DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA EMPRESA HECC CURRIER BASADO EN ISO 27001

ANGEL NOEL DURAN FLOREZ
Cód. 20152678109
IVAN CAMILO LUMBAQUE FIGUEROA
Cód. 20152678023

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS
FACULTAD TECNOLÓGICA
INGENIERIA EN TELEMÁTICA
BOGOTÁ D.C.
2018

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA EMPRESA HECC CURRIER BASADO EN ISO 27001

ANGEL NOEL DURAN FLOREZ
Cód. 20152678109
IVAN CAMILO LUMBAQUE FIGUEROA
Cód. 20152678023

PROYECTO DE GRADO PARA OPTAR AL TITULO DE:
INGENIERO EN TELEMATICA

TUTOR
Ing. MIGUEL ANGEL LEGUIZAMON PAEZ

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS
FACULTAD TECNOLÓGICA
INGENIERIA EN TELEMÁTICA
BOGOTÁ D.C.
2018

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

Jurado

AGRADECIMIENTOS

El presente proyecto se ha realizado gracias al apoyo incondicional de nuestras familias, quienes siempre estuvieron brindándonos su fuerza, motivándonos para lograr los objetivos que teníamos, son fuente de comprensión entendiendo el sacrificio que nos llevó la dedicación de este trabajo como prioritario en nuestras vidas. Es también por ellos que logramos realizarlo de la mejor manera posible.

También es necesario agradecer a nuestros compañeros de carrera, de quienes aprendimos y nos colaboramos todo el tiempo para poder llegar a donde estamos, esos grupos de trabajo en clases y parciales nos llevaron hasta aquí y nuestro conocimiento creció en estos dos años en los cuales estuvimos juntos.

Queremos agradecer al Profesor Guillermo Hurtado, que desde el principio confió en nosotros, nos asesoró en lo que más pudo, dándonos las bases necesarias y el camino a seguir. A pesar de que por motivos personales no pudo continuar con nosotros siempre estaremos agradecidos y le deseamos muchos éxitos en todos sus proyectos.

Así mismo, le damos las gracias al Profesor Yesid Tibaquirá quien fue nuestro guía y asesor durante gran parte del proyecto sin ser nuestro tutor, quien dedicó horas de clase, compartió información útil y brindó su conocimiento para que pudiéramos avanzar en la realización de los objetivos.

Agradecemos a nuestro tutor actual, el Profesor Miguel Ángel Leguizamón quien confió en nosotros, nos asesoró en la parte final del proyecto y nos mostró el camino a donde debíamos llegar. Gracias a su aporte y motivación logramos organizar el proyecto, encaminarlo y terminarlo de la mejor forma posible.

Por último, agradecer a nuestra alma mater, la Universidad Distrital Francisco José de Caldas por hacernos crecer como personas, como intelectuales, y por brindarnos los elementos necesarios para que nuestro conocimiento creciera en cada asesoría, cada clase, cada práctica.

NOTA ACLARATORIA

Los autores del presente proyecto aclaran un error de digitación efectuado en el título del presente trabajo denominado “DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA EMPRESA HECC CURRIER BASADO EN ISO 27001” ya que la empresa para la cual se basa el proyecto se llama HECC COURRIER EXPRESS LTDA y no HECC CURRIER como se ha descrito en el título. Creemos que por normatividad de la Universidad no se debe efectuar el cambio en el título, pero si hacemos la salvedad en esta nota aclaratoria para evitar problemas de cualquier índole.

Durante el proyecto se nombrará a HECC COURRIER EXPRESS LTDA como HECC COURRIER para un mejor manejo de redacción y de no extendernos cada vez que se haga mención de ella.

TABLA DE CONTENIDO

RESUMEN 10
ABSTRACT 11
INTRODUCCIÓN 12
1. DEFINICIÓN Y ANÁLISIS 13
1.1 TEMA 13
1.2 TITULO 13
1.3 PLANTEAMIENTO DEL PROBLEMA 13
1.4 OBJETIVOS 14
1.4.1 OBJETIVO GENERAL 14
1.4.2 OBJETIVOS ESPECIFICOS 14
1.5 FORMULACIÓN DEL PROBLEMA 14
1.6 JUSTIFICACIÓN 14
1.7 ESTADO DEL ARTE 15
1.8 METODOLOGÍA 19
1.9 FACTIBILIDAD 21
1.10 CRONOGRAMA 23
1.11 RESULTADOS ESPERADOS 23
1.12 IMPACTO 24
2. SITUACIÓN ACTUAL 25
2.1 CARACTERIZACIÓN DE LA RED ACTUAL 26
2.2 ESTRUCTURA DE LA RED ACTUAL 27
2.3 REDES DE AREA LOCAL 27
2.4 SISTEMA ELÉCTRICO DE EMERGENCIA 27
2.5 APLICACIONES ACTUALES 27
2.6 ESTUDIO GAP DE ACUERDO AL ANEXO A 28

3. DIAGNÓSTICO DE AMENAZAS Y VULNERABILIDADES 32
3.1 IDENTIFICACIÓN DE ACTIVOS 32
3.2 IDENTIFICACIÓN Y VALORACIÓN DE VULNERABILIDADES 37
3.3 IDENTIFICACIÓN DE AMENAZAS 44
4. ANÁLISIS DE RIESGOS 49
4.1 TABLA DE VALORACIÓN DE RIESGOS 49
4.2 TABLA DE PROBABILIDAD 50
4.3 VALORACIÓN DE IMPACTO 51
4.4 IDENTIFICACIÓN DE RIESGOS 52
4.5 EVALUACIÓN DE RIESGOS 55
4.6 DOMINIOS, OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD 56
5. POLÍTICAS DE SEGURIDAD 95
6. GUÍA DE IMPLEMENTACIÓN 96
7. MÓDULO WEB 98
8. CONCLUSIONES 99
9. RECOMENDACIONES 100
10. BIBLIOGRAFÍA E INFOGRAFÍA 101
11. ANEXOS 103

LISTA DE ILUSTRACIONES

Ilustración 1. Utilidad del SGSI 15
Ilustración 2. Documentación de un SGSI. 16
Ilustración 3. Cronograma de Actividades 23
Ilustración 4. Diagrama de alto nivel Red Actual.....26
Ilustración 5. Organigrama HECC COURRIER.....29
Ilustración 6. Tipos de Activos 32
Ilustración 7. Tabla de Valoración de Riesgos.....49
Ilustración 8. Valoración del Riesgo vs Riesgo 96
Ilustración 9. Valoración del Riesgo vs Tiempo 97

LISTA DE TABLAS

Tabla 1. Material de oficina y gastos de papelería 21
Tabla 2. Costo Personal 22
Tabla 3. Hardware Necesario 22
Tabla 4. Licencia de Software 22
Tabla 5. Costo total de ejecución 22
Tabla 6. Aplicaciones actuales HECC COURRIER 28
Tabla 7. Descripción de cargos HECC COURRIER 30
Tabla 8. Matriz RACI HECC COURRIER 31
Tabla 9. Criterios de Valoración 34
Tabla 10. Valoración de Activos 37
Tabla 11. Escalas de Probabilidad de Vulnerabilidades 37
Tabla 12. Identificación y Valoración de Vulnerabilidades 44
Tabla 13. Listado de Amenazas 48
Tabla 14. Descripción Valoración de Riesgos 50
Tabla 15. Tabla de Probabilidad 51
Tabla 16. Valoración de Impacto 52
Tabla 17. Identificación de Riesgos 55
Tabla 18. Escalas de Impacto y Probabilidad 55
Tabla 19. Mapa de Calor de Riesgos 56
Tabla 20. Análisis de Controles aplicables 94
Tabla 21. Asociación de riesgos con los controles ISO 27001:2013. 94

RESUMEN

El presente trabajo está basado en la realización del diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para una empresa de mensajería llamada HECC COURRIER. Durante el desarrollo se establece como base la gestión de la seguridad dada por la ISO 27001 y de allí se efectúa todo el análisis correspondiente para la óptima realización de las políticas de seguridad de la empresa y de la guía de implementación consecuente a dichas políticas. Todo este trabajo busca que la empresa mejore la seguridad en sus procesos de correspondencia principalmente y en las actividades relacionadas a esta, para que con ello en un futuro puedan pensar en la obtención de la certificación ISO 27001 teniendo en cuenta el documento presente.

El contenido del trabajo se basa en el desarrollo de los objetivos, los cuales están divididos en cinco capítulos, así mismo se describe por qué se está desarrollando este proyecto y la situación actual de la empresa. A continuación, se detalla brevemente cada capítulo:

Primero se desarrolla el capítulo de Definición y análisis, con el cual se describe el planteamiento del problema, la formulación, la justificación, los objetivos, el cronograma de actividades, la metodología, el estado del arte, la factibilidad económica y el impacto deseado.

El segundo capítulo describe la situación actual de la empresa, su funcionamiento, organigrama y la infraestructura tecnológica actual, detallando su cableado, red de datos y aplicaciones que maneja.

Luego se efectúan las soluciones de los objetivos planteados, en primera medida se realiza el diagnostico de amenazas y vulnerabilidades, con lo cual se hace la identificación de activos, vulnerabilidades y amenazas, para finalizar con el respectivo análisis del impacto que estos tienen sobre los activos de la empresa.

El cuarto capítulo detalla la gestión de los riegos y las medidas apropiadas para proteger los activos de información, haciendo un análisis de los dominios y controles del anexo A de la ISO 27001.

El quinto capítulo es el desarrollo principal del presente trabajo, las políticas de seguridad de la empresa, así mismo en el sexto capítulo se tiene la guía de implementación de dichas políticas y del sistema de gestión de seguridad de la información.

Por último, se muestra el desarrollo del módulo web enfocado a la gestión del control de incidentes durante la implementación del SGSI.

ABSTRACT

The present work is based on the realization of the design of an Information Security Management System (ISMS) for a messaging company called HECC COURRIER. During the development, the security management based by ISO 27001 is established as a basis and from there all the corresponding analysis is carried out for the optimal performance of the company's security policies and the implementation guide consistent with the policies. All this work seeks that the company improves security in its correspondence processes mainly and related activities, so that in the future they can think about obtaining the ISO 27001 certification according to this document.

The content of the work is based on the development of the objectives, which are divided into five chapters, likewise describes the current situation of the company and why this project is being developed. Here is a brief description of each chapter:

First, the definition and analysis chapter is developed, which describes the problem statement, the formulation, the justification, the objectives, the schedule of activities, the methodology, the state of the art, the economic feasibility and the impact desired.

The second chapter describes the current situation of the company, its operation, organization chart and the current technological infrastructure, detailing its wiring, data network and applications.

Then the solutions of the proposed objectives are made, firstly the diagnosis of threats and vulnerabilities is made, with which the identification of assets, vulnerabilities and threats is made, to end with the respective analysis of the impact they have on the assets of the company.

The fourth chapter details the management of risks and the appropriate measures to protect information assets, making an analysis of the domains and controls of Annex A of ISO 27001.

The fifth chapter is the main development of the present work, the security policies of the company, likewise in the sixth chapter we have the guide of implementation of these policies and of the information security management system.

Finally, the development of the web module focused on the management of incident control during the implementation of the ISMS is realized.

INTRODUCCIÓN

La seguridad de la información en el mundo actual es de vital importancia para el funcionamiento de todas las empresas; la protección de sus activos de información es la prioridad y en lo que se basa la gestión de dicha seguridad y por la cual se implementan metodologías y procesos capaces de protegerla estructuradamente y efectivamente. Para ello, se tiene como idea principal el desarrollo de sistemas de seguridad de la información, que fundamentan su realización en el aseguramiento de los tres pilares de la información como lo son la confidencialidad, la integridad y la disponibilidad.

HECC COURRIER es una organización enfocada servicio al servicio de mensajería especializada, administración de centros de correspondencia y gestión documental, para los distintos sectores económicos públicos y privados a nivel nacional; cumpliendo con las necesidades y expectativas del cliente en cuanto a oportunidad y calidad del servicio, apoyados en talento humano competente y responsable. Teniendo en cuenta la importancia que la empresa en mención realiza en su actividad diaria se ha identificado la debilidad en su gestión de seguridad, pero no en sus procesos como tal si no en general al no tener unas políticas de seguridad establecidas y con las cuales se pueda desarrollarse procesos que permitan determinar el tratamiento adecuado de la información tanto de la empresa como de sus clientes.

El presente trabajo tiene como fundamento diseñar un sistema de gestión de seguridad dado bajo el desarrollo prioritario de las políticas de seguridad y la definición su proceso de implementación. Con base en esto se han definido proyectos relacionados y exitosos que se basan en dicha idea promulgada por la norma ISO 27001. Es claro que la seguridad de la información como activo más valioso e importante y no solo de la propia empresa si no de los clientes que maneja HECC COURRIER, hay que realizarle una serie de procesos para su protección debida. Gracias a esto se ha descrito el cronograma de actividades dado bajo el método PHVA con una duración de seis meses y un presupuesto acorde a lo que es necesario para desarrollar la idea. Así mismo como valor agregado se tiene el desarrollo de un módulo web para la gestión del control de incidentes que se puedan presentar durante el proceso de implementación basado en las políticas de seguridad establecidas.

1. DEFINICIÓN Y ANÁLISIS

1.1 TEMA

El presente trabajo tiene como tema principal el diseño de un sistema de gestión de seguridad de la información, con lo cual la empresa HECC COURRIER tendrá la posibilidad de mejorar sus procesos con una normativa que determina de manera adecuada el tratamiento de la información dado gracias la gestión de los riesgos analizados y evaluados.

1.2 TITULO

Diseño de un sistema de gestión de seguridad de la información (SGSI) para la empresa HECC COURRIER basado en ISO 27001.

1.3 PLANTEAMIENTO DEL PROBLEMA

HECC COURRIER es una organización enfocada servicio al servicio de mensajería especializada, administración de centros de correspondencia y gestión documental, para los distintos sectores económicos públicos y privados a nivel nacional; cumpliendo con las necesidades y expectativas del cliente en cuanto a oportunidad y calidad del servicio, apoyados en talento humano competente y responsable.

En la creciente expansión de la organización se necesita que se tenga un manejo de la información confiable e íntegro, ya que se han tenido inconvenientes con el tratamiento de la información de los clientes la cual reposa en la base de datos de la compañía, estos inconvenientes generan información errónea, como por ejemplo cuando se envía correspondencia a lugares incorrectos. La información que se registra en bases de datos, documentos, archivos, stickers de correspondencia e imágenes, se convierte en el principal activo para la organización, en consecuencia, se puede presentar un riesgo alto e impacto severo.

Con base a lo anterior, se debería contar con un sistema de gestión de seguridad de la información que se componga de políticas, procedimientos y normas, las cuales son esenciales para un buen manejo de la información. El sistema de gestión de la seguridad de la información debe trabajar en un ciclo de mejora continua que se integre con los procesos de la compañía y de esta manera no se sigan presentando los problemas que causan considerables fallas en la ejecución sistemática de los procedimientos de correspondencia especializada, lo cual puede causar una mala reputación de la empresa, perdidas económicas, etc.

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

Diseñar el Sistema de Gestión de la Seguridad de la Información (SGSI) y definir su proceso de implementación de acuerdo con la norma ISO 27001 para la empresa HECC COURRIER.

1.4.2 OBJETIVOS ESPECIFICOS

- Diagnosticar las amenazas y vulnerabilidades presentadas en el flujo de tratamiento de la información y analizar el impacto en los activos de la empresa.
- Analizar los riesgos de seguridad de la empresa y con ello definir las medidas apropiadas a aplicar para proteger los activos de información.
- Diseñar un documento guía que especifique las políticas de seguridad de la empresa.
- Definir mediante un documento el proceso de Implementación de acuerdo con las políticas de Seguridad de la empresa.
- Desarrollar un módulo web que permita gestionar el control de incidentes durante el proceso de implementación y operación del SGSI.

1.5 FORMULACIÓN DEL PROBLEMA

¿Cómo se puede tener una manipulación segura, confiable e íntegra de la información en la empresa HECC COURRIER gracias al diseño de un Sistema de Gestión de la Seguridad de la Información?

1.6 JUSTIFICACIÓN

La empresa HECC COURRIER necesita establecer e implementar de manera eficaz una serie de políticas de seguridad, capaces de mantener protegidos tantos los activos de información como los procesos que lo respaldan. Es por eso, que se han planteado una serie de soluciones a los problemas evidenciados, de acuerdo a la falta de un compromiso de seguridad se deben efectuar dichas políticas dadas bajo un documento escrito que permita llevar a cabo las normas y comportamientos que los actores que se encuentran en la empresa deben cumplir a cabalidad. En dicho documento se establecen claramente los activos de información, los riesgos, las amenazas, los controles que se deben ejecutar, políticas para el acceso y manipulación de la información, entre muchas más.

Desarrollar las políticas de seguridad de la empresa HECC COURRIER es el eje principal del proyecto, pero definirlas no basta para que se cumplan los objetivos, y es allí donde se tiene también una guía que va a definir el proceso de implementación de dichas políticas y que pondrá en ejecución el Sistema de Gestión

de la Seguridad de la Información. Se va a estructurar y determinar cómo se debe implementar dicho SGSI, definir los roles a los usuarios, accesos a la información y sobretodo la normatividad a cumplir para que los procesos se realicen adecuadamente. Detallar claramente el paso a paso de la implementación de controles de seguridad definiendo prioridades para ello, teniendo presente los riesgos que pueden causar un impacto más alto, así estos deberán ejecutarse como primera medida.

1.7 ESTADO DEL ARTE

Sistema de Gestión de Seguridad de la Información (SGSI)

Este sistema está definido bajo el objetivo fundamental de la Norma ISO27001, el cual describe cómo gestionar la seguridad de la información de una empresa. Así mismo la norma no discrimina el tipo de organización ni su fundamento. Un sistema de Seguridad de la Información bien gestionado puede lograr que la empresa tenga la posibilidad de certificarse en dicha norma y darle un estatus mayor y credibilidad en su labor.

