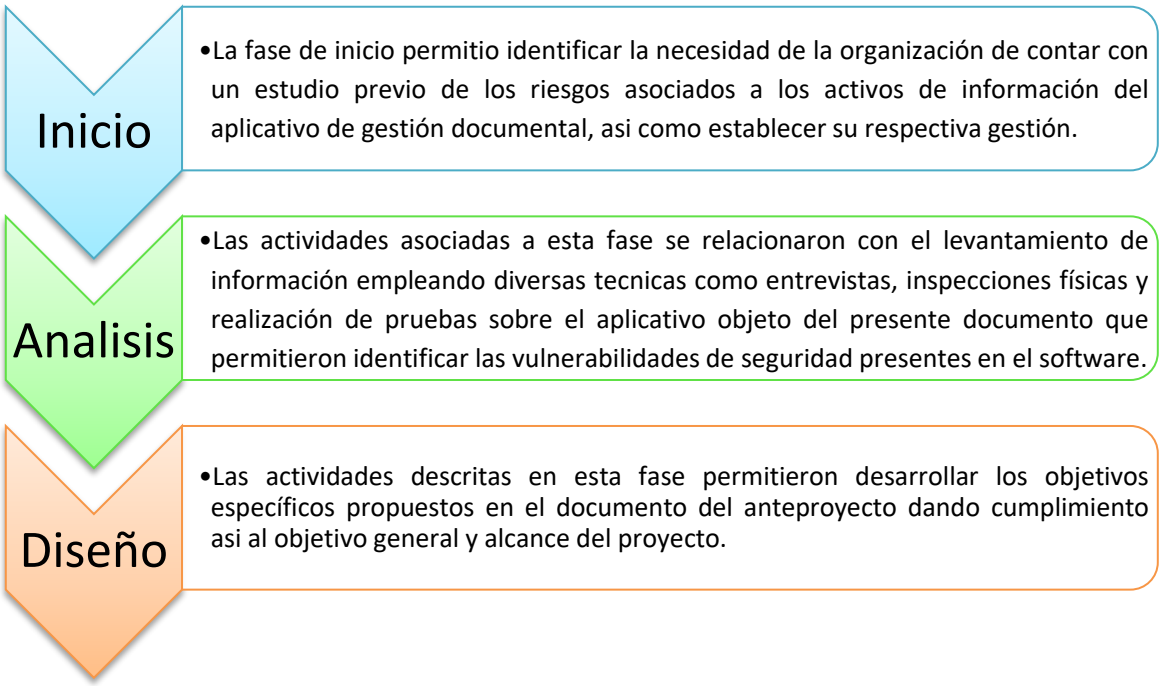

Figura 2 – Fases del plan de trabajo propuesto

La información recopilada en la fase de análisis permitió dar inicio al desarrollo de los objetivos específicos para dar cumplimiento con los entregables descritos en el anteproyecto aprobado por la Universidad. Acorde a esto se describe a continuación los resultados obtenidos al culminar el presente proyecto.

5.1 ENTREGABLE 1 – Inventario de activos asociados al sistema de gestión documental

Los resultados específicos relacionados con este entregable son:

OE1. Definir la metodología a emplear para identificar, valorar, clasificar y tratar los activos de información que apoyan la gestión del aplicativo de gestión documental.

OE2. Realizar un inventario de los activos de información que engloba el aplicativo de gestión documental resultado de aplicar la metodología de identificación, clasificación y valoración de los activos de información del software de gestión documental.

OE1 - Definir la metodología a emplear para identificar, valorar, clasificar y tratar los activos de información que apoyan la gestión del aplicativo de gestión documental.

La metodología empleada para identificar, valorar y clasificar los activos de información asociados al aplicativo de gestión documental se estableció en base a la metodología de análisis y gestión de riesgos de los sistemas de información MAGERIT, la cual propone el modelo de clasificación descrito en la tabla 3 – Clasificación de los activos establecida en la metodología MAGERIT del presente documento.

Una vez definida e identificadas las características relevantes del modelo de clasificación de los activos asociados a la información se dio inicio al levantamiento de información que permitió llevar a cabo el desarrollo del segundo objetivo específico asociado al entregable N.1.

OE2 - Realizar un inventario de los activos de información que engloba el aplicativo de gestión documental resultado de aplicar la metodología de identificación, clasificación y valoración de los activos de información del software de gestión documental.

El inventario de activos de información se realizó de acuerdo al alcance del proyecto a través de las entrevistas realizadas a los líderes encargados en la organización de las áreas de desarrollo, tecnología y consultoría quienes a través de sus orientaciones permitieron identificar los activos asociados al aplicativo de gestión documental objeto del presente trabajo de grado.

La identificación de los activos asociados a la información del software de gestión documental, permito establecer en conjunto con el CEO de la organización la valoración de los activos en términos de confidencialidad, integridad y disponibilidad teniendo presente la importancia del activo para la continuidad del negocio, así como el impacto

que podía causar para la organización a nivel financiero, jurídico y de imagen corporativa la perdida de alguna de las características de la seguridad de la información relacionada con el aplicativo de gestión documental debido a la materialización de una amenaza, procedimiento que se puede evidenciar en el ítem 4.3.1 del presente documento, así como en el anexo 5 que contiene el inventario de los activos asociados a la información.

Gracias a la identificación y valoración que se realizó sobre los activos de información se identificó la criticidad del activo, generando un agrupamiento de los activos de acuerdo a su relación funcional para realizar sobre dichos activos el respectivo análisis de riesgos. Como resultado de lo descrito los activos seleccionados para realizar el respectivo análisis de riesgo fueron:

IDENTIFICACIÓN DEL ACTIVO DE INFORMACIÓN			
N. ACTIVO	NOMBRE DEL ACTIVO	CRITICIDAD DEL ACTIVO	CONTENEDOR Y/O ACTIVO DE INFORMACIÓN SELECCIONADO PARA EL ANALISIS DE RIESGOS
GD - A1	Software de control de versiones (Subversión y GIT)	Alto	Código fuente
GD - A3	Código fuente	Alto	
GD - A15	Interfaz de desarrollo (Netbeans con lenguaje de programación Java)	Alto	
GD - A18	Aplicativo de gestión documental	Alto	Aplicación de gestión documental
GD - A4	Servidor de aplicaciones	Alto	Servidores
GD - A5	Servidor de bases de datos	Alto	
GD - A19	Sistemas de gestión de bases de datos	Alto	
GD - A6	Servidor de imágenes	Alto	
GD - A14	Servicio de File Systems	Alto	
GD - A9	Dispositivos de red	Alto	Cuarto de infraestructura tecnológica (Cuarto de Equipos)
GD - A10	Cuarto de equipos	Alto	
GD - A12	Red de área local - LAN	Alto	Red LAN corporativa
GD - A13	Red Inalámbrica - WLAN	Alto	
GD - A17	Antivirus	Alto	Antivirus
GD - A20	Medios de almacenamiento electrónico (USB, Discos duros externos)	Medio	Unidades de almacenamiento de información
GD - A11	Desarrolladores	Medio	Talento humano

Tabla 23 - Activos objeto de análisis de riesgos

5.2 ENTREGABLE 2 – Análisis de riesgos detectados sobre el aplicativo de gestión documental

Los objetivos específicos que permitieron alcanzar este resultado de aprendizaje son:

> **OE3.** Especificar la metodología para la identificación y valoración de los riesgos de seguridad que se encuentran presentes en el aplicativo de gestión documental.
>
> **OE4**. Identificar y valorar los riesgos de seguridad sobre los activos de información del aplicativo de gestión documental al interior de la empresa propietaria del software.

A continuación se describen las actividades que permitieron desarrollar los objetivos específicos descritos.

OE3 - Especificar la metodología para la identificación y valoración de los riesgos de seguridad que se encuentran presentes en el aplicativo de gestión documental.