El Sistema de Gestión de Seguridad de la Información, según ISO 27001 consiste en preservar la confidencialidad, integridad y disponibilidad, además de todos los sistemas implicados en el tratamiento dentro de la organización. Este SGSI debe estar gestionado de forma correcta garantizando que se cumpla el fundamento de los tres principios anteriormente mencionados: Confidencialidad. La información no se pone a disposición de nadie, ni se revela a individuos o entidades no autorizados. Integridad. Mantener de forma completa y exacta la información y los métodos de proceso. Disponibilidad. Acceder y utilizar la información y los sistemas de tratamiento de la misma parte de los individuos, entidades o proceso autorizados cuando lo requieran.



Ilustración 1. Utilidad del SGSI Fuente: Iso27000.es

Los beneficios que se pueden obtener al efectuar un SGSI se describen a continuación: Establecer una metodología de Gestión de la Seguridad estructurada y clara. Reducir el riesgo de pérdida, robo o corrupción de la información sensible. Los clientes tienen acceso a la información mediante medidas de seguridad. Los riesgos y los controles son continuamente revisados. Se garantiza la confianza de los clientes y los socios de la organización. Las auditorías externas ayudan de forma cíclica a identificar las debilidades del SGSI y las áreas que se deben mejorar. Facilita la integración con otros sistemas de gestión. Se garantiza la continuidad de negocio tras un incidente grave. Cumple con la legislación vigente sobre información personal, propiedad intelectual y otras. La imagen de la organización a nivel internacional mejora. Aumenta la confianza y las reglas claras para las personas de la empresa. Reduce los costes y la mejora de los procesos y el servicio. Se incrementa la motivación y la satisfacción del personal. Aumenta la seguridad en base la gestión de procesos en lugar de una compra sistemática de productos y tecnologías.

La documentación mínima que se debe tener en cuenta a la hora de implementar un SGSI: Política y objetivos de seguridad. El alcance del SGSI. Los procedimientos y los controles que apoyan al SGSI. Describir toda la metodología a la hora de realizar una evaluación de riesgo. Generar un informe después de realizar la evaluación de riesgo. Realizar un plan de tratamiento de riesgos. Procedimientos de planificación, manejo y control de los procesos de seguridad de la información y de medición de la eficacia de los controles. Declaración de aplicabilidad. Procedimiento de gestión de toda la documentación del SGSI. [1]



Ilustración 2. Documentación de un SGSI.

Fuente Iso27000.es

Teniendo clara la documentación y de cómo esta debe estar formada, también se debe gestionar de manera adecuada su desarrollo e implementación y es por ello que se requiere mantener un procedimiento siguiendo las siguientes acciones: Aprobar documentos apropiados antes de su emisión. Revisar y actualizar documentos cuando sea necesario y renovar su validez. Garantizar que los cambios

[1] El Portal de ISO27001 en español. Que es un SGSI. Julio 2015. Recuperado de http://www.iso27000.es/sgsi.html

y el estado actual de revisión de los documentos están identificados. Garantizar que las versiones relevantes de documentos vigentes están disponibles en los lugares de empleo. Garantizar que los documentos se mantienen legibles y fácilmente identificables. Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente destruidos acorde con los procedimientos aplicables según su clasificación. Garantizar que los documentos procedentes del exterior están identificados. Garantizar que la distribución de documentos está controlada. Prevenir la utilización de documentos obsoletos. Aplicar la identificación apropiada a documentos que son retenidos con algún propósito. [2]

Estado del Arte:

Las organizaciones a través de su ciclo de crecimiento se han dedicado en muchos procesos en el tratamiento de la información este es un activo primordial de los procesos de organización donde se debe salvaguardar, procesar y transferir adecuadamente donde se garantice una "protección" en todos los aspectos (físicos, lógicos, humanos). Resolviendo en una idea principal la importancia de crear un SGSI se debe constituir un modelo normativo el cual puede estructurarse mediante el documento de políticas, teniendo en cuenta uno a uno todos los dominios y normas que complementen a la política y que agrupen los objetivos de control existentes en un entorno como la ISO 27001. Estableciendo controles efectivos que impidan colocar en riesgo la información. En producto de este nuevo enfoque empresarial se han desarrollado estudios, investigaciones y proyectos de grado relacionados con la visión de un diseño de un sistema de gestión de la información, los cuales han sido tomados como referentes para el desarrollo del presente trabajo, los cuales se describen a continuación:

SALCEDO, Robin J. en la ciudad de Barcelona, desarrolló una investigación con el nombre de "plan de implementación del SGSI basado en la norma ISO/IEC 27001:2013".

La investigación se centra en la implementación de un SGSI en la empresa ISAGXXX para solucionar problemas de seguridad en los servicios de información con la finalidad de llevar el riesgo a un nivel tolerable. El autor concluye que el apoyo de la gerencia es vital para el desarrollo de proyecto y que se deben realizar auditorías periódicamente, por otro lado, es necesario aumentar el presupuesto para la implementación de estrategias de seguridad informática en la organización. El aporte teórico de esta investigación al desarrollo del presente trabajo es el apoyo que el autor hace de la norma ISO/IEC 27001:2013.

[2] El Portal de ISO27001 en español. Que es un SGSI. Julio 2015. Recuperado de http://www.iso27000.es/sgsi.html

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL ÁREA DE CONTABILIDAD DE LA E.S.E. HOSPITAL LOCAL DE RIO DE ORO CESAR

Mediante un SGSI sistema de gestión de seguridad de la información, el área de contabilidad de la E.S.E hospital local de rio de oro cesar conseguirá minimizar considerablemente el riesgo de que su productividad se vea afectada debido a la ocurrencia de un evento que comprometa la confidencialidad, disponibilidad e integridad de la información o de alguno de los sistemas informáticos. Este sistema permite identificar, gestionar y minimizar los riesgos reales y potenciales de la seguridad de la información, de una forma documentada, sistemática, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. (CASADIEGOS SANTANA, 2014).

ELABORACIÓN DE POLÍTICAS DE SEGURIDAD FÍSICA Y AMBIENTAL BASADOS EN EL ESTÁNDAR INTERNACIONAL ISO/IEC 27002:2013 EN EL HOSPITAL REGIONAL JOSÉ DAVID PADILLA VILLAFAÑE ESE. DE LA CIUDAD DE AGUACHICA-CESAR.

Este documento tiene por objetivo la creación de las políticas de seguridad física y ambiental que brinde apoyo para poder proteger la información en el hospital José David padilla Villafañe de Aguachica, para las mejores prácticas en el uso adecuado según los lineamientos del estándar internacional ISO/IEC 27002:2013, y a su vez proporcionar un plan de mejora para la optimización, brindando recomendaciones en forma sencilla y entendible, acerca de cómo mejorar los procesos par a proteger la in formación. (MOSQUERA QUINTERO, 2015).

Elaboración de políticas y normas de seguridad de la información en base a la norma de seguridad ISO/IEC 27001, y al análisis de riesgos realizado aplicando la metodología Magerit y la herramienta Pilar. Tixilima Cisneros, Viviana de los Ángeles

Este documento informa la creación de políticas de Seguridad basadas en las normas ISO/IEC 27001 para la red de la Universidad Politécnica Salesiana Sede Quito Campus Sur, mediante la utilización de la metodología MAGERIT para el Análisis y Gestión de Riesgos. Su principal fin es conocer el estado actual de red, definir los activos y el valor que estos tienen para la empresa, identificar amenazas, evaluar riesgos, ya que la información es un recurso vital para toda institución; y esta es generada en función de las actividades que se llevan a cabo en cada área o departamento, por lo que se busca establecer e implementar políticas de seguridad, que permitan controlar el acceso a recursos en la red, mismas que permitan asegurar la disponibilidad, integridad y confidencialidad en el manejo de la información, minimizando e identificando los riesgos de ocurrencia.

Desarrollo de un sistema de información para gestionar la implantación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2013. Mahecha Guzmán, Mayra Lorena; Coello Falcones, Gabriel Ricardo

Se analiza el contexto general y los antecedentes de la solución propuesta que basada en la experiencia de sus autores sugiere que gestionar la implantación y mantenimiento de un SGSI debería ser más ágil con la ayuda de un sistema de información que automatice la gestión de los activos de información y sus riesgos. Se presenta el marco teórico de la seguridad de la información y la Norma ISO 27001, se explican también los conceptos relacionados a un SGSI como activo de información, amenaza, vulnerabilidad, riesgo y la estrecha relación del SGSI con el ciclo de PHVA. Se expone además el enfoque y la nueva estructura de la norma en la versión 2013 así como también una comparativa con la versión del 2008 para verificar los cambios más sustanciales. Se presentan los resultados de las pruebas de la solución propuesta una vez que se completan con éxito cada una de las fases planteadas en función de los objetivos propuestos y del uso del sistema per se.

1.8 METODOLOGÍA

Teniendo en cuenta la normativa ISO 27001 y como esta se fundamenta mediante los Sistemas de Gestión de Seguridad de la Información se ha determinado una metodología que es idónea para efectuar el diseño y posterior definición del proceso de implementación de dicho SGSI. Como tal, no está definida como una metodología, pero los pasos y actividades que se determinan allí hacen que sea lo indicado para efectuar este proyecto, el ciclo PHVA o método de Demming. PHVA (Planear, Hacer, Verificar y Actuar) es un ciclo o método de mejora continua que es idóneo para efectuar dichos procesos de gestión de riesgos y de seguridad de la información como tal donde su objetivo es establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

Método de Demming o Ciclo PHVA

El ciclo PHVA o ciclo de Deming fue dado a conocer por Edwards Deming en la década del 50, basado en los conceptos del estadounidense Walter Shewhart. PHVA significa: Planificar, hacer, verificar y actuar. En inglés se conoce como PDCA: Plan, Do, Check, Act.

Este ciclo constituye una de las principales herramientas de mejoramiento continuo en las organizaciones, utilizada ampliamente por los sistemas de gestión de la calidad (SGC) con el propósito de permitirle a las empresas una mejora integral de la competitividad, de los productos ofrecidos, mejorado permanentemente la calidad, también le facilita tener una mayor participación en el mercado, una optimización en los costos y por supuesto una mejor rentabilidad. Por su dinamismo puede ser utilizado en todos los procesos de la organización y por su simple

aplicación, que, si se hace de una forma adecuada, aporta en la realización de actividades de forma organizada y eficaz. [3]

Para tener más claro las etapas de dicho método, se hace una breve descripción de cada uno:

Planificar: En esta etapa se establece un análisis de las políticas, objetivos y procesos de calidad que cuenta la empresa, hay que identificar todo tipo de riesgos y detalles que puedan perjudicar la seguridad de la información, ya que este es el activo más valioso con que se cuenta, no solo información de la empresa si no la sensibilidad de la información de los clientes que han confiado su trabajo. Así mismo se definen las metas y métodos como los planes de acción y procesos de implementación a desarrollar, todo de acuerdo a las políticas organizacionales y necesidades de los clientes. Puede ser de gran utilidad realizar grupos de trabajo, escuchar opiniones de los trabajadores y utilizar herramientas de planificación como por ejemplo: 5W2H en la cual se responden 7 preguntas claves cuyas palabras en inglés inician con W y H : ¿Qué (What), ¿Por qué (Why), ¿Cuándo (When) ¿Dónde (Where) ¿Quién (Who), ¿Cómo (How) y ¿Cuánto (How much). Hay que tener en cuenta que esta etapa es la base fundamental para la ejecución de las siguientes, se debe hacer claridad y énfasis en la estructura de lo que se piensa hacer.

Hacer: La segunda etapa del método se basa en aplicar lo planeado, es decir empezar a implementar lo que se tiene como base y lo que el análisis ha arrojado. Para este caso se puede demostrar a los empleados de la empresa como se debe efectuar los servicios y del cuidado que deben tener para que no hayan fugas de información, por ende, se debe educar, entrenar y capacitar para que cada miembro que tiene un rol a su cargo lo cumpla a cabalidad. Aquí ya se debe desarrollar las políticas de seguridad de la empresa, definir el Sistema de Gestión de Seguridad y los procesos que se deben realizar para implementarlo acorde a lo estipulado en la planeación.

Verificar: Esta etapa verifica y analiza lo que se ha implementado en la anterior ejecución, donde se efectúa seguimiento y medición de los procesos que se realizaron de acuerdo a las políticas y objetivos estipulados, así como los planes y metas, ya que esto es a donde se quiere llegar. Se debe hacer un análisis de calidad y productividad para evidenciar que todo este marchando de la mejor manera.

Actuar: El último paso determina el proceso de mejora continua, ya que con los resultados arrojados por la verificación se toman decisiones que permitan estandarizar cundo los procesos satisfacen los requerimientos y objetivos o si se encontraron problemas y errores saber cómo corregirlos con planes de acción correctivos y preventivos para una próxima iteración del ciclo.

[3] Sanchez Moreno, Yuli Paola. Ciclo PHVA. 2014. Recuperado de https://www.gerencie.com/ciclo-phva.html

Visto lo anterior, vemos la interdependencia entre las cuatro partes del ciclo. De manera que, si no se realiza adecuadamente alguna de ellas, se traducirá en un bajo rendimiento del SGSI e incumplimiento de los objetivos referentes a la política de Seguridad. Esto pone de relieve la suma importancia de una correcta realización del ciclo. Además de lograr esos beneficios de optimizar rendimiento y cumplir objetivos, la ejecución del ciclo como apoyo al SGSI contribuye a proteger a sus empleados y otras partes interesadas, así como ayuda a mejorar la imagen comercial. [4]

Después de describir brevemente el ciclo PHVA y de porque es necesaria su implementación en Sistemas de Gestión de Seguridad de la Información, hay que aclarar que para este proyecto como se enfoca básicamente en el diseño y definición del proceso de implementación del SGSI solo se tomaran las dos primeras fases del ciclo, es decir, la fase de Planear y la de Hacer, claro está que en la parte de Hacer no se va a implementar el SGSI, pero si se toman algunas actividades para la creación de las políticas, la capacitación que pueda surgir para fomentar en los empleados dichos valores y comportamientos de acuerdo a la seguridad, y la definición como tal del proceso de Implementación. Puede que todo el proceso abarque la fase de planear, ya que allí se hace todo el análisis de la seguridad de la empresa, pero como tal el desarrollo del proyecto debe realizarse en el hacer. La fase de Verificar y Actuar como ciclo de mejora continua corresponde a la empresa desarrollarlas al momento de ejecutar e implementar el SGSI.

1.9 FACTIBILIDAD

El presupuesto realizado para la ejecución del presente proyecto se describe bajo cuatro ítems, los cuales describen detalladamente su costo, cantidad y costo total, a continuación, se muestran los gastos necesarios para efectuarlo:

Descripción	Costo aproximado	Cantidad	Costo total del desarrollo
Material de oficina	$ 60.000,00	5	$ 300.000,00
Papel de impresión	$ 10.000,00	5	$ 50.000,00
Cartuchos de impresión	$ 150.000,00	1	$ 150.000,00
Recarga de cartuchos	$ 20.000,00	4	$ 80.000,00
Servicio de Internet Claro 5Gb	$ 45.000,00	2	$ 90.000,00
Total	$ 240.000,00	15	$ 580.000,00

Tabla 1. Material de oficina y gastos de papelería
Fuente: Los Autores

[4] ISOTools Colombia. OHSAS 18001: La importancia del ciclo PHVA (Planificar-Hacer-Verificar-Actuar). Mayo 2016. Recuperado de http://www.isotools.com.co/ohsas-18001-la-importancia-del-ciclo-phva-planificar-hacer-verificar-actuar/

Recurso humano	Sueldo hora	Cantidad de horas	Sueldo total
Estudiante	$ 20.000,00	200	$ 4´000.000,00
Director	$ 30.000,00	20	$ 600.000,00
Asesor	$ 25.000,00	40	$ 1’000.000,00
Total	$ 75.000,00	260	$ 5’600.000,00

Tabla 2. Costo Personal
Fuente: Los Autores

Descripción	Valor unitario	Cantidad	Valor total
Lenovo 40e	$ 1.900.000,00	1	$ 1.900.000,00
Toshiba Satellite s855-S5369	$ 1.380.000,00	1	$ 1.380.000,00
Impresora Samsung Sl-m2020w	$ 285.000,00	1	$ 350.000,00
Accesorios de conexión	$ 15.000,00	2	$ 30.000,00
Total	$ 3’144.016,00	4	$ 3.660.000,00

Tabla 3. Hardware Necesario
Fuente: Los Autores

Descripción	Valor unitario	Cantidad	Valor total
Licencia Windows 10 Profesional	$ 350.000,00	2	$ 700.000,00
Total	$ 350.000,00	2	$ 700.000,00

Tabla 4. Licencia de Software
Fuente: Los Autores

Descripción	Valor
Material de oficina	$ 580.000,00
Recurso humano	$ 5’600.000,00
Hardware	$ 3.660.000,00
Software	$ 700.000,00
Total	$ 10.540.000,00

Tabla 5. Costo total de ejecución
Fuente: Los Autores

1.10 CRONOGRAMA

Se presenta el siguiente cronograma para la realización del proyecto a seis meses:

Id	Modo de tarea	Nombre de tarea	Duración
1		**FASE DE PLANEACION**	60 días
2		Levantamiento de Informacion	2 días
3		Establecer el contexto con la organización	4 días
4		Alcance del Sistema de Gestión de la Seguridad de la Información	3 días
5		Definir la Politica del SGSI	13 días
6		Definir una metodología de evaluación del riesgo apropiada para el SGSI	4 días
7		Identificación de los Riesgos	12 días
8		Analisis y Evauacion de los Riesgos	6 días
9		Identificar y evaluar las distintas opciones de tratamiento de los riesgos	6 días
10		Seleccionar los objetivos de control y los controles	7 días
11		Aceptacion de los Riesgos	5 días
12		**FASE DE IMPLEMENTACIÓN**	50 días
13		Diseño, creacion y eventos de base de datos para modulo de incidentes	30 días
14		Definir un plan de tratamiento de riesgo	7 días
15		Determinar el proceso de Implantacion del plan del tratamiento de riesgos	8 días
16		Definir un sistema de métricas	6 días
17		Definir proceso de implementacion programas de formación y	5 días
18		Gestionar la operación del SGSI	6 días
19		Gestionar recursos necesarios asignados al SGSI	7 días
20		Implementar procedimientos y controles para la gestión de incidentes de seguridad	9 días