Estableciendo como referencia la metodología de análisis y gestión de riesgos de los sistemas de información MAGERIT y los objetivos organizacionales de la empresa propietaria del software, se definieron las siguientes actividades para realizar el respectivo análisis de riesgos sobre el aplicativo de gestión documental.

- ✓ Identificación de vulnerabilidades y amenazas sobre los activos asociados a la información así como su respectivo impacto.
- ✓ Definición de los riesgos de seguridad.
- ✓ Establecer la cuantificación de la probabilidad de ocurrencia del riesgo y el impacto que puede generar para la organización la materialización del riesgo.
- ✓ Construir la matriz de riesgos inherente.
- ✓ Diseñar el plan de tratamiento y gestión de riesgos de seguridad de la información

El desarrollo de cada una de las actividades descritas se encuentra en el numeral 4.3.2 del presente documento, lo que permitió desarrollar el siguiente objetivo.

OE4 - Identificar y valorar los riesgos de seguridad sobre los activos de información del aplicativo de gestión documental al interior de la empresa propietaria del software.

Posterior a la identificación de los riesgos de seguridad establecidos a partir de la identificación de las vulnerabilidades y amenazas a las cuales se encuentran expuestos los activos asociados a la información objeto del presente análisis, se definieron los riesgos de seguridad presentes sobre los activos, siendo estos valorados en términos de probabilidad de ocurrencia del riesgo y el nivel de impacto que podría generar para la organización la materialización del riesgo.

Los aspectos definidos en la valoración en términos de probabilidad se realizaron acorde a lo establecido en conjunto con el CEO de la organización, esto debido a que la organización no ha presentado eventos y/o situaciones que hayan comprometido la seguridad de la información que manejan actualmente y tampoco tienen un registro de ello. Con respecto a la valoración del impacto se realizó teniendo en cuenta la afectación a nivel económico y operativo que puede generar al interior de la organización la materialización de un riesgo de seguridad. Las variables descritas contaron con la aprobación del CEO de la entidad.

El anexo 6 contiene la matriz de riesgos de seguridad asociados al aplicativo de gestión documental, así como se encuentra descrito paso a paso el procedimiento realizado en el numeral 4.3.2 en el que se explica el desarrollo de la metodología propuesta para la identificación y valoración de los riesgos de seguridad a los que está expuesta la aplicación de gestión documental actualmente debido a la ausencia de controles que establezcan su control y mitigación.

5.3 ENTREGABLE 3 – Plan de tratamiento y gestión de riesgos de seguridad de la información

Los objetivos específicos ya descritos permitieron desarrollar el objetivo general del proyecto de grado el cual es:

> **OG.** Realizar el análisis de riesgos de seguridad de la información sobre la aplicación de gestión documental, proponiendo un plan de tratamiento orientado a mitigar y controlar los riesgos de seguridad detectados en el aplicativo de software objeto del presente estudio.

Acorde al análisis de riesgos de seguridad identificados para el aplicativo de gestión documental se estableció la estrategia de tratamiento del riesgo, la cual permitió evaluar en conjunto con la organización el costo beneficio que tendría para la entidad el evitar, reducir, transferir o aceptar los riesgos identificados sobre el software. Como resultado del análisis costo beneficio se estableció “Reducir el Riesgo” en los riesgos de nivel medio y alto, así como “Aceptar el riesgo” en los riesgos de nivel “muy bajo”.

En el ítem 4.3.3 de la metodología se desarrolló paso a paso el plan de tratamiento y gestión de riesgos, como estrategia para mitigar y controlar los riesgos de seguridad identificados sobre la aplicación de gestión documental, así como se evidencia el resultado obtenido en el anexo 7 al presente documento.