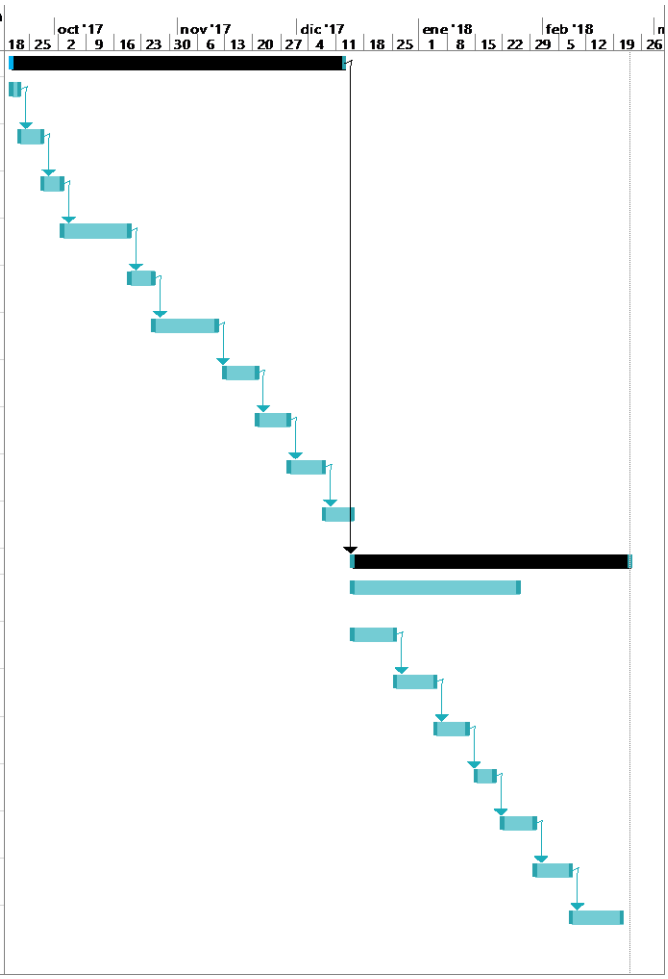


Ilustración 3. Cronograma de Actividades
Fuente: Los Autores

1.11 RESULTADOS ESPERADOS

El actual proyecto descrito, tiene como fundamento que se identifiquen todo tipo de riesgos que se presentan actualmente en la empresa, habiendo realizado un diagnóstico de todos los procesos y de cómo se podría afectar los activos de información se pretende efectuar el desarrollo de un SGSI, definiendo claramente unas políticas de seguridad que la empresa pueda establecer de acuerdo al presupuesto que maneja. Así mismo se definirá un plan de acción dado por una guía para el proceso de implementación de dicho SGSI que determine los procesos críticos que se manejan en la empresa y de cómo esta debe priorizarlo para gestionar debidamente la seguridad de los activos con que cuenta. Se espera que

todos los actores de la empresa obtengan una conciencia con todo lo relacionado a la seguridad de la información, y de como esta, cuando es afectada puede ocasionar daños en todos los aspectos de la organización y donde ellos pueden tener el riesgo de perder sus trabajos respectivos. Es por todo esto que se espera que el buen desarrollo de dichas políticas genere dicho interés por salvaguardar sus activos y de cómo teniendo esta base se mejore en la productividad que puede ocasionar una confianza en los clientes a su cargo.

1.12 IMPACTO

Gracias a las soluciones mencionadas anteriormente, se pretende generar conciencia en la organización sobre la importancia de los activos que se manejan y de cómo los procesos involucrados deben ser llevados de manera eficaz para generar una mayor productividad, eficiencia y sobretodo una satisfacción de los clientes a la hora de solicitar y recibir el servicio de mensajería.

Como un valor agregado, el diseño y definición del proceso de implementación del SGSI puede ser la base para que la empresa HECC COURRIER obtenga la certificación ISO 27001, dado que ejecutando correctamente el SGSI definido y acatando todas las normativas que ISO 27001 propone, es posible que durante las auditorias correspondientes no se encuentren hallazgos o incidentes que provoquen retrasos en la adquisición del certificado, pero si las hay es necesario efectuar el SGSI como ciclo de mejora continua donde al encontrar fallas se debe analizar y efectuar todo el procedimiento de nuevo para su correcta solución.

Así mismo, se ha determinado como solución tecnológica concreta, diseñar e implementar un desarrollo web que permita gestionar y controlar los incidentes durante el proceso de implementación y operación del SGSI. Es claro que dicho desarrollo se centrará en efectuar un módulo capaz de ello y además debe tomar como base lo analizado durante la fase de planeación del proyecto. Dicho módulo de control de incidentes puede colaborar en un proceso futuro de certificación de la ISO 27001, además dará el primer paso para que la empresa pueda implementar más procesos haciendo que dicho desarrollo se convierta en un sistema de información web completamente estructurado bajo los lineamientos de las políticas de seguridad y el SGSI a ejecutar.

2. SITUACIÓN ACTUAL

La empresa HECC COURRIER actualmente presta servicios de correspondencia bancaria, a continuación, se detalla el flujo de información en el proceso de dicha correspondencia:

Para el servicio de correspondencia bancaria se recibe la información de los productos, esta llega por un canal seguro SFTP, donde allí el banco dispone de la base de datos en un archivo encriptado por PGP. Este almacenamiento es del banco, la persona encargada de HECC COURRIER se conecta por medio de SFTP con un usuario y contraseña al directorio virtual que dispone el banco y descarga las carpetas de la relación de lo que va a llegar a HECC COURRIER. Luego en el transcurso del día se genera una planilla dada en formato Microsoft Excel, con la cual la persona encargada de descargar la información convierte dicho archivo en formato Excel a un archivo plano tipo .dbs4, y este es subido al SIM (Sistema de mensajería de la empresa), después otra persona crea las guías por el sistema dándoles una OIP como un número de identificación. El siguiente proceso es la generación de un numero de guía, el cual si dicha guía dice que se dirige a otra ciudad se contrata el servicio con un tercero como puede ser Servientrega u otra empresa de mensajería, estos realizan el envío a una de las sedes de HECC COURRIER del país dependiendo de donde se encuentre el destinatario. En cada sede hay una persona encargada de recibir el archivo Excel de lo que se envió y vuelve a separarlo para ser distribuido por HECC COURRIER a las ciudades correspondientes. Con esto se identifica que se realiza manipulación de la información en todo el proceso de correspondencia.

Otra opción que proporciona HECC COURRIER para el envío de correspondencia, dejando de lado el tema bancario, se basa en que los clientes pueden entregar la relación de los productos a enviar vía email o USB. La empresa HECC COURRIER no tiene un canal propio y seguro donde los clientes puedan dejar la relación de los productos.

En cuanto al acceso a la organización y sus instalaciones no se tienen tarjetas de acceso ni ningún nivel de seguridad en el área de operaciones que es la encargada de realizar la administración anteriormente descrita.

Todo el punto central de la sucursal de Bogotá tiene acceso a una red normal, está configurada por un servidor proxy y un servidor de base de datos que es el encargado de tener la base de datos del sistema de correspondencia SIM de Bogotá. Este sistema solo lo posee esta sede, en las demás sedes la información es manipulada y enviada por correo a la central de Bogotá. La documentación del manejo de este sistema radica en una persona encargada de dirigir toda la operación día a día.

La administración de contraseñas se tiene por medio de un directorio activo, pero no se tiene un cambio de contraseñas periódico, se mantienen siempre las mismas. Los servidores cuentan con un cuarto pequeño donde solo tiene acceso el encargado de sistemas; adicional a lo anterior no se tienen acuerdos de confidencialidad ni clasificación de la información tratada.

2.1 CARACTERIZACIÓN DE LA RED ACTUAL

Es importante tener claridad de la estructura de la red actual que presenta la empresa HECC COURRIER, con ello se puede comprender algunos aspectos que más adelante en el proyecto servirán para analizar en cuanto a la parte de infraestructura y aplicaciones los posibles riesgos que puedan encontrarse y de cómo deban ser tratados de acuerdo a esta descripción. A continuación, se presenta el diagrama de Alto nivel de la red actual:

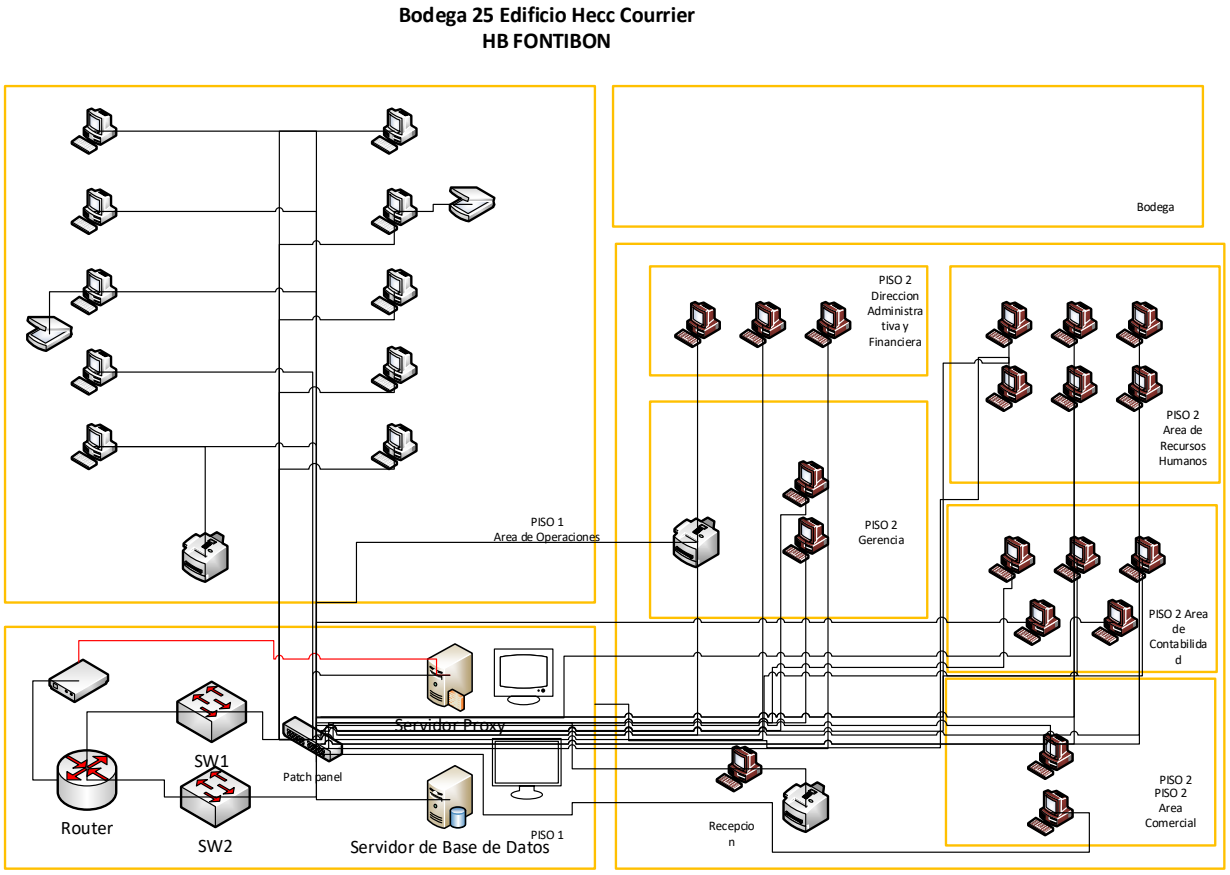


Ilustración 4. Diagrama de alto nivel Red Actual
Fuente: Los Autores

2.2 ESTRUCTURA DE LA RED ACTUAL

En la actualidad Hecc Courrier cuenta con una red con las siguientes características:

- Topología Estrella Jerárquica.
- 1 módem de fibra (ISP).
- 2 switch Cisco SLM 2048
- Cableado horizontal categoría6
- 1 rack de 34 unidades.
- 2 servidores (1 Servidor de base de datos, Windows Server 2003 y 1 Servidor Proxy, Windows Server 2008).
- 1 Patch panel cat. 5e, 24 puertos
- Organizador de cables horizontal para gabinete o rack
- Rack piso, abierto, altura 45U (210 cm), aluminio.
- Cableado UTP Cat5e.
- 2 ventiladores de torre con temporizador de 2 horas manual Bionaire.
- 1 Ups Batería De Energía Javan De 1000 Va.

2.3 REDES DE AREA LOCAL

Esta es la que utiliza la Hecc Courrier para compartir datos dentro de la sede principal, Cuando se forma una tormenta de broadcast se cae toda la red de la organización esto debido a que no hay una buena segmentación sería una buena práctica independizar las por VLAN'S por área para que en el momento en que se detecte un fallo considerable en la red se pueda definirá rápidamente donde se encuentra el problema presentado y darle una óptima solución sin afectar la mayor parte de la red.

2.4 SISTEMA ELÉCTRICO DE EMERGENCIA

En la red LAN actual cuando hay emergencia por falta de energía eléctrica, la UPS solo mantiene encendido los equipos principales solo por un lapso de media hora, para lo cual solo es tiempo suficiente para el apagado correcto de los equipos. Sería buena idea la implementación de una UPS con más capacidad de almacenamiento de energía y paralelo a esto que la compañía adquiera un generador eléctrico con mayor capacidad.

2.5 APLICACIONES ACTUALES

El software instalado en los servidores está orientado de acuerdo a las diferentes prácticas y su comportamiento por ello este se fundamenta como la plataforma

lógica sobre la cual se evaluarán los diferentes tipos de datos a transmitir de las tecnologías.

Aplicación	Tipo	Número de Usuarios	Observaciones
Base de datos SQL SERVER	Base de datos alfanuméricas	20	Sistema encargado de contener toda la data concerniente al negocio.
SIM	Software de Mensajería	8	Software especial de servicio de correspondencia
Correo Electrónico	Aplicativo encargado del correo corporativo.	30	Sistema encargado de manejar todo el correo corporativo de la compañía cuentan con office 365

Tabla 6. Aplicaciones actuales HECC COURRIER
Fuente: Los Autores

2.6 ESTUDIO GAP DE ACUERDO AL ANEXO A

El estudio gap se realizó en el capítulo numero 4 numeral 4.6 del presente proyecto.

Habiendo descrito anteriormente el flujo de información en el proceso de correspondencia y seguridad de la empresa se expone mediante un gráfico el organigrama y así mismo una tabla con la cual se detalla cada cargo que se presenta.

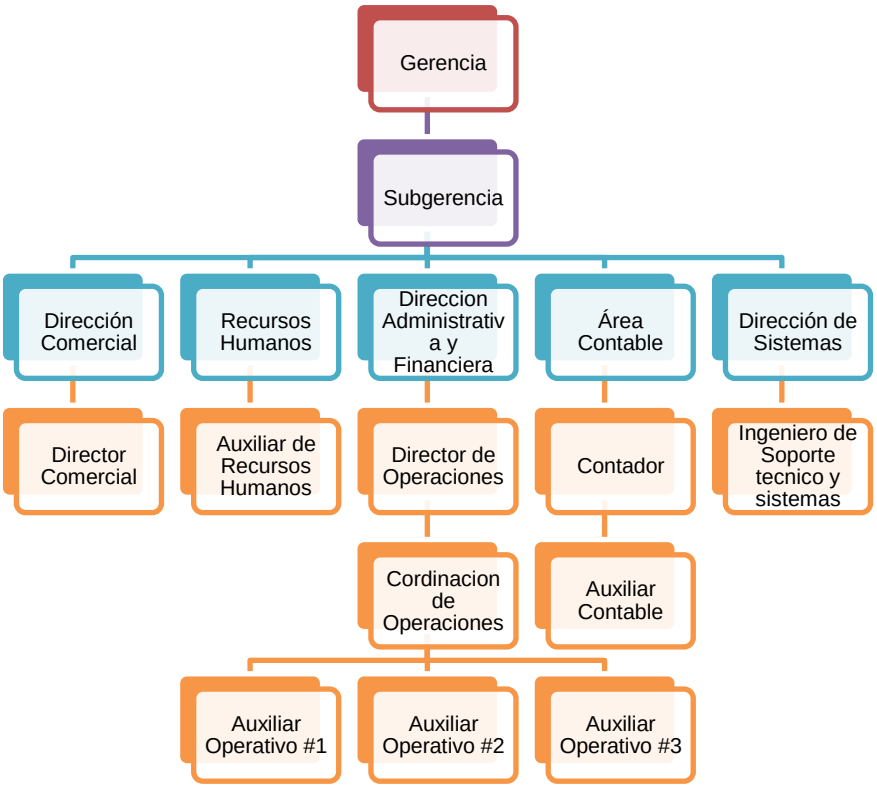


Ilustración 5. Organigrama HECC COURRIER
Fuente: Los Autores

La siguiente tabla describirá cada uno de los cargos que se encuentran en el organigrama anterior:

Cargo	Descripción
GERENTE	Cargo o posición dentro de la organización de una institución o empresa. El gerente es una persona que se encuentra a cargo de la coordinación o dirección de las actividades y funciones de una parte, de un departamento, sector o grupo de trabajo.
SUBGERENTE	Cargo de jefatura responsable de dirigir, supervisar y controlar las funciones, reemplazar al gerente en las actividades desarrolladas por el mismo cuando él se encuentre ausente.
DIRECTOR ADMINISTRATIVO Y FINANCIERO	Es la persona a cargo de administrar y vigilar los recursos económicos y financieros de la organización para poder laborar con las mejores condiciones de precio, fluidez, beneficio y seguridad.

Cargo	Descripción
DIRECTOR DE OPERACIONES	Es el encargado de supervisar y administrar que las operaciones de correspondencia y el proceso de correspondencia se lleve en un orden adecuado de mano de la coordinación de operaciones.
DIRECTOR DE RECURSOS HUMANOS	Ejecutivo encargado de la formación y el desarrollo, las relaciones laborales, la salud y la seguridad, los salarios y los programas de beneficios, y la planificación de las futuras necesidades de contratación.
DIRECTOR COMERCIAL	Es la persona responsable del objetivo de cumplir con las metas de las ventas, mercadeo y una excelente imagen de la empresa.
CONTADOR	Sujeto experto para efectuar un rol técnico dentro del área contable de una organización y el uso de. Su tarea esencial consiste en llevar los libros principales y auxiliares de la misma. Adicional de ser el encargado de llevar informes ante la alta gerencia y manejar la aplicación de nómina.
AUXILIAR DE RECURSOS HUMANOS	Profesional administrativo que realiza una variedad de deberes sobre transacciones en apoyo al capital humano del negocio. Así mismo coordinar o realizar las capacitaciones a los empleados de la organización.
AUXILIAR CONTABLE	Es la persona encargada de registrar las transacciones contables de las operaciones de la compañía y verificar su adecuada contabilización y ser la mano derecha del contador.
INGENIERO DE SOPORTE TECNICO Y SISTEMAS	Conocer los sistemas y redes informáticos es una responsabilidad primaria de un ingeniero de soporte técnico. Estos profesionales tienen un conocimiento mucho más extenso que el personal primario de apoyo técnico. Los ingenieros de soporte técnico deben sobresalir en la resolución de problemas.
OORDINADOR DE OPERACIONES	Es la perdona que se encarga de dirigir el desarrollo de las actividades operativas de la empresa, garantizar que los procesos de lleven a cabo en el tiempo y la forma estipulados por la compañía con el fin de que se haga entrega de las mercancías de manera oportuna, coordinar que se cuente con los insumos necesarios para desarrollar las operaciones.
AUXILIAR OPERATIVO	Administrar la Base de Datos interna, filtrando información sistémicamente. Encargado de recibir y cumplir el proceso de correspondencia.

Tabla 7. Descripción de cargos HECC COURRIER
Fuente: Los Autores

Para finalizar la descripción de la empresa se tiene la matriz RACI correspondiente, donde las siglas descritas en la tabla se refieren a lo siguiente: Responsable (R), Encargado (A), Consultor (C) e Informado (I).

Tabla 8. Matriz RACI HECC COURRIER

	Seguridad de la información	***TI***	***Operaciones***	***RR.HH***	***Negocio***	***Dirigentes funcionales***
CONTADOR	*C*	*C*	*R A*	*I*	*C*	*C*
AUXILIAR DE RECURSOS HUMANOS	*I*	*I*	*C*	*R A*		
GERENTE		*I*	*C*	*I*	*C*	*R A*
SUBGERENTE		*I*	*C*	*I*	*C*	*R A*
DIRECTOR ADMINISTRATIVO Y FINANCIERO	*C*	*I*	*R A*	*I*	*R A*	*C*
DIRECTOR DE OPERACIONES	*C*	*C*	*R A*	*I*	*R*	*C*
INGENIERO DE SOPORTE TECNICO Y SISTEMAS	*R A*	*C*	*C*	*I*	*C*	
DIRECTOR COMERCIAL	*C*				*I*	*R*
DIRECTOR DE RECURSOS HUMANOS	*C*	*CI*	*I*	*A*	*A*	*C*
AUXILIAR CONTABLE	*C*	*C*	*R*	*I*	*C*	
COORDINADOR DE OPERACIONES		*I*	*R A*		*R*	
AUXILIAR OPERATIVO	*I*	*I*	*R*	*I*	*R*	

Fuente: Los Autores

3. DIAGNÓSTICO DE AMENAZAS Y VULNERABILIDADES

En este capítulo se efectúa el desarrollo de las diferentes etapas definidas para el diseño del SGSI de la empresa HECC COURRIER, teniendo en cuenta la recolección de la información y su respectivo análisis de acuerdo a la metodología descrita y la norma 27001 definida anteriormente, todo esto con el fin de poder cumplir con los objetivos trazados.

3.1 IDENTIFICACIÓN DE ACTIVOS

Se denominan activos a los recursos vitales de la empresa HECC COURRIER que generan, procesan, almacenan o transmiten información, los cuales son necesarios para que la Organización funcione en su proceso de correspondencia correctamente y alcance los objetivos propuestos por su dirección.



Ilustración 6. Tipos de Activos
Fuente: Los Autores

Gracias a esta clasificación se pueden determinar el listado de activos presentes en el caso a desarrollar. Pero primero se deben tener en cuenta los criterios de valoración de los activos en cuanto a la disponibilidad, integridad y confidencialidad. La clasificación de activos de información tiene como objetivo asegurar que la

información recibe los niveles de protección adecuados, ya que con base en su valor y de acuerdo a otras características particulares requiere un tipo de manejo especial.

La confidencialidad se refiere a que la información no esté libre y que no sea divulgada a personas, organizaciones o procesos no autorizados. La integridad se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción. La disponibilidad es el dominio de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso. La valoración se puede observar desde la necesidad de proteger, pues lo más valioso es un activo, y requiere mayor nivel de protección en la dimensión (o dimensiones) de seguridad que sea pertinentes.

Criterio	Disponibilidad	Integridad	Confidencialidad
Muy Alto (MA)	En el momento que se efectué un problema donde el activo debe estar disponible siempre.	Los activos que tenga una pérdida de exactitud y completitud en el proceso de correspondencia de la organización HECC COURRIER por ello su solución deben ser inmediata Solo se modifica con autorización de la Alta Gerencia.	Solo es posible el acceso por personal de la Alta gerencia y externos pertenecientes a un grado de director para tomar decisiones de los daños o perdidas causados en los activos
Alto(A)	Los errores o daños que afecten la disponibilidad de los activos ocasionan un impacto altamente negativo tanto a la entidad como a sus clientes en marcos legales, económicos, operacionales y de reputación. El error debe ser corregido en unas horas, los activos deben estar funcionando en todo momento.	Los activos que tenga una pérdida de exactitud y completitud en el proceso de correspondencia de la organización HECC COURRIER por ello su solución deben ser en unas horas. Afecta a la organización en sí y la integridad de los clientes de esta.	Los activos para el proceso de correspondencia debe ser confidencial de la organización, debe ser manejada cuidadosamente ya que si se conoce por un agente exterior puede causar impactos negativos ya sean legales, operativos, económicos o en su reputación.
Medio(M)	Al momento de efectuarse un problema en la organización con la pérdida o falla en los activos que posee la compañía deben	La pérdida del activo o daño del mismo, en cuanto a la exactitud y completitud de los procesos puede conllevar a consecuencias negativas	Los activos disponibles para todo el proceso de correspondencia debe ser manejada con cautela, aunque no tiene un impacto muy

	ser corregidas en el transcurso de 2 días. Es posible que la afectación sea tolerable en este tiempo y la entidad pueda funcionar a pesar de dicho error.	dentro de la entidad, afectando áreas específicas de la entidad y por ende los funcionarios que se desempeñan allí. Debe haber una solución pronta.	grande hay que ser precavidos en su uso, y si por alguna razón un agente externo la conoce tiende sobre todo a afectar negativamente procesos en áreas específicas.
Bajo(B)	Las fallas en los activos que afecten la disponibilidad de la información pueden ser aún más tolerables con una solución que se puede dar superior a una semana. No hay daño grave en la entidad para su funcionamiento ni con la información de sus clientes.	Errores que provocan pérdida de exactitud y completitud de los activos con una consecuencia negativa tolerable hacia la entidad en sí como de sus clientes. La brecha para corregir los errores tiende a ser un poco mayor al criterio Medio.	Los activos disponibles para todo tipo de personas ya sea funcionario de la entidad o agente externo que no tiene influencia negativa en el proceso de correspondencia de la organización.
Muy Bajo(MB)	El activo puede durar más de 2 semanas presentando fallos los cuales no influyen el funcionamiento de la correspondencia de la organización	Puede ser modificado en cualquier momento por Cualquier usuario sin influir el proceso de correspondencia de HECC COURRIER.	La información es accedida por cualquier usuario sin traer daños y perjuicios a la organización y su proceso de negocio.

Tabla 9. Criterios de Valoración
Fuente: Los Autores

A continuación, se muestra la tabla con el listado de activos, su tipo (referenciado en la Ilustración 5), una breve descripción y lo más importante la definición del criterio en cuanto a la confidencialidad, integridad y disponibilidad que tienen en la entidad, dado esto se efectúa una valoración para determinar su importancia en general.

Listado de Activos	Tipo	Descripción	Confidencialidad	Integridad	Disponibilidad	Valor del Activo
Dispositivos de Telecomunicaciones de internet	RC	Se identifican los router, switch y modem para brindar acceso a la red de la organización.	Alto	Alto	Alto	Alto
Servidores de Base de Datos y Servidor Proxy	H	Provee servicios a la red de la entidad para mejorar su	Alto	Muy Alto	Alto	Alto

		gestión.				
Listado de Activos	**Tipo**	**Descripción**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Valor del Activo**
Windows Server 2008	SO	Sistemas operativos para los servidores de Base de datos y Servidor Proxy	Alto	Muy Alto	Alto	Alto
Windows 7 y Xp	SO	Sistema operativo que se encuentra distribuidos en los equipos de la organización.	Bajo	Medio	Medio	Medio
Disco duro extraíble de 1 T	SI	Medio de almacenamiento de información como disco de respaldo	Alto	Alto	Bajo	Medio
Memorias USB	SI	Medio de almacenamiento portátil donde se copia información transferible al área de operaciones	Medio	Bajo	Bajo	Bajo
DVD de respaldo	SI	Backup de equipos de auxiliares de operaciones	Alto	Alto	Bajo	Medio
Ingeniero de Soporte y de sistemas	RH	Quienes están a cargo de brindar y configurar adecuadamente los servicios.	Alto	Medio	Alto	Alto
Coordinador y auxiliares	RH	Quienes se encargan de las operaciones del área de correspondencia.	Ato	Medio	Medio	Medio
Alta Gerencia	RH	Directores y Gerentes	Muy Alto	Alto	Alto	Alto
SIM(Sistema de Información de Mensajería)	SW	Sistema de Información Documental	Medio	Alto	Medio	Medio

Listado de Activos	Tipo	Descripción	Confidencialidad	Integridad	Disponibilidad	Valor del Activo
Bases de Datos basado en motor Microsoft SQL Server	I	Toda información de Usuarios, clientes.	Alto	Alto	Alto	Alto
Impresoras Lexmark, Hp, Xerox	H	Hardware	Alto	Medio	Medio	Medio
Edificio Bodega 25	E	Instalaciones donde se encuentra la organización	Medio	Bajo	Bajo	Medio
Interfaces Web	SW	Página web de la organización	Alto	Medio	Alto	Alto
Documentación	I	Información de nuevos dispositivos, sistemas y aplicaciones a utilizar.	Medio	Bajo	Bajo	Medio
Red Local	RC	Red de Área Local, interna de la empresa permite la interconexión de las computadoras internas así como el acceso a diferentes servicios.	Alto	Alto	Muy Alto	Alto
Clave Criptográfica	C	Clave para acceder a los archivos cifrados con pgp.	Alto	Alto	Alto	Alto
Servicio de transferencia de fichero SFTP	S	Servicio de trasferencia de archivos	Alto	Alto	Muy Alto	Alto
Información de clientes	I	Información de correspondencia	Muy Alto	Muy Alto	Alto	Muy Alto
World Office	SW	Aplicación de	Bajo	Bajo	Medio	Bajo

		Microsoft				
Listado de Activos	**Tipo**	**Descripción**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Valor del Activo**
Correo Electrónico	S	Correo electrónico interno de la organización	Alto	Medio	Medio	Medio

Tabla 10. Valoración de Activos
Fuente: Los Autores

3.2 IDENTIFICACIÓN Y VALORACIÓN DE VULNERABILIDADES

Una vulnerabilidad se define como la debilidad que se encuentra en los activos y que puede ser explotada por las amenazas existentes afectando. De acuerdo a esto es necesario definir unas escalas de probabilidad que ayudan a identificar el nivel en que se encuentran las vulnerabilidades detalladas después.

Probabilidad	**Descripción**	**Valor**	
Muy Frecuente	A diario	75-100%	Critico
Frecuente	Una vez al mes	50-75%	Alto
Frecuencia Normal	Una vez al año	25-50%	Medio
Poco Frecuente	Cada varios años	0-25%	Bajo

Tabla 11. Escalas de Probabilidad de Vulnerabilidades

Fuente: Medina Javier. Evaluación de vulnerabilidades. Laderas del Campillo, Murcia, Julio 2014. Editorial sg6.es.

Tras tener la anterior escala de probabilidad, se hace una identificación de las vulnerabilidades.

Vulnerabilidad	**Valoración**	**Impacto sobre Activos**
Falta de documentación y registro de los equipos de infraestructura.	Critico	Los equipos de infraestructura pertenecen al tipo de activo Hardware, Software y Sistemas Operativos, ya que con ellos se constituyen como base para el funcionamiento de los servicios que provee la empresa. Es clave destacar que las vulnerabilidades tienen una valoración crítica ya que el impacto que pueda ocurrir en ellos es alto, puede ocasionar que el proceso de correspondencia no se pueda realizar y todo el flujo de procesos se detenga hasta no poder solucionarlo.
Falta de documentación de la estructura de red.	Critico	Los soportes de información son un tipo de activos dentro de la empresa, si estos no se encuentran debidamente diligenciados no va a haber un respaldo en caso de incidentes para su solución rápida y oportuna. La vulnerabilidad identificada en este caso se refiere a la estructura de la red, que se maneja de la misma forma como un equipo de

		infraestructura, así que siendo algo critico implica un impacto alto que ocasiona no solo que el proceso de correspondencia se detenga si no que el área de sistemas no pueda realizar sus labores debidamente.
Falta de capacitación de los empleados en su cargo.	Critico	Los empleados entran en la categoría de Recursos Humanos, es probable que teniendo una inadecuada capacitación para ejercer sus labores estos conlleven a rendimiento pobres dentro de sus áreas respectivas, haciendo que los procesos no se realicen debidamente. Los empleados son un activo importante, son quienes realizan los procesos para que todo fluya, si no se realiza una capacitación adecuada, el rendimiento será bajo y la dirigencia se verá obligado a prescindir de ellos, ocurriendo problemas en tiempos, ya que se requerirá otro proceso de selección para reclutar nuevo personal.
No se tienen acuerdos de confidencialidad o No divulgación que guíen a los empleados en su conducta empresarial.	Critico	Así mismo como la anterior, se presenta una vulnerabilidad enfocada hacia el recurso humano. Esta va de la mano con la capacitación del personal para ejercer sus labores, pero enfocada en la ética profesional que debe tener cada persona. Esta vulnerabilidad es crítica y tiene un impacto grande en el empleado, ya que si este tiene actitudes inapropiadas y es descubierto tiene que ser removido de su cargo, requiriendo que otra persona del área se sobrecargue de labores mientras se consigue un reemplazo capacitado.
Falta de verificación de información en los procesos de selección de personal.	Alto	La persona encargada de Recursos humanos debe ejercer su labor de manera eficaz, ya que debe determinar quienes ingresan a trabajar en la empresa, conociendo todos sus aspectos tanto académicos como psicológicos para saber la aptitud de dicha persona para laborar en la empresa. Si hay fallas en el proceso y la persona no cumple con los requisitos establecidos debe ser removida de su cargo y sobrecargando laboralmente a alguien de su área, afectando la calidad dl trabajo en el área respectiva.
La ausencia de logs para ataques de intrusos y o errores humanos en el procesamiento de la información.	Critico	Al no haber registro de actividades de algún ataque o de errores del personal no se tiene presente de los problemas que se presentan. Esta ausencia afecta

		notablemente los servicios, sistemas operativos, información, redes de comunicaciones, claves criptográficas, ya que todo se puede corromper mientras se hace un trabajo interno sin darse cuenta de que ocurre.
Ausencia de un proceso claro para la respuesta de eventos de seguridad que comprometan la información.	Critico	Al no existir soportes de información que permitan tener un plan de respaldo ante incidentes es claro que se afecta todo el servicio, las redes de comunicación, hardware, software, claves criptográficas, sistemas operativos, etc. El impacto es a nivel general de todos los activos ya que no existe una respuesta ante eventualidades y se pierde tiempo mientras se busca la manera de corregirlo, de allí que afecte todo el flujo de los procesos.
Falta de Políticas de Seguridad de la empresa.	Critico	Esta vulnerabilidad afecta toda la empresa en general. Si no se tienen políticas de seguridad toda la información es vulnerable porque no hay lineamientos para su protección, toda la infraestructura, las redes, los sistemas, etc. va a estar indefenso de un plan de contingencia que se adoptar ante algún incidente o de algo que lo puedo prever y controlar desde antes.
Ausencia de un proceso disciplinario para quienes cometen violaciones en políticas de seguridad.	Alto	Si no se tiene una política no se va a tener algo que establezca el incumplimiento de estas, y de allí que los activos sean altamente vulnerables en cada uno de los procesos, ya que la persona que logre corromper el sistema, va a pasar impune y sin el debido castigo porque no hay como detallarle dicho proceso disciplinario.
Ausencia de software de monitoreo y control.	Alto	El software es uno de los activos más importantes de la empresa, ya que con él se basa el proceso de correspondencia para determinar su funcionamiento y sus procesos. Es clave que además de ello tenga la capacidad de poder monitorear y controlar las actividades que ocurran no solo en ese proceso sino también en el de las demás áreas. La información y los sistemas pueden sufrir de manera grave si no se tienen registros para efectuar auditorías internas.
Empleados que ingresan a trabajar para HECC COURRIER, y desconocen el manejo de la operación de correspondencia.	Alto	La información que maneja el proceso de correspondencia es demasiado sensible y debe ser manipulada con mucho cuidado para no afectarla o corromperla,