Los controles de seguridad propuestos para reducir los riesgos detectados en los activos asociados a la información del aplicativo de gestión documental se clasificaron en preventivos, detectivos y correctivos, los cuales teniendo en cuenta el alcance del presente proyecto, se deja a consideración de la organización la implementación, seguimiento y control del plan de tratamiento de riesgos descrito enfocado a reducir, mitigar y controlar los riesgos existentes a los que se encuentran expuestos actualmente los activos de información que engloba el software de gestión documental de la cual es propietaria.

5.4 ENTREGABLE 4 – Política de seguridad de la información para la organización

El entregable N.4 desarrollo el siguiente objetivo específico.

> **OE5.** Definir la política de seguridad de la información de la organización propietaria del software de gestión documental.

El respectivo entregable correspondiente al objetivo descrito se encuentra en el Anexo N. 8, en donde se estableció los lineamientos que deben aplicar todos los empleados directos, trabajadores ocasionales, contratistas, practicantes y terceros para proteger y asegurar la confidencialidad, integridad, disponibilidad y autenticidad de la información de la organización a fin de propender la continuidad del negocio y mantener la imagen corporativa de la entidad.

Como guía para la elaboración de la política de seguridad de la entidad se aplicaron las recomendaciones que brinda el documento de: “Políticas de Seguridad de la Información” de la institución universitaria Politécnico GranColombiano, correspondiente al módulo de Teoría de seguridad de la especialización en seguridad de la información. (Institución Universitaria Politecnico GranColombiano, 2016).

Se recomienda a la organización la revisión de la política de seguridad propuesta a fin de realizar los ajustes a que haya lugar acorde a las necesidades en la gestión de la seguridad de la información de la entidad, así como su respectiva aprobación y aplicación sensibilizando al personal de la importancia del conocimiento y aplicación de la política de seguridad de la información en la organización.

6. CONCLUSIONES

- El análisis de riesgos de seguridad de la información sobre el aplicativo de gestión documental permitió evidenciar las debilidades relacionadas con el diseño y funcionamiento del software, así como las deficiencias existentes en la infraestructura tecnológica que almacena, procesa y transporta la información tanto del software como la contenida dentro del mismo haciendo evidente la necesidad de implementar un plan de tratamiento de riesgos que permita disminuir los riesgos a los cuales está expuesta la información de la organización.

- Los riesgos de seguridad detectados sobre el aplicativo de gestión documental son de criticidad “Alta”, motivo por el cual se sugiere a la organización la implementación del plan de tratamiento de riesgos diseñado como resultado de este documento, el cual está enfocado a reducir y controlar los riesgos de seguridad existentes que ponen en riesgo la seguridad de la información y por ende la continuidad del negocio.

- Se invita al CEO y directivas de la organización a comprometerse con la seguridad de la información en los procesos y líneas de negocio que engloba a entidad, estableciendo los recursos necesarios que permitan la implementación de las actividades enfocadas a salvaguardar la información de la organización a través de la gestión de la seguridad dentro de la entidad.

- Se exhorta a la organización propietaria del software de gestión documental, objeto del presente estudio la creación de área de TI dentro de la organización, la cual debe estar liderada por un profesional de TI Especialista en Seguridad de la Información, quien tendrá como función principal planificar, diseñar e implementar las acciones pertinentes que le permitan establecer en la organización una adecuada gestión de la seguridad de la información que le brinde a la organización una continuidad del negocio a través del desarrollo de sus líneas de negocio y cumplimiento de los objetivos .

- Se motiva a las directivas de la organización propietaria del software de gestión documental a documentar los procesos de sus actividades y líneas de negocio,

información que es valiosa en el establecimiento de la gestión de la seguridad de la información en la organización.

- Se invita a la organización a diseñar y establecer de manera prioritaria los acuerdos de confidencialidad de la información de la organización y sus clientes, con sus colaboradores internos y/o externos que por desarrollo de su objeto de contrato tengan acceso a la información que almacena, procesa, gestiona o transporta en las diversas líneas de negocio de la entidad.