		de allí que se deba capacitar de la mejor manera a sus empleados que estén en dicha área. Si estos no tienen la capacidad necesaria para realizar su labor la información no fluirá de manera adecuada, haciendo que la información de los clientes no llegue a sus destinos de manera correcta con consecuencias legales y económicas para la empresa dejando de funcionar eficientemente.
Empleados con Profesiones, experiencia o datos personales alterados o falsos.	Alto	Personal nuevo con información falsa es un caso muy común de trabajo interno para extraer información o corromperla. Casi siempre ocurre de alguna persona que trabaja en competencia o de un hacker que trabaja por su cuenta. Es necesario que el proceso de selección sea estricto y se verifique toda la información posible para que no se tenga personal extraño en la empresa que perjudique los servicios y procesos de manera notable.
Ausencia de mecanismo para identificación real de asignación de los activos de software y hardware.	Alto	Los activos de software y hardware son parte fundamental en el funcionamiento de la empresa, y es deber prioritario que se tengan asignados el uso de ellos y la forma de manipulación de la información allí contenida. Si no se tiene esto cualquier usuario puede acceder a su uso sin limitaciones, algo que debe estar restringido de acuerdo a los roles en que se encuentre. Al presentarse fallas por manipulación equivocada no se tendrá responsable a cargo y la forma de solventar el incidente no tendrá alguien específico a cargo para solucionarlo.
Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información ej.: Servidores.	Alto	Los equipos de infraestructura como servidores y hardware deben estar protegidos y monitoreados siempre, ya que son la fuente de proveer físicamente que los servicios de la empresa efectúen sus procesos debidamente. No tener un monitoreo de ellos tiende a que en algún momento se presenten fallas y no se evidencie de inmediato que se deba realizar una solución establecida previamente. Dicho problema afecta notablemente los servicios de la empresa y los procesos internos en cada una de las áreas.
Falla en el envío de correspondencia por información errónea de destino.	Critico	La información del cliente es de tipo sensible, ya que se tiene en algunos casos envíos bancarios o de índole

		económico que se tiene que proteger y asegurar la llegada a su destino. Si se en algún momento se presenta una falla en el envío de acuerdo al destino, se tiene que identificar donde se produjo la pérdida y de inmediato hacer que retome su curso normal. La afectación y el impacto es bastante grave ya que el cliente confía plenamente en la empresa para su correspondencia, y si esto falla tiende a tener repercusiones legales y económicas que afecta al proceso de funcionamiento normal de la empresa.
Susceptibilidad a las variaciones de voltaje.	Medio	La electricidad en algún momento puede fallar, y los activos de la empresa como los equipos de infraestructura, de hardware e instalaciones tienden a afectarse de manera que no funcionen correctamente por las variaciones, en algunos casos con fallas irreparables y la información contenida allí tiende a perderse si no hay un respaldo adecuado.
Falla en la verificación de funcionamiento de los equipos en su configuración.	Alto	Los activos de hardware y equipos de infraestructura deben estar configurados de manera correcta para que funcionen de manera idónea. Si se tiene una configuración errónea y no se verifica que estos presenten fallas tienden a que algunos procesos no se realicen de la mejor manera y o funcionen a medias, afectando el flujo del envío de correspondencia o de procesos de cada área.
Fallo en controles de seguridad para medios de almacenamiento de información.	Critico	Los medios de almacenamiento tienden a ser activos como hardware y soportes de respaldo, capaces de contener información sensible tanto de la empresa como de los clientes, es por ello que no tener un control para su manipulación o acceso hace que sea vulnerable y tiende a tener un impacto alto por la misma información que maneja.
Ausencia de auditorías periódicas preestablecidas que garanticen el correcto manejo de la información.	Alto	Hay un impacto alto en la información como activo, ya que si no se ejecutan auditorias periódicas no se identificarán los problemas que se puedan encontrar y así mismo no hay un plan de corrección a tiempo. Dicha vulnerabilidad debe minimizarse por medio de políticas que permitan establecer dichas auditorias y se enfoque en el manejo de la información, ya que si esta no se trata de la manera correcta puede ser corrupta al

		momento del flujo de los procesos de la empresa.
Ausencia de personal Especialistas en cada área.	Alto	El recurso humano como activo importante de la empresa debe estar capacitado para ejercer sus labores. Si esto no se cumple se debe retirar al personal y realizar procesos que conlleven a una selección adecuada del reemplazo, esto conlleva perdidas monetarias y de tiempo así mismo los procesos se pueden retrasar por falta de personal capacitado en este caso de líderes y especialistas que propongan métodos estructurados en cada área.
Ausencia de procedimiento formal para el registro y retiro de usuarios.	Critico	Al no existir un procedimiento formal para registrar y retirar usuarios, cualquier persona que haya estado trabajando en la empresa puede ingresar a los sistemas y obtener información clasificada y sensible para un uso indebido si no existe la ética profesional al estar fuera de la empresa. Aquí la información esta vulnerable y su impacto será grande si se manipula, corrompe o se extrae.
Ausencia de mecanismos que permitan restricciones que limiten el tiempo de conexión en aplicaciones de alto riesgo.	Critico	Al no tener un impedimento de sesiones en las aplicaciones, puede ocurrir que algún empleado o agente externo ingrese a la sesión de algún compañero que no alcanzo a cerrar correctamente su sesión, con esto puede ingresar y extraer información si lo desea. Así esta persona estará impune ya que la sesión estaba establecida a algún compañero. Este ejemplo es muy común que se presente y debe ser resuelto para que se limite el tiempo de trabajo durante la aplicación.
Falencia en los controles de acceso de personal a áreas seguras.	Critico	Los controles de acceso realizan la labor de verificación para permitir que los usuarios tengan la opción de manipular la información de manera correcta. Si estos controles fallan la información es expuesta y cualquier persona pueda obtenerla, siendo demasiado grave si se determina que pueda ser un intruso haciendo labor interna para la extracción.
La aplicación no tiene una configuración de contraseñas seguras.	Critico	Si no existen contraseñas seguras es más fácil para los intrusos el acceso a los procesos y sistemas de información que maneja la empresa. Con esto se tiene un impacto demasiado alto en donde la información puede ser manipulada y extraída por dicho intruso, logrando que

		su activo más importante ya no les pertenezca y se atengan a las consecuencias que pueda realizar los clientes por la pérdida de su información sensible.
Los equipos de los empleados no tienen restricción de acceso a dispositivos de entrada DVD (R/W), USB, etc.	Critico	Los equipos de infraestructura, de redes, hardware como tal y hasta software pueden verse afectados notablemente si no se tiene un tratamiento adecuado ante el uso de dispositivos de entra como DVD o USB. Estos pueden ser usados en cualquier momento sin verificación de contener algún tipo de virus o software para extracción de información. Es altamente peligroso que no se tengan políticas para el uso de dichos dispositivos.
La información en algunos puntos de montaje no se encuentra cifrada y cualquier empleado con acceso puede verla.	Critico	Los empleados no tienen una restricción como tal a la información en puntos de montaje, pueden manipularla o identificarla, siendo esto una amenaza ya que algún empleado infiltrado pueda acceder a ella con fines extorsivos en algunos casos. La información que maneja la empresa es sensible porque es lo que el cliente requiere enviar bajo correspondencia, pero si esta se ve afectada toda la empresa puede dejar de funcionar si no se le responde al cliente por dicho envío.
No se tienen directrices de control de transferencia de información por herramientas seguras, la información se envía por cualquier método.	Alto	El flujo de información presente en el proceso de correspondencia no tiene unas directrices como tal para efectuar el envío de información, los canales aunque tratan de ser seguros con claves encriptadas pueden sufrir de ataques que corrompan la información, la extraigan y la divulgan, haciendo que la información de los clientes quede expuesta y sea catastrófico para la empresa por las demandas que se puedan presentar.
No se tienen políticas "buenas prácticas", políticas de escritorio limpio y de pantalla limpia.	Alto	El software y los sistemas operativos son altamente vulnerables y pueden sufrir un impacto alto si no se tienen políticas para bloquear su área de trabajo, en especial sus computadores cuando no se encuentran en él. Es claro que la información se puede corromper y que también los sistemas operativos pueden verse afectados con la manipulación de información, el ingreso a procesos no debidos y exposición de información

		sensible.
No se tienen planes de respaldo de información periódicos.	Alto	Dos aspectos importantes ante esta vulnerabilidad, el primero es la información, el cual es el activo vital de la empresa si no se tienen planes de respaldo puede que se vea afectada en algún momento y sin forma de recuperar lo perdido. Esto es grave para la empresa porque manejan información sensible del cliente y si no son capaces de responder tienden a tener repercusiones legales y económicas. Y lo otro es el soporte de información que esta vulnerable al no ser utilizado de la forma correcta para salvaguardar información.
Ausencia de políticas, procedimientos y controles formales para el control de acceso a páginas de internet.	Critico	Los activos como la información, los sistemas operativos, el software y hasta el mismo hardware pueden verse altamente afectados si no hay un lineamiento que controle el acceso a las paginas, donde se pueden obtener cualquier cantidad de virus afectando los activos ya nombrados afectando el funcionamiento de la empresa y sus procesos en cada área.
Ausencia de un documento para el etiquetado, manejo de la información, procesamiento, almacenamiento, transmisión, clasificación y destrucción de la información.	Critico	El impacto sobre cualquier activo de información de la empresa al no tener un documento que determine como manipular la información es demasiado alto, por eso la vulnerabilidad está en estado crítico. Aquí se busca que los soportes de información sean necesarios de realizar y de mejorar para que el riesgo disminuya y toda la información sea tratada de manera segura y confiable por cada área.
Ausencia de elementos para control de incendios y catástrofes naturales.	Alto	Las instalaciones son altamente afectadas ante esta vulnerabilidad identificada, cualquier amenaza de riesgos naturales y sin algún elemento de control capaz de colaborar a buscar medidas de seguridad permite que dicho activo sea afectado de manera notable sin defensa posible.

Tabla 12. Identificación y Valoración de Vulnerabilidades

Fuente: Los Autores.

3.3 IDENTIFICACIÓN DE AMENAZAS

Las amenazas son los eventos que ocurren sobre un activo que podría causarle daño a una organización. Se realizó un análisis de las posibles amenazas, que se

podrían llegar a materializar en la organización.

AMENAZA	TIPOS DE AMENAZA	TIPOS DE ACTIVOS
Los dispositivos de telecomunicaciones pueden ser robados ya que no se encuentran relacionados. No se cuenta con un registro o inventario almacenado en ninguna parte.	● Extorsión de información. ● Sabotaje o vandalismo. ● Robo. ● Compromisos con la propiedad intelectual ● Espionaje o intrusión	(RC) y (SW)
No tener la documentación de la línea base los dispositivos nuevos puede que no funcionen correctamente y se tenga una gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	● Error humano o falla. ● Fallas o errores técnicos de hardware. ● Fallas o errores técnicos de software. ● Espionaje o intrusión	(I) , (SI) y (H)
Empleados suministren información no autorizada sin tener que responder por ello.	• Error humano o falla. • Compromisos con la propiedad intelectual • Falta, inadecuada o incompleta	(RH) e (I)
Empleados con tendencias delictivas que ingresen a la organización.	● Falta, inadecuada o incompleta de los controles	(RH) e (I)
Empleados no cumplen con sus funciones adecuadamente y no hay forma de determinar dichas acciones al no encontrar registros que los comprometan.	• Compromisos con la propiedad intelectual • Falta, inadecuada o incompleta • Error humano o falla • Fallas o errores técnicos del software	(I) , (SW) y (H)
Incidentes de seguridad recurrentes con aumento en su nivel de impacto sin procesos ni directrices de control que lo solucionen de manera rápida y segura.	• Falta, inadecuada o incompleta de los controles	(I) y (SI)
Empleados que efectúan violaciones de seguridad y recurren en sus actos sin tener una forma de corrección de ello.	• Falta, inadecuada o incompleta de los controles • Compromisos con la propiedad intelectual	(I), (SW), (SI), (S) y (H)
Empleados nuevos que obstaculizan y retrasan los procesos de correspondencia al desconocer el manejo de envíos de la empresa.	• Error humano o falla. • Fallas o errores técnicos de hardware. • Fallas o errores técnicos de software.	(I) y (RH)

AMENAZA	• TIPOS DE AMENAZA	TIPOS DE ACTIVOS
Empleados con información alterado pueden corromper, alterar o robar información para fines propios o de la competencia.	• Robo. • Espionaje o intrusión • Sabotaje o vandalismo	(I) y (RH)
Al no haber asignación de los activos de software y hardware cualquier empleado puede extraer información para uso indebido.	• Robo. • Extorsión de información.	(I), (H), (SI) y (RC)
Errores persistentes en software para el envío de correspondencia sucediendo por la falta de monitoreo y controles detallados.	• Fallas o errores técnicos de software.	(SW) y (I)
Fallas en servidores y equipos de infraestructura que persisten al no haber monitoreo sobre ellos.	• Fallas o errores técnicos de software. • Errores de Configuración	(I) y (SO)
Monitoreo inadecuado de los canales de comunicaciones.	• Anticuadas u obsoletas tecnologías. • Espionaje o intrusión • Robo	(RC), (H) y (SW)
Sincronización de fechas erróneas de los sistemas.	• Fallas o errores de Software	(SW) y (SO)
Variaciones de voltaje causan problemas en el funcionamiento de los equipos.	• Error humano • Fallas o errores técnicos de Hardware.	(H) y (RC)
Configuración incorrecta de parámetros de configuración de equipos.	• Error humano o falla • Ataques de software • Espionaje o intrusión • Sabotaje o vandalismo. • Robo • Extorsión de información	(SW) y (SO)
Elección errónea de controles de seguridad para medios de almacenamiento de información, Ej. Copias de respaldo.	• Falta, inadecuada o incompleta de los controles • Compromisos con la propiedad intelectual	(SI) e (I)
Errores recurrentes en el manejo de información sin identificación de una solución pronta ya que no hay un encargado de auditoria interna que regule.	• Falta, inadecuada o incompleta de los controles • Compromisos con la propiedad intelectual	(I) y (SW)

AMENAZA	TIPOS DE AMENAZA	TIPOS DE ACTIVOS
Procesos no estructurados y elaborados de forma correcta al no tener especialistas en cada área que determine el camino correcto.	• Falta, inadecuada o incompleta de los controles • Error humano	(RH) e (I)
Accesos a personas no autorizadas.	• Falta, inadecuada o incompleta de los controles.	(SW) e (I)
Perfilación errada de los derechos de acceso de usuarios.	• Error humano	(RH) e (SW)
Modificación de perfiles de usuario por deficiencia en dicho proceso.	• Falta, inadecuada o incompleta de los controles. • Compromisos con la propiedad intelectual	(RH), (I) y (S)
Corrupción de información en el flujo del envío de correspondencia por deficiencia en restricciones.	• Falta, inadecuada o incompleta de los controles. • Fallas o errores técnicos de software.	(I) y (SW)
Personal no autorizado con acceso a áreas no establecidas.	• Falta, inadecuada o incompleta de los controles. • Espionaje o intrusión • Sabotaje o vandalismo. • Robo	(E), (S) e (I)
La aplicación permite la generación de contraseñas poco seguras.	• Fallas o errores técnicos de software.	(I), (C), (SO) y (SW)
Algunos empleados pueden sacar información confidencial de las instalaciones de HECC COURRIER para trabajar en equipos no seguros.	• Espionaje o intrusión • Sabotaje o vandalismo. • Robo	(I) y (H)
El uso de dispositivos de entrada en los equipos de cómputo de los empleados pueden corromper o extraer información de la empresa.	• Espionaje o intrusión • Sabotaje o vandalismo. • Robo	(SI)
Los empleados pueden acceder a información sensible de los puntos de montaje porque esta no se encuentra cifrada.	• Robo. • Compromisos con la propiedad intelectual • Espionaje o intrusión	(I) y (C)
Corrupción de información en la transferencia de información por canales no seguros.	• Falta, inadecuada o incompleta de los controles.	(I) y (SW)
Cualquier empleado puede acceder a cualquier tipo de información sin	• Falta, inadecuada o incompleta de los controles.	(I)

limitaciones.		
AMENAZA	**TIPOS DE AMENAZA**	**TIPOS DE ACTIVOS**
Extracción de información de cualquier tipo en los diferentes procesos existentes.	• Falta, inadecuada o incompleta de los controles.	(I)
Acceso sin restricción a cualquier página de internet.	• Falta, inadecuada o incompleta de los controles.	(I) y (SW)
Incendio y catástrofes naturales.	• Compromisos con la propiedad intelectual	(E)

Tabla 13. Listado de Amenazas
Fuente: Los Autores

4. ANÁLISIS DE RIESGOS

El análisis de riesgos es una de las bases en que se basa el presente trabajo, de aquí se determinan los aspectos por los cuales es importante y necesario efectuar unas políticas de seguridad e implementarlas de manera efectiva. Este análisis no solo se determina hacia unos riesgos identificados, sino que se realizan actividades como la identificación de vulnerabilidades y amenazas que puedan ocasionar inconvenientes en los procesos de la empresa. Teniendo en cuenta esto y realizando un análisis efectivo se logra llegar a las valoraciones de los riesgos de una manera más clara para poder tratarlos y controlarlos.

4.1 TABLA DE VALORACIÓN DE RIESGOS

Se ha determinado unas escalas de valoración de riesgos de acuerdo al conocimiento sobre el tema, algunos trabajos relacionados y asesorías de parte de los tutores y asesores del proyecto. De esto se identifica la siguiente ilustración y así mismo se hacen definiciones de cada escala en una tabla que se encuentra más adelante.

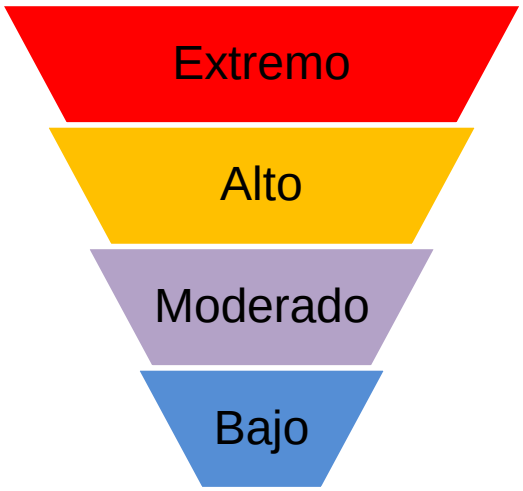


Ilustración 7. Tabla de Valoración de Riesgos
Fuente: Los Autores

VALORACIÓN	DEFINICIÓN	OPCIONES DE MANEJO	CALIFICACIÓN
Extremo	Implica tomar medidas que REDUZCAN EL IMPACTO de la materialización del riesgo, a través de la tercerización o transferencia, como en el caso de los seguros.	• Reducir el riesgo • Compartir o transferir • Eliminar el riesgo	13 a 25

Alto	Implica tomar medidas encaminadas a PREVENIR que el riesgo se materialice, evitar la materialización del riesgo es la primera alternativa a considerar, y esto se logra cuando al interior del proceso se generan cambios sustanciales. Estos controles y sus acciones, están orientadas a disminuir o evitar la materialización del riesgo y evitar el impacto de la materialización del riesgo. Lo anterior con el propósito de llevar el riesgo a zona moderada.	• Reducir el riesgo • Compartir o transferir	8 a 12
Moderado	Implica tomar medidas encaminadas a DISMINUIR la PROBABILIDAD (medidas de prevención), y el IMPACTO (medidas de protección). Se implementan controles preventivos y sus acciones de manejo se orientan a disminuir la probabilidad de materialización del riesgo, se busca llevar los riesgos en esta categoría a zona baja.	• Reducir el riesgo	4 a 7
Bajo	Implica que se ACEPTAN las consecuencias o efectos de la materialización del riesgo; en este caso no es necesario tomar medidas para seguir disminuyendo la probabilidad e impacto del riesgo.	• Aceptar el riesgo	1 a 3

Tabla 14. Descripción Valoración de Riesgos
Fuente: Los Autores

4.2 TABLA DE PROBABILIDAD

La tabla de probabilidad determina las escalas de ocurrencia de eventos. De acuerdo a algunos proyectos relacionados y a la asesoría de los tutores, se ha determinado una serie de escalas con su respectiva descripción y calificación.

PROBABILIDAD	DESCRIPCIÓN	CALIFICACIÓN
Raro o Remoto	Es muy remoto que el evento ocurra casi no pasa. No se espera que se materialice el riesgo, aunque es concebible. (1 vez cada 20 años)	**1**
Improbable	Es inusual que el evento ocurra. Es posible que suceda el daño alguna vez. (1 vez cada 10 años)	**2**
Posible	Es posible que el evento ocurra (1 vez cada 5 años)	**3**

Probable	Es posible que el evento que ocurra. La materialización del riesgo es posible que suceda varias veces en el ciclo de trabajo de la organización. (1 vez cada año)	**4**
Casi seguro	Normalmente es seguro que se materialice el riesgo ocurre con una alta frecuencia. (más de una vez por año)	**5**

Tabla 15. Tabla de Probabilidad
Fuente: Los Autores

4.3 VALORACIÓN DE IMPACTO

El impacto determina las consecuencias o efectos a procesos y activos de la empresa. Se han determinado una serie de escalas para clasificar dicho impacto, con su respectiva descripción, ejemplo y calificación cuantitativa.

IMPACTO	DESCRIPCION	CALIFICACIÓN
Insignificante	Si el hecho se presenta, las consecuencias o efectos son imperceptibles sobre el proceso o la organización, dado en que no se ve afectada la prestación del servicio. **Por ejemplo:** Daño de la impresora. Falta de insumos de papelería.	**1**
Menor	Si el hecho se presenta, hay un impacto o efecto sobre el proceso o la organización, pero solucionable con prontitud. **Por ejemplo:** Ausentismo de personal. Daño de un equipo portátil.	**2**
Moderado	Si el hecho se presenta, las consecuencias o efectos sobre el proceso o la organización son perceptibles, afectando los tiempos de operación y requieren un esfuerzo (recursos) para solucionarlo. **Por ejemplo:** Falla en la conexión a las carpetas compartidas. Falla del servicio de mensajería. Fallas de internet menores a 4 horas (esporádico)	**3**
Mayor	Si el hecho se presenta, las consecuencias o efectos sobre el proceso o la organización, implicarían perdida de tiempos de operación o incluso impedimentos para prestar el	**4**

	servicio (tiempo sin servicio perceptible por el cliente). **Por ejemplo:** Renuncia o ausentismo masivo de personal Fallas continuas en el servicio de internet. Falta continua de correo electrónico.	
Catastrófico	Si el hecho se presenta, las consecuencias o efectos sobre el proceso o la organización impiden la prestación del servicio (El proceso o la organización no pueden continuar prestando el servicio). **Por ejemplo:** Falla prolongada de energía eléctrica Falta de conexión con los servidores.	**5**

Tabla 16. Valoración de Impacto
Fuente: Los Autores

4.4 IDENTIFICACIÓN DE RIESGOS

El primer paso dentro de la metodología es la identificación de las amenazas y vulnerabilidades, para ello, se deberá escoger aquellos activos de información que fueron considerados los más importantes en la identificación y valoración de activos y se evaluará a que amenazas y vulnerabilidades se encuentran expuestas. Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. A continuación, se identificaron los riesgos determinados a partir de las amenazas previamente encontradas, con ello se puede determinar su impacto y la probabilidad de ocurrencia.

No	CLASIFICACIÓN DEL RIESGO		RIESGO
1	Riesgos de Fraude o Corrupción.	Interno y Externo	Uso fraudulento de los aplicativos o herramientas de transferencia de información.
		Interno	Alteración de la información del área de operaciones
		Interno	Hurto o desviación de información privilegiada por ejemplo información del cliente.
		Interno y Externo	Fraude en procesos contractuales, manejo de servicios, robo de dinero, etc.
		Interno y Externo	Manejos ilícitos, fraudulentos y delictivos, de los datos en la aplicación.
		Interno	Robo de equipos que no se encuentran en inventarios por falta de identificación de los equipos informáticos que sirven para el tratamiento de información.
2	Riesgos con el recurso humano.	Interno	Desconocimiento de los Acuerdos de nivel de servicios establecidos.
		Interno	Quejas e insatisfacción de los clientes.
		Interno	Desequilibrio en la carga laboral por cargo o por empleados departamentales.
		Interno	Empleados con problemas judiciales.

		Interno	Incumplimiento de las normas de seguridad social y salud en el trabajo.
		Interno	Conocimiento centralizado
		Interno	Contratación de personal no apto para los cargos.
		Interno	Condiciones laborales riesgosas, que generen enfermedades profesionales o accidentes.
		Interno	Desactualización en los conocimiento requeridos para ejecutar el cargo
		Interno	No tener al personal requerido por incapacidades
		Interno	Desconocimiento de los estándares y controles de seguridad de la información
3	Riesgos Operativos y de procesos	Interno	Fallas en el flujo e interrelación de los procesos.
		Interno	Documentación obsoleta.
		Interno	Incumplimiento de estándares empresariales.
		Interno	Servicio rechazado. Por incumplimiento del mismo.
		Interno	No se tiene un método prudente para el registro y retiro de usuarios
		Interno	No se tiene procedimiento formal para el registro y retiro de usuarios
		Interno	Procesos y actividades no documentadas, generando dependencia de personas.
		Interno	Métodos de trabajo y prácticas obsoletas o no efectivas.
4	Riesgo de contratación externa	Interno / Externo	Selección de proveedores o clientes vinculados a la lista Clinton.
		Externo	Incumplimiento de los proveedores
		Interno	Selección de productos o servicios que no correspondan con los requerimientos de negocio
		Externo	Incumplimiento de los proveedores
		Interno / Externo	Falla en la recepción se productos o servicios contratados.
5	Riesgos Tecnológicos y de Infraestructura	Interno	Fallas en la disponibilidad y funcionalidad del Software.
		Interno	Fallas en redes y comunicaciones.
		Interno	Uso de equipos obsoletos o con sistemas no soportados.
		Interno	Generación o recepción de virus.
		Interno	Fallas en la disponibilidad y funcionalidad del Hardware.
		Interno	Ataques de intrusión, hackers, el colapso de las telecomunicaciones o actividades que pueden originar el deterioro de la información o la interrupción del suspensión.
		Interno	Disponibilidad del sistema eléctrico
		Interno	Cambios tecnológicos no planificados que genere que la empresa no se encuentre preparada para adoptar las nuevas tecnologías.
		Interno	Infraestructura insuficiente (puestos de trabajo y capacidad de las instalaciones)
		Externo	Falta de la otra parte en un negocio y la incapacidad de reclamar jurídicamente el desempeño de los acuerdos adquiridos.
		Interno	Descoordinación de las fechas de los equipos de cómputo y servidores
		Interno	Demoras en el proceso de compra de equipos y recursos tecnológicos

6	Riesgos de Información	Interno / Externo	Información alterada
		Interno	Eventos o situaciones que generan perdida de información por uso y manejo inadecuado.
		Interno	Uso de canales ineficientes e inadecuados de comunicación que pueda distorsionar la información
		Interno	Utilización de información "confidencial" de la empresa para beneficio personal o de terceros.
		Interno	No se tienen planes de respaldo de información periódicos.
		Interno / Externo	Falla en la disponibilidad de la información.
7	Riesgos externos, (de entorno)	Interno / Externo	Seguridad Física del personal: secuestro, asesinato y accidentes.
		Interno	Incendio en el edificio donde se encuentra ubicado HECC COURRIER
		Interno	Generación de corto circuito, explosión física, o daños.
		Externo	Riesgo de fuego en oficinas paralelas.
8	Riesgos Naturales, ambientales y antrópicos	Externo	Riesgos meteorológicos e hidrológicos como: Lluvias intensas, granizo, tormentas, Inundaciones, Olas de frío.
		Externo	Desconocimiento de las actividades a ejecutar por los empleados ante una emergencia.
		Externo	Riesgo de fenómenos sísmicos
		Externo	Riesgo de Rayos
		Externo	Riesgo fenómenos climáticos y meteorológicos.
		Externo	Riesgos geológicos como: Vulcanismo, Terremotos, Tsunamis-maremotos, Deslizamiento de laderas.
9	Riesgos legales o regulatorios	Externo	Incumplimiento de requisitos legales
		Externo	Multas y demandas
		Externo	Pérdidas económicas por pérdida o alteración de información.
10	Riesgos de Acceso	Interno	Acceso no autorizado a equipos de operaciones
		Interno	Acceso no autorizado al área de correspondencia
		Interno	No tener registro de las acciones realizadas el sistema de correspondencia de HECC COURRIER
		Interno	No tener un nivel de acceso con protección de contraseña a información critica
11	Riesgos Estratégicos	Interno	Disminución de la demanda del servicio de correspondencia.
		Interno	Fallas en la estimación y proyección de recursos para los proyectos o para la función del proceso.
		Interno	Dificultad para detectar, aprovechar y reconocer las capacidades de cada empleado
		Interno	Fallas en la estimación y proyección de recursos para los proyectos o para la función del proceso.
		Interno	Incumplimiento en la gestión de su personal a cargo.
		Interno	Fallas de Planeación y comunicación de objetivos, metas y prioridades
		Interno	Insatisfacción del cliente
		Interno	Detrimento de la imagen o reputación de HECC COURRIER
		Interno	Disminución de la demanda del servicio de

			correspondencia.
		Interno	Dificultad para detectar, aprovechar y reconocer las capacidades de cada empleado
		Interno	Detrimento de la imagen o reputación de HECC COURRIER
		Interno	Debilidades en competencia de liderazgo y generación de resultados.

Tabla 17. Identificación de Riesgos
Fuente: Los Autores

4.5 EVALUACIÓN DE RIESGOS

En la evaluación de los riesgos es necesario determinar la valoración que van a tener dependiendo de su impacto en los procesos de la empresa, la probabilidad de que puedan ocurrir. En la siguiente tabla se muestran los riesgos identificados y se obtiene una valoración efectuando una multiplicación de acuerdo al impacto y probabilidad con el fin de obtener cuantitativamente un resultado para poder determinar cuáles son los riesgos que tienen prioridad en el tratamiento de acuerdo a los controles a implementar.

RIESGOS	IMPACTO	PROBABILIDAD	VALORACION
R1	**4(Mayor)**	**4(Probable)**	**16(Extremo)**
R2	**4(Mayor)**	**2(Improbable)**	**8(Alto)**
R3	**3(Moderado)**	**2(Improbable)**	**6(Moderado)**
R4	**2(Menor)**	**3(Posible)**	**6(Moderado)**
R5	**3(Moderado)**	**5(Casi Seguro)**	**15(Extremo)**
R6	**5(Catastrófico)**	**2(Improbable)**	**10(Moderado)**
R7	**2(Menor)**	**1(Raro o Remoto)**	**2(Bajo)**
R8	**5(Catastrófico)**	**1(Raro o Remoto)**	**5(Moderado)**
R9	**4(Mayor)**	**1(Raro o Remoto)**	**4(Moderado)**
R10	**3(Moderado)**	**4(Probable)**	**12(Alto)**
R11	**3(Moderado)**	**3(Posible)**	**9(Alto)**

Tabla 18. Escalas de Impacto y Probabilidad
Fuente: Los Autores

A continuación, se muestra el mapa de calor correspondiente donde se posicionan los riesgos dependiendo de su valoración de impacto y probabilidad:

PROBABILIDAD	Valor	IMPACTO				
		Insignificante	Menor	Moderado	Mayor	Catastrofico
		1	2	3	4	5
Raro o Remoto	1		R7		R9	R8
Improbable	2			R3	R2	R6
Posible	3		R4	R11		
Probable	4			R10	R1	
Casi Seguro	5			R5		

Tabla 19. Mapa de Calor de Riesgos
Fuente: Los Autores

4.6 DOMINIOS, OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD

La norma ISO/IEC 27001 determina que hay unos criterios de cumplimiento para que se efectúen cambios de mejora continua para un Sistema de Gestión de Seguridad de la Información. Con esto se debe realizar un análisis para que el tratamiento de los riesgos se efectúe correctamente y es allí cuando se toma el anexo A de la norma, que muestra los dominios, objetivos de control y los controles de seguridad, con el fin de que esto sirva de base para efectuar unas políticas de seguridad adecuadas y pertinentes para que la empresa HECC COURRIER tome en cuenta y se implemente en el futuro cercano.

Teniendo en cuenta el anexo A, el enfoque que este trabajo toma son los numerales 5 al 18 que corresponden a los dominios y sus controles los cuales serán analizados con lo que hay en actualidad y lo que debe implementarse en caso de ser necesario. A continuación, se muestra una tabla describiendo cada uno de los controles existentes de acuerdo al dominio y objetivos correspondientes.

CONTROL ID	CONTROL	APLICABLE	ANÁLISIS
A.5	POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN		
A.5.1	Orientación de la dirección para la gestión de la seguridad de la información. **Objetivo:** Brindar orientación y soporte por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.		
A.5.1.1	Políticas para la seguridad de la información.	SI	Actualmente la empresa no posee políticas de seguridad establecidas, no se ha desarrollado un documento que al menos estipule requerimientos mínimos de seguridad y por tanto se desconoce la realización de un SGSI. La norma ISO 27001 determina obligatoriamente que se efectúen políticas de seguridad, es necesario que haya documentos aprobados por la dirección con el cual se soporte el enfoque de la organización y los objetivos de seguridad gestionados correctamente. Estas políticas deben estar soportadas por temas, en este caso lo determinan los tipos de riesgos y los mismos riesgos que se han determinado en el análisis respectivo, con el cual se pueden tener organizados adecuadamente para una implementación lineal y segura. Este documento debe ponerse a disposición de todos los empleados de la empresa para que en su labor diaria se tengan en cuenta todas las observaciones y desarrollen su labor minimizando los riesgos que se puedan presentar. **Solución:** En general se determina con la creación de las políticas de seguridad.
A.5.1.2	Revisión de las políticas para seguridad de la información.	SI	Al no tener en la empresa una serie de políticas de seguridad, se identifica que este control no se ha aplicado actualmente. Al cumplirse el control A.5.1.1 se determina la revisión de dichas políticas en un intervalo determinado por el director de operaciones, ya que no hay un jefe o director de seguridad de la información se le ha dado el poder a este rol con el aval de la alta gerencia quien también debe estar pendiente de dicho proceso. Así mismo se propone que los líderes de las diferentes áreas estén al tanto de estos cambios y reuniones para analizar y revisar lo concerniente a la seguridad de la información de la empresa. Cada reunión debe documentarse para tener registro de lo que se determinó y para las reuniones futuras revisar si se ha cumplido o

			debe reforzarse.
			Solución: En general se determina con la creación de las políticas de seguridad.
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.		
A.6.1	Organización Interna. **Objetivo:** Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.		
A.6.1.1	Roles y responsabilidades para la seguridad de la información.	SI	La empresa al no tener implementado un SGSI ni al tener unas políticas de seguridad definidas no tiene roles ni responsabilidades para el tratamiento de la información y lo más importante la seguridad que esto conlleva. La seguridad de la información es vital, los activos son lo más valioso que tiene la empresa, y por ende debe haber roles que protejan esto. Determinar roles de seguridad en las áreas de la empresa es obligatorio y lo determina la norma ISO 27001, con lo cual cada cargo debe tener a su cargo algo en específico por lo qué responder para que los procesos de seguridad fluyan de manera adecuada.
			Solución: Política de Seguridad de los Recursos Humanos (Ver Anexo A Numeral 1.2.1)
A.6.1.2	Separación de deberes.	SI	Actualmente hay una separación de deberes en la empresa, cada área tiene sus responsables, los cargos que se encuentran tienen sus responsabilidades y realizan las labores sin afectar las demás. A veces por cambios en el personal, mientras se encuentran reemplazos y se hacen procesos de selección, algunos cargos deben efectuar labores que no les corresponde, eso sí teniendo algo de afinidad en el área en que se encuentra y por la que adicionalmente debe realizar. A pesar de que en algunos momentos haya empleados que deban cumplir otras funciones temporales, sus roles seguirán siendo los mismos en la organización, ya que el acceso a la información debe ser determinado por sus superiores quienes les otorgan el acceso respectivo con niveles de seguridad dados en los procesos del envío de correspondencia.
			Solución: Política de Seguridad de los Recursos Humanos (Ver Anexo A Numeral 1.2.1)

A.6.1.3	Contacto con las autoridades.	SI	La empresa en sus procesos de seguridad que son limitados, trata de resolverlos internamente. No hay un contacto con una autoridad o entidad encargada de vigilar dichos procesos. Es necesario tener contactos con autoridades, veedores, o algún ente que pueda verificar que los procesos se están desarrollando debidamente. A veces el manejo interno de las situaciones tiende a omitir acciones que incurren en problemas de seguridad que afectan el flujo de trabajo de la organización, tal es el caso del proceso de envío de correspondencia, donde algún incidente en el manejo y envío de la información tiende a afectar por completo si no se verifica donde hubo quebrantos en su proceso. Los líderes operativos y de sistemas deben estar pendientes del proceso para mantener una comunicación con las autoridades, los cuales pueden asesorarlos y definirles rutas de salida claras para cualquier incidente que se presente en los procesos de envío de correspondencia.
			Solución: Política de Seguridad de los Recursos Humanos (Ver Anexo A Numeral 1.2.1)