- Se sugiere realizar la implementación de la política de seguridad de la información diseñada con el objetivo de establecer los lineamientos y procedimientos que deben cumplir todas las personas internas y/o externas de la organización que por estrategias de negocio puedan tener acceso a la información de la organización, las cuales deben propender por proteger y asegurar la confidencialidad, integridad, disponibilidad y autenticad de la información de la entidad.

- Realizar una actualización y depuración de los directorios existentes, que permita identificar las cuentas de usuario que no cumplan con las políticas de seguridad, así como las cuentas huérfanas, en desuso y cuentas que carezcan de atributos que pueden ser relevantes para la gestión de identidades dentro de la organización.

7. BIBLIOGRAFÍA

Archivo General de la Nación Colombia. (2014). *http://observatoriotic.archivogeneral.gov.co.* Recuperado el 2 de Abril de 2017

Gobierno de España. (Octubre de 2012). MAGERIT - Versión 3.0 Metodologia de análisis de riesgos de los sistemas de información. . *Libro II - Catalogo de elementos*. Madrid. Recuperado el 16 de Mayo de 2017

Gobierno de España. (Octubre de 2012). MAGERIT - Versión 3.0. Metodología de análisis y gestión de riesgos de los sistemas de información. *Libro I - Método*. (M. d. Públicas, Ed.) Recuperado el 15 de Mayo de 2017, de http://administracionelectronica.gob.es/

Institución Universitaria Politécnico GranColombiano. (2016). Analisis de Riesgo. *Introducción teórica al analisis de riesgos: Conceptos*. Bogota. Recuperado el 15 de Mayo de 2017

Institución Universitaria Politécnico GranColombiano. (2016). Gestión de identidad. *Gestión de identidad y funcionalidad*. Bogota. Recuperado el 15 de Mayo de 2017

Institución Universitaria Politécnico GranColombiano. (2016). Gestión de seguridad. . *Principios de la seguridad de la información*. Bogota. Recuperado el 15 de mayo de 2017

Institución Universitaria Politecnico GranColombiano. (2016). Teoria de la seguridad. *Politicas de seguridad de la información*. Bogota. Recuperado el 30 de mayo de 2017

Institución Universitaria Politécnico GranColombiano. (2016). *Teoria de la Seguridad. Principios de la seguridad de la información.* Bogota.

Institución Universitaria Politécnico GranColombiano. (2017). Seguridad Fisica. *Medidas de Prevención*. Bogota.

Instituto Colombiano de Normas Técnicas ICONTEC. (11 de Diciembre de 2013). Norma Tecnica Colombiana NTC-ISO-IEC 27001. Recuperado el 15 de Mayo de 2017

International Standar ISO/IEC 27000. (15 de Febrero de 2016). Information technology, Security Techniques. Recuperado el 15 de Mayo de 2017

Ministerio de Cultura. (14 de Diciembre de 2012). *http://www.mintic.gov.co.* Recuperado el 5 de Abril de 2017

MinTIC. (08 de Abril de 2014). *http://www.mintic.gov.co.* Recuperado el 20 de Abril de 2017

Quintero, B. P., & Fuentes, P. A. (2007). Diseño de un sistema de gestión documental para el programa de ingeniería de sistemas de la universidad San Buenaventura - Sede Bogota. Bogota DC. Recuperado el 17 de Abril de 2017

8. ANEXOS

A continuación se relacionan los anexos del presente documento.

Anexo N. 1 – Cronograma del plan de trabajo realizado en MS – Project.

Anexo N. 2 – Entrevista líder de desarrollo.

Anexo N. 3 – Entrevista líder de soporte IT.

Anexo N. 4 – Infraestructura relacionada con la seguridad física.

Anexo N. 5 – Entregable N.1 - Inventario de Activos asociados a la Información.

Anexo N. 6 – Entregable N.2 - Análisis de Riesgos de SI.

Anexo N. 7 – Entregable N.3 - Plan de Tratamiento de Riesgos de SI.

Anexo N. 8 – Entregable N.4 – Política de seguridad de la información.