A.6.1.4	Contacto con grupos de interés especial.	NO	La empresa actualmente no tiene contacto con grupos de interés para definir temas de seguridad en la empresa. Así como no tiene comunicación con autoridades pertinentes tampoco ha tenido la necesidad hoy en día de comunicarse con grupos especiales y dialogar sobre dicho tema, ya que no ha visto que el flujo en el proceso de envío de correspondencia se vea afectado, o si lo encuentra lo trata internamente. No es algo obligatorio tener grupos de interés especial para tratar los temas de seguridad, puede ser considerado como algo adicional que puede mejorar y lo puede asesorar de manera más clara y efectiva. Estos grupos no solo se limitan al tema de seguridad si no a los procesos que se llevan en la empresa, ya sea en temas tecnológicos, administrativos o financieros. Como en el caso del contacto con las autoridades, los líderes operativos y de sistemas son los que más deberían estar pendientes en la organización para comunicarse con estos grupos de interés especial, ya que teniendo en cuenta los procesos que desarrollan y la información que se maneja pueden tomar una importancia mayor para que sean resueltas dudas y su implementación sea rápida efectiva con cualquier tipo de incidencia.
A.6.1.5	Seguridad de la información en la gestión de proyectos.	SI	A pesar de no tener claro un enfoque de seguridad en los procesos que se realizan en la empresa, las diferentes áreas entienden que la seguridad es importante, es algo que no está planificado pero que se desarrolla. En los procesos de envío de correspondencia es claro que hay niveles de seguridad que deben ser implementados, pero no hay una estructura plasmada como tal y por la cual se debe regir, es sobre la marcha y el desarrollo de los procesos en que se va ejecutando, ya sea por medio de firewalls, claves criptográficas, etc. Elementos que son necesarios pero que no se detallan tanto en los procesos cuando se hace una gestión de los proyectos. Es claro que desde el comienzo del proyecto de debe determinar la seguridad que tiene que implementarse, a pesar de que sea obvio lo que se realice, es necesario tenerlo en cuenta y detallarlo en todos los documentos de gestión de dichos proyectos y procesos que se van a

			ejecutar, así cualquier persona que ingrese a la organización sabrá estructuralmente como está diseñado y organizado un proyecto en el tema de seguridad de la información. Es labor de los jefes operativos y de sistemas velar porque esto se defina de manera entendible y detallada desde un comienzo.
			Solución: Política de Continuidad en las Operaciones (Ver Anexo A Numeral 1.2.2)
A.6.2	Dispositivos móviles y teletrabajo. **Objetivo:** Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.		
A.6.2.1	Políticas para dispositivos móviles.	SI	Actualmente no hay restricciones ni políticas para el uso de dispositivos móviles en la empresa. Los empleados en su labor diaria tienen dispositivos móviles suministrados por la empresa para uso netamente laboral, aunque no se tenga por escrito esto. El uso de dispositivos móviles en el mundo actual es una necesidad no solo en su parte personal si no ya en forma de trabajar. La conexión a internet como al uso de planes de voz deben ser exclusivos para sus ejercicios laborales, este debe estar restringido y vigilado por los ingenieros y jefes operativos y de sistemas.
			Solución: Política de Gestión de Activos (Ver Anexo A Numeral 1.2.3)
A.6.2.2	Teletrabajo.	NO	No se implementa el teletrabajo en la empresa. Tampoco es necesario efectuar una política al no tener pensado que se pueda realizar alguna actividad por fuera de la organización.
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS		
A.7.1	Antes de asumir el empleo **Objetivo**: Asegurar que los empleados y contratistas comprenden las responsabilidades y son idóneos en los roles para que los consideran.		
A.7.1.1	Selección	SI	Para un buen proceso de selección se debe solicitar referencias personales y profesionales al prospecto o candidato. Revisión y verificación de antecedentes (hoja de vida, experiencia laboral adecuada para el cargo o función que realizara, experiencia crediticia y antecedentes penales). Se tiene que separar y catalogar que información va estar libre para estos tanto para los funcionarios como para terceros. La información sobre todos los prospectos que es considerada para vacantes dentro de la organización, se debería

			recolectar y manejar apropiadamente de acuerdo con la legislación existente. Dependiendo de la legislación aplicable, se debería informar de antemano a los prospectos acerca de las actividades de selección.
			Solución: Política de Seguridad de los Recursos Humanos (Ver Anexo A Numeral 1.2.1)
A.7.1.2	Términos y condiciones del empleo	SI	Tanto para colaboradores como para los contratistas estos tienen que conocer los términos y los requisitos del convenio profesional tener presente las responsabilidades y compromisos frente al tratamiento de información confidencial y no revelación de esta. (El contrato tiene que abarcar, derechos, deberes, responsabilidades, estar de acuerdo a la ley y posibles sanciones por falta). En los contratos se debe estipular la confidencialidad y la integridad del manejo de la información recibida de otras organizaciones o agentes externos. También se debe explicar las medidas a tomar por la organización por si el empleado o contratista no tiene en cuenta los mínimos requisitos de seguridad. Se puede realizar un código de ética donde se tenga claro que, para futuros empleado, empleados y contratistas se establezcan las debidas responsabilidades de seguridad de la información que de acuerdo a su cargo se debe tener en cuenta la protección de datos y el buen uso de los activos de la organización. Para los candidatos referidos al área de mensajería se deberá tener adicional un acuerdo de información confidencial de los clientes.
			Solución: 6.12 Código de ética y conducta de HECC COURRIER (Ver Anexo B Numeral 1.12).
A.7.2	Durante la ejecución del empleo **Objetivo:** Asegurarse de los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.		
A.7.2.1	Responsabilidades de la dirección	SI	La alta gerencia deberá definir políticas y procedimientos donde los empleados y contratistas estén informados del cargo que están desempeñando y responsabilidades de la seguridad de la información, antes de entregar acceso a información confidencial. Se debe dar motivación a empleados y contratistas ya que esto tiende a ser más

			confiable e íntegro y causa menos incidentes de seguridad. La desmotivación del personal puede llevar a que no se usen adecuadamente los activos de la organización y en resultado la organización tenga riesgos altos.
			Solución: Política de Seguridad de los Recursos Humanos (Ver Anexo A Numeral 1.2.1)
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	SI	Se debe tener un procedimiento que esté acorde a las políticas de la seguridad de la información donde se establezcan regulares capacitaciones, foros, reuniones que concienticen al personal de la seguridad de la información y de la importancia que esta tiene, se deben también realizar campañas para la confidencialidad e integridad de los activos de la organización. Todas estas actividades del programa de toma de conciencia, se deberían programar en un periodo cada 3 meses, de preferencia con regularidad, de manera que las actividades se repitan y abarquen a nuevos empleados y contratistas. Toda esta formación de conciencia también se debería actualizar regularmente, de manera que permanezca en línea con las políticas y procedimientos organizacionales, y se debería construir con base en las lecciones aprendidas de incidentes de seguridad de la información. Las campañas de concientización se deben considerar diferentes formas de educación y formación, por ejemplo, conferencias o estudio por cuenta propia.
			Solución: Política de Seguridad de los Recursos Humanos (Ver Anexo A Numeral 1.2.1)
A.7.2.3	Proceso disciplinario	SI	En lo concerniente los colaboradores y contratistas partes que incumplan las políticas de seguridad se dirigirá a cabo un procedimiento disciplinario de acuerdo a los estatutos de la organización. Se debe tener una verificación del mal manejo si se tiene de la información.
			Solución: Política de Seguridad de los Recursos Humanos (Ver Anexo A Numeral 1.2.1)
A.7.3	Terminación y cambio de empleo **Objetivo:** Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.		
A.7.3.1	Terminación o cambio de responsabilidades de empleo	SI	Hecc Courrier realiza de un método conveniente el fin del contrato o cambio de contrato y una vez completo el contrato se

			deberá verificar que los equipos entregados para desempeñar funciones se encuentran en correcto estado. El cambio de cargo deberá tener cambios de responsabilidad o de empleador, se deberían manejar como la terminación de la responsabilidad o contrato actual, combinada con el inicio de una nueva responsabilidad o contrato. Se debe informar los cambios de cargo a todo el personal para que se mantenga informado las disposiciones operativas. Se debe tener una descripción de políticas de aplicación de privilegios sobre la información.
			Solución: Política de Control de Accesos (Ver Anexo A Numeral 1.2.4)
A.8	GESTIÓN DE ACTIVOS		
A.8.1	Responsabilidad por los activos **Objetivo:** Identificar los activos organizacionales y definir las responsabilidades apropiadas.		
A.8.1.1	Inventario de activos	SI	Es importante identificar los activos de acuerdo a su grado de importancia dentro de la organización, en la deja claro que cada activo se encuentra ubicado y nivel de importancia de cada área de la empresa. Este inventario de activos se debe actualizar mensualmente y tener un sistema claro de identificación como un código de barras el cual. Para los activos se debe tener un proceso de recepción, almacenamiento, trasmisión y eliminación como mejor convenga para HECC COURRIER.
			Solución: Formato de Inventario de activos (Ver Anexo B Numeral 1.1) y Política de Gestión de Activos (Ver Anexo A Numeral 1.2.3).
A.8.1.2	Propiedad de los activos	SI	Todo activo en el inventario deberá tener un responsable o propietario que se haga cargo de su seguridad. Cada responsable sobre su activo deberá asegurarse que el activo este inventariado y clasificado. Y deberá firmar un acuerdo de responsabilidad que la organización está haciendo entrega del activo y es su responsabilidad de seguir los lineamientos de seguridad y control de acceso.
			Solución: Formato de Inventario de activos (Ver Anexo B Numeral 1.1) y Política de Gestión de Activos (Ver Anexo A Numeral 1.2.3).
A.8.1.3	Uso aceptable de los activos	SI	Se debe tener un criterio aceptable del uso adecuado de los activos, se deben definir buenas prácticas para el buen uso del activo. Los empleados o contratistas relacionados con activos deberán ser responsables del uso que hacen de cualquier recurso de procesamiento

			de la información, y de cualquier uso ejecutado bajo su obligación. No se permite el uso de activos externos a la organización. **Solución:** Política de Gestión de Activos (Ver Anexo A Numeral 1.2.3).
A.8.1.4	Devolución de activos	SI	Al termino del contrato o cambio de cargo o de funciones se deberá formalizar la reposición de todos los activos físicos y electrónicos entregados previamente, que son propiedad de la organización o que se le han confiado a los empleados o contratistas según sea el caso. **Solución:** Política de Gestión de Activos (Ver Anexo A Numeral 1.2.3).
A.8.2	Clasificación de la información **Objetivo:** Asegurar que la información recibe un nivel apropiado de protección, de acuerdo a su importancia para la organización.		
A.8.2.1	Clasificación de la información	SI	La información debe ser clasificada, en sugerencia se da la siguiente clasificación que indicar el valor de los activos dependiendo de su sensibilidad y criticidad para la organización, por ejemplo, en términos de confidencialidad, integridad y disponibilidad: • Confidencial o Privada: Este tipo de Información involucra al cliente o titular de la cuenta, ya que la información que se maneja puede afectar la intimidad o recursos que tiene. La información manejada de correspondencia será confidencial o privada. Esto mismo afecta a los administradores de las plataformas quienes en su acceso deben tener una seguridad para el ingreso. En algunos casos esto se presenta para darle seguridad a áreas que no tienen permisos para ingresar a otras o el uso de sus sistemas, de allí que también se integren en este tipo, aunque estén laborando dentro de la misma entidad. • Estratégica o de Uso Interno: La información de los trabajadores quienes deben suministrar esta para efectuar sus labores de manipulación y configuración de sistemas y aplicaciones dentro de la entidad. Todo queda constatado en la documentación realizada para el manejo de información en los diferentes casos y procesos, así como también los estándares a trabajar y las políticas, procedimientos que se usan de manera interna. • Pública: Es aquella información que

			HECC COURRIER tiene a su cargo y que puede publicar sin afectar a los miembros de la empresa ni a los clientes. También la información que se muestre en las plataformas sin necesidad de un login o acceso está dentro de este tipo de información ya que solo se presenta de manera informativa.
			Solución: Política de Gestión de Activos (Ver Anexo A Numeral 1.2.3) y Metodología para el manejo de información (Ver Anexo B Numeral 1.3).
A.8.2.2	Etiquetado de la información	SI	Las etiquetas se deberían poder reconocer fácilmente. Los procedimientos deberían brindar orientación acerca de dónde y cómo se colocan las etiquetas, teniendo en cuenta que la forma en que obtiene el acceso a la información o se manejan los activos, depende de los tipos de medio.
			Solución: Metodología para el manejo de información (Ver Anexo B Numeral 1.3).
A.8.2.3	Manejo de activos	NO	Se debería tener un procedimiento para el manejo de activo pero ya que no se tiene una clasificación clara de la información y del acceso a esta no se debe declarar un procedimiento sobre la manipulación de esta hasta que no se realice el A.8.2.1
A.8.3	Manejo de medios **Objetivo:** Evitar la divulgación, modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.		
A.8.3.1	Gestión de medios removibles	SI	Se deberá tener un procedimiento de medios o manejo de medios removibles para que no se puedan recuperar este procedimiento deberá contar con autorizaciones de los responsables para que sean retirados de las organizaciones y posteriormente destruidos. Para los medios necesarios se debe tener una confidencialidad e integridad de la información donde se use niveles de protección a ataques informáticos.
			Solución: Política para el Uso de Medios Removibles (Ver Anexo A Numeral 1.2.5).
A.8.3.2	Disposición de los medios	SI	Se deberá tener una ubicación segura, deberá contar con procedimientos donde sea detectado los elementos que podrían requerir este aseguramiento. Los medios con información confidencial se deberán almacenar en la ubicación segura y luego mediante algún método de destrucción se deberá ejecutar borrado de la información.

			Solución: Política para el Uso de Medios Removibles (Ver Anexo A Numeral 1.2.5).
A.8.3.3	Transferencia de medios físicos	NO	Ya que HECC COURRIER es una organización de mensajería se adoptaran medidas de seguridad para que en sus bodegas se mantenga los medios controlados por controles de accesos.
A.9	CONTROL DE ACCESO		
A.9.1	Requisitos del negocio para el control de acceso **Objetivo:** Limitar el acceso a información y a instalaciones de procesamiento de información		
A.9.1.1	Política del control de acceso	SI	Se deberá implementar y crear una política de acceso que permitan garantizar la seguridad de las áreas de HECC COURRIER donde se trabaje con activos sensibles para la organización. Esta política debe dar a conocer a los colaboradores de la organización los niveles de seguridad de la información y la importancia de esos niveles de acuerdo a su clasificación. Se deberá tener reglas que requieran aprobación y las que n requieran aprobación, se deberá tener una política donde tendrá lo que los empleados necesitan conocer y lo que necesita tener para el uso de las actividades en el trabajo.
			Solución: Política de Control de Accesos (Ver Anexo A Numeral 1.2.4).
A.9.1.2	Acceso a redes y a servicios en red	SI	Se deberá contar con un proceso de seguridad para el acceso a las redes y servicios de red que cada empleado debe tener debe ser el necesario, para este proceso se debe tener autorizaciones para que se determine a quien se le permite el acceso a cuáles redes. El acceso a las redes deberá ser controlado por requisitos de autenticación de usuarios para proteger la información que circula en la red.
			Solución: Política de Control de Accesos (Ver Anexo A Numeral 1.2.4).
A.9.2	Gestión de Accesos de Usuarios **Objetivo**: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.		
A.9.2.1	Registro y cancelación del registro de usuarios	SI	Se tiene que tener un proceso preciso del registro y cancelación de usuarios, para el registro tendrá que realizarse un procedimiento que vaya desde la autorización y mantener la responsabilidad por las acciones que se realicen con los usuarios asignados que deben ser únicos. Se deberá realizar un proceso para la des habilitación de usuarios que ya no

			trabajen en HECC COURRIER, para evitar la suplantación y ataques de fraude en la organización. **Solución:** Política de Control de Accesos (Ver Anexo A Numeral 1.2.4).
A.9.2.2	Suministro de acceso de usuarios	SI	Se deberá contar con un proceso formal para asignar o revocar permisos de acceso este proceso deberá contar con autorización, verificación de acceso para conocer si es el apropiado para la función a desempeñar, soportar un registro central de los derechos de acceso suministrado a un usuario, revisar mensualmente de los derechos de acceso no han caducado. Se recomienda considerar la inclusión, en los contractos del personal y en los contratos de servicio, numerales que especifiquen sanciones si miembros del personal o contratistas intentan acceso no autorizado. **Solución:** Política de Control de Accesos (Ver Anexo A Numeral 1.2.4).
A.9.2.3	Gestión de derechos de acceso privilegiado	SI	Se deberá tener el acceso no permitido y el control sobre la asignación de cada derecho privilegiado entiéndase por derecho al equipo, sistema de información a la que es debido asignar cada usuario. Este acceso deberá ser en base a la necesidad de uso basado en la política de acceso, deberá contar con requisitos para el vencimiento de los derechos privilegiados. Para el acceso de usuario de administración, se debería mantener la confidencialidad de la información de autenticación privada cuando se comparta (por ejemplo, cambiar las contraseñas con frecuencia, y tan pronto como sea posible cuando un usuario privilegiado ha dejado el trabajo o cambia de trabajo, comunicarlas entre los usuarios privilegiados con los mecanismos apropiados. **Solución:** Política de Control de Accesos (Ver Anexo A Numeral 1.2.4).
A.9.2.4	Gestión de información de autenticación secreta de usuarios	SI	Se deberá tener un proceso claro de definición para el acceso a los equipos, las claves son un tipo de información de autenticación privada usado comúnmente, y son un medio común para corroborar la exactitud del usuario estas se entregarán de forma personal y se obligara que sea remplazado en el primer ingreso a los sistemas para los que sean establecidos. **Solución:** Política de Control de Accesos (Ver

			Anexo A Numeral 1.2.4).
A.9.2.5	Revisión de los derechos de acceso de usuario	SI	La organización HECC COURRIER deberá considerar revisar en intervalos regulares los derechos de acceso que posee cada usuario. Dando seguridad que no se hayan asignado privilegios no autorizados, adicional a lo anterior se deben revisar las autorizaciones que se otorgan para esos derechos de acceso.
			Solución: Política de Control de Accesos (Ver Anexo A Numeral 1.2.4).
A.9.2.6	Retiro o ajuste de los derechos de acceso	SI	Se deberá contar con un proceso o una directriz en la política de retiro de privilegios de usuario cuando el colaborador se encuentre en vacaciones, esté ausente en la organización mayor a un lapso de 10 días o que el empleado ya se encuentre desempeñando ningún cargo en la organización en resumen los derechos de acceso a la información y a los activos asociados so9bre todo al área de operaciones donde se procesa información importante del negocio se deberían retirar antes de que el empleo termine o cambie, dependiendo de la evaluación de factores de riesgo.
			Solución: Política de Control de Accesos (Ver Anexo A Numeral 1.2.4).
A.9.3	Responsabilidades de los usuarios **Objetivo**: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.		
A.9.3.1	Uso de la información de autenticación secreta	SI	Se debe notificar a los empleados que se soporte la confidencialidad de la información de autenticación, asegurándose de que no sea publicada a ninguna otra parte, se evite tener las claves de acceso a los sistemas de información y los equipos de cómputo visibles en notas de papel o en archivos públicos del equipo. Se deberá recomendar a los empleados que las contraseñas sean fáciles de recordar sean con una longitud considerable que contengan caracteres alfanuméricos, mayúsculas, minúsculas y caracteres especiales para que no sean vulnerables a ataques.
			Solución: Política de escritorio y pantalla limpia (Ver Anexo A Numeral 1.2.6).
A.9.4	Control de acceso a sistemas y aplicaciones **Objetivo**: Evitar el acceso no autorizado a sistemas y aplicaciones		

A.9.4.1	Restricciones de acceso a la información	SI	La organización deberá restringir el acceso a la información de acuerdo a la política de control de acceso, deberá controlar y limitar la información a la que tiene permisos cada empleado que información puede visualizar y cual no. Proveerá controles físico o lógico para el aislamiento de datos críticos para la organización o sistemas críticos como el Sim utilizado en el área de operaciones. **Solución:** Política de Control de Accesos (Ver Anexo A Numeral 1.2.4).
A.9.4.2	Procedimiento de ingreso seguro	SI	Para el ingreso o acceso físico al área de operaciones se deberá tener un seguro mediante tarjeta inteligente. Para el ingreso a información contenida en esta área se deberá contar registros de acceso donde se lleve una fecha y hora del ingreso no se deberá contar con transmisión de contraseñas en un texto claro se deberá utilizar llaves criptográficas que permitan proteger la información. Para el área de los servidores se contara con un control de acceso de tarjetas inteligentes que permitan solo el acceso del personal autorizado. **Solución:** Política de Seguridad Física y del Entorno (Ver Anexo A Numeral 1.2.7).
A.9.4.3	Sistemas de gestión de contraseñas	Si	Como se mencionó antes en el control 9.3.1 la calidad de las contraseñas deber ser de la manera más segura se forzará para que los usuarios estén cambiando frecuentemente las contraseñas cada 2 meses y no se repitan contraseñas ya utilizadas. El sistema de información no deberá permitir la visualización de contraseñas en la pantalla cuando se está ingresando. **Solución:** Política de Control de Accesos (Ver Anexo A Numeral 1.2.4).
A.9.4.4	Uso de programas útiles privilegiados	SI	Los encargados del área de sistemas verifican que sean instalados solo los sistemas y programas estrictamente necesarios y licenciados en ningún equipo se hace uso de programas administradores para los usuarios. También se realiza la verificación de programas utilitarios innecesarios que se encuentran instalados. **Solución:** Inventario de software libre autorizado y software base (Ver Anexo B Numeral 1.6).
A.9.4.5	Control de acceso a códigos fuente de programas	No	No se implementara control de acceso a código fuente de programas ya que no se posee fuentes de los programas usados en ninguna parte de la organización

A.10	CRIPTOGRAFÍA		
A.10.1	Controles criptográficos **Objetivo**: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.		
A.10.1.1	Política sobre el uso de controles criptográficos	SI	La organización deberá contar con controles criptográficos para el procedimiento de información se deberá contar con el uso de encriptación para la seguridad de información trasladada por dispositivos o a través de líneas de comunicación. Los controles criptográficos se deberán usar con objetivos de seguridad de la información tales como confidencialidad, integridad, no-repudio y autenticación. **Solución:** Política de Controles Criptográficos (Ver Anexo A Numeral 1.2.8).
A.10.1.2	Gestión de claves	NO	Por el momento se recomendará tener a futuro el uso de claves criptográficas tales como llaves o algoritmos de cifrado de información. Se estudiara la posibilidad de tener certificados de llaves públicas las cuales deberán ser actualizadas y destruidas para reducir la probabilidad de uso inapropiado de las mismas, estas llaves tendrán fecha de vencimiento para que solo puedan usarse por un periodo de tiempo no mayor a tres meses.
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO		
A.11.1	Áreas seguras: **Objetivo**: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.		
A.11.1.1	Perímetro de seguridad física	SI	La organización deberá definir claramente el perímetro de seguridad, contar con delimitaciones de acceso, definir el personal autorizado para el acceso de área restringida que se recomienda se controle por tarjetas de control de acceso. Adicional los tejados, muros externos y el material de los pisos deberán ser de construcción sólida. El acceso a las instalaciones de HECC COURRIER está siendo controlado por alarmas y cerraduras, adicional al control de acceso que posee el conjunto de bodegas donde se encuentra ubicada la organización. **Solución:** Política de Seguridad Física y del Entorno (Ver Anexo A Numeral 1.2.7) e Instructivo para el acceso a las instalaciones de Hecc Courrier (Ver Anexo B Numeral 1.2).

A.11.1.2	Controles de acceso físico	SI	Las áreas que necesiten protección se deberán tener controles para asegurar solo el permiso de acceso a personal autorizado debe llevarse un registro de fecha y hora de entrada y salida de visitantes, esto se debe tener en la recepción de la organización, Aquí mismo se otorgara la tarjeta de acceso que le permitirá acceder a ciertas áreas de la empresa. Para los visitantes se debe verificar que los funcionarios que ingresen porten un documento visible que lo identifique como personal autorizado. El acceso a áreas donde se almacena información de cierta clasificación confidencial se deberá contar con previa autorización de parte de la alta gerencia. Las tarjetas de acceso deben ser programadas debidamente para tener un registro de hora de entrada y salida de las mismas. **Solución:** Política de Seguridad Física y del Entorno (Ver Anexo A Numeral 1.2.7) e Instructivo para el acceso a las instalaciones de Hecc Courrier (Ver Anexo B Numeral 1.2).
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	SI	Se tiene que tener en cuenta los requisitos de alumbrado, ventilación salubridad, infraestructura antiincendios, medidas que evitan inundaciones robos etc. Se debe elegir el área de la estructura de la oficina y la atención al público debe estar retirada del área restringida, establecer de oficiales de seguridad y de alarmas. **Solución:** Política de Seguridad Física y del Entorno (Ver Anexo A Numeral 1.2.7) e Instructivo para el acceso a las instalaciones de Hecc Courrier (Ver Anexo B Numeral 1.2).
A.11.1.4	Protección contra amenazas externas y ambientales	SI	Se deberá contactar con asesores especiales que indiquen a la organización acerca de cómo evitar daños a causa de incendios, inundaciones, terremotos, explosiones, disturbios civiles y otras formas de desastres naturales. Como recomendación de seguridad para temas de inundaciones los centros de cómputo de los servidores no deberán están en el nivel 1 o sótano. **Solución:** Plan de Emergencias (Ver Anexo B Numeral 1.10).
A.11.1.5	Trabajo en áreas de seguridad	NO	No se tiene área de seguridad.
A.11.1.6	Áreas de despacho y carga	SI	Las áreas como archivo histórico y ubicación de servidores se designan áreas de mucho cuidado por la información que se manipula, por tanto, se debe evitar que los contratistas o personas ajenas a la organización puedan

			llegar a tener acceso a esta. Las áreas de carga y despacho de carga solo tienen acceso los mensajeros donde se les hace entrega de los paquetes a entregar, todo el material que se despacha y se recibe es registrado de acuerdo a la organización. La información entrante se inspecciona para determinar la no manipulación por el personal no autorizado.
			Solución: Política de Seguridad Física y del Entorno (Ver Anexo A Numeral 1.2.7) e Instructivo para el acceso a las instalaciones de Hecc Courrier (Ver Anexo B Numeral 1.2).
A.11.2	Seguridad de los equipos **Objetivo**: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.		
A.11.2.1	Ubicación y protección de los equipos	SI	Los equipos de la central de cómputo como (Servidores, racks etc.) están distribuidos en un lugar donde no se tenga riesgo, es decir en un lugar retirado y resguardado tanto de amenazas naturales ambientales, físicas y humanas, adicional a esta medida se restringirá el acceso. Es decir que, solo podrán acceder los funcionarios autorizados con su credencial y los accesos y tareas a realizar serán un trabajo documentado por el encargado de la seguridad; las labores de aseo serán verificadas para evitar daños y hurtos. Al igual la organización cuenta con un circuito de televisión cerrada para monitorizar las labores del personal en el área de operaciones. Se deben establecer directrices referentes a comer, consumir líquidos y fumar en cercanías a las instalaciones internas.
			Solución: Se sugiere en las normas de trabajo incluir las normas para la prohibición de comer, consumir líquidos y fumar en las instalaciones. Con lo referente a la ubicación el Instructivo para el acceso a las instalaciones de Hecc Courrier (Ver Anexo B Numeral 1.2).
A.11.2.2	Servicios de suministros	SI	En cada ciclo se debe revisar el correcto funcionamiento de las construcciones eléctricas para prevenir incidentes, la empresa debe optar por resistir desperfectos en el suministro de energía como la compra de una planta eléctrica, la compra de ups para los pc, los computadores deben bloquearse después de diez (10) minutos de inactividad, el usuario tendrá que autenticarse antes de reanudar su sesión. Todos los usuarios deben bloquear la sesión al retirarse de los dispositivos. Se deberá suministrar iluminación y medios de

			comunicación de emergencia.
			Solución: Política de Escritorio y Pantalla Limpia con referente a los suministros se debe adquirir ups para los servidores y los equipos del área de operaciones (Ver Anexo A Numeral 1.2.6).
A.11.2.3	Seguridad de cableado	NO	Las líneas de potencia y de telecomunicaciones que entran a instalaciones de procesamiento de información deberían ser subterráneas en donde sea posible, o deberían contar con una protección alternativa adecuada es por esto que el cableado de datos interno debe ir por medio de canaletas no visibles si es posible. El cableado eléctrico y el cableado de datos deberán ir separado para evitar interferencia.
A.11.2.4	Mantenimiento de equipos	SI	Se deberán realizar con frecuencia mantenimientos preventivos programados a los equipos, estos mantenimientos deben ser registrados y documentados donde no afecten a la operación, solo el personal del área de sistemas debe ser el encargado de ejecutar los mantenimientos o reparaciones de los equipos. Después de realizar los mantenimientos en los equipos de debe verificar que los equipos se encuentren funcionando y no afecten a la operación.
			Solución: Instructivo de Mantenimiento (Ver Anexo B Numeral 1.8).
A.11.2.5	Retiro de equipos	SI	La organización se tiene que identificar a los colaboradores, proveedores y usuarios de partes externas que tienen autoridad para retirar los activos de la organización, aunque HECC COURRIER no posee usuarios autorizados para retirar activos de la organización. Solo cuando sea necesario y apropiado, se debería registrar cuando los activos se retiran de las instalaciones de la organización y cuando se hace su devolución, se debe documentar la identidad, el rol y la fijación de cualquiera que maneje o se utilice activos, y devolver esta documentación con el equipo, la información y el software. Solo cuando un equipo es remplazado de lugar o destruido se debe tener total cuidado con los medios de almacenamiento como por ejemplo discos duros los cuales deben ser limpiados o eliminados de una manera segura para prevenir incidentes con la información

			Solución: Instructivo para el traslado y retiro de activos (Ver Anexo B Numeral 1.9).
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones.	NO	Como se menciona en el punto 11.2.5 no se tienen activos por fuera de la organización que no se tengan controlados.
A.11.2.7	Disposición segura o reutilización de equipos	SI	Los dispositivos de almacenamiento que tienen información confidencial o protegida por derechos de autor se deberían destruir físicamente, eliminar o sobrescribir usando formas para hacer que la información original no sea recuperable, en vez de hacer uso de formatear y eliminar. Los equipos que tienen algún defecto y que se encuentran almacenados para ser reutilizados se deben hacer una valoración de riesgos para especificar si los elementos se deberían destruir físicamente en vez de enviarlos a reparación o desecharlos.
			Solución: Instructivo para el traslado y retiro de activos (Ver Anexo B Numeral 1.9).
A.11.2.8	Equipo de usuario desatendido	SI	La organización debe garantizar la sensibilización y el correcto uso de los equipos para esto se debe notificar a los usuarios que bloqueen los equipos cuando no se encuentren en el sitio de trabajo, se debe cerrar la sesión que se encuentra activa, se debe cerrar la sesión de las aplicaciones y se debe salir de la ubicación de los servicios de red cuando ya no los necesiten.
			Solución: Política de Escritorio y Pantalla Limpia (Ver Anexo A Numeral 1.2.6).
A.11.2.9	Política de escritorio limpio y pantalla limpia.	SI	La política de escritorio limpio protege la información sensible o critica de la organización, con la política de pantalla limpia disminuye los riesgos de acceso no autorizado y de fraude o pérdida de información durante y por fuera de las horas laborales normales. HECC COURRIER cuenta con una caja de seguridad para proteger la información almacenada en ella contra desastres tales como incendios, terremotos, inundaciones o explosión.
			Solución: Política de Escritorio y Pantalla Limpia (Ver Anexo A Numeral 1.2.6).
A.12	SEGURIDAD DE LAS OPERACIONES		
A.12.1	Procedimientos operacionales y responsabilidades **Objetivo**: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.		

A.12.1.1	Procedimientos de operación documentado.	SI	Los procedimientos de operación especificaran las instrucciones operacionales que incluyen como la instalación y configuración de los sistemas necesarios para que el colaborador pueda desempeñar sus funciones, las instrucciones para el manejo de errores que podrían surgir durante la ejecución del trabajo, incluidas las restricciones sobre el uso de sistemas utilitarios, instrucciones sobre el manejo de medios magnéticos como usb, cds etc.
			Solución: Política para el uso de Medios Removibles (Ver Anexo A Numeral 1.2.5) e Inventario de software libre autorizado y software base (Ver Anexo B Numeral 1.6).
A.12.1.2	Gestión de cambios	SI	Los cambios operacionales se deben verificar para que no afecten la seguridad en los equipos que son controlados. Los cambios deben ser revisados, aprobados previamente y se tendrán en cuenta las siguientes formas: Estimación del cambio y posible colisión, planificación, ensayo, e identificación de deberes en caso de que el cambio sea el no esperado.
			Solución: Solicitud de cambios y o servicios (Ver Anexo B Numeral 1.11).
A.12.1.3	Gestión de capacidad	SI	Los encargados del área de sistemas deben tener monitoreo continuos de los recursos disponibles y programar la adquisición de nuevos recursos y estos deben estar proyectos para beneficios de la organización todo para poder desempeñar más rápido y subir la calidad de seguridad de la organización. Se debe prestar atención particular a cualquier recurso con un tiempo prolongado de uso por tanto el área de sistema debe hacer búsqueda de la utilización de los recursos clave de sistemas que hagan parte de la operación.
			Solución: Instructivo para el monitoreo de registros técnicos (Ver Anexo B Numeral 1.7).
A.12.1.4	Separación de ambientes de desarrollo, pruebas y operación	NO	No se tienen ambientes de desarrollo de software, ni de prueba la organización trabaja con aplicaciones netamente ya dominadas y las cuales en un futuro cercano no son actualizadas
A.12.2	Protección contra códigos maliciosos **Objetivo**: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.		

A.12.2.1	Controles contra códigos maliciosos	SI	Se debe realizar un plan de capacitación de concientización a los empleados basados en la seguridad de la información y los riesgos a los que están vulnerables los activos, fundamentalmente sobre el software de código malicioso. El área de sistemas y los colaboradores deben especificar que el software está resguardado con antivirus y debe existir una directriz documentada de actualización de todo el software utilizado, antivirus y sistema operativo. Al mismo tiempo se prohíbe la instalación de ningún software, se monitorea constantemente el software de los servidores.
			Solución: Política Contra Código Malicioso (Ver Anexo A Numeral 1.2.9).
A.12.3	Copias de respaldo **Objetivo**: Proteger contra la pérdida de datos		
A.12.3.1	Respaldo de la información	SI	El área de sistemas será el responsable de la información definirán un resumen de defensa de la información entre ellas: Copias de seguridad y prueba de restauración, se debe establecer un esquema de etiquetado de copias, guardar copias de seguridad en una ubicación no fisica, el guardado de copias de seguridad debe estar físicamente seguro con un esquema de seguridad especial. El procedimiento es documentado y se realizan pruebas de restablecer a intervalos programados.
			Solución: Política de Almacenamiento y Respaldo (Ver Anexo A Numeral 1.2.10).
A.12.4	Registro y seguimiento **Objetivo**: Registrar eventos y generar evidencia		
A.12.4.1	Registro de eventos	SI	El encargado de seguridad debe establecer un registro del uso de los sistemas como: Tiempo de inicio, cierre, errores del sistema, la finalidad de acceso al sistema, medidas tomadas etc. El sistema de información sim tiene un registro de logs de accesos al sistema. Este control establece las bases para que los sistemas de seguimiento automatizados que están en la capacidad de generar informes consolidados y generar alertas de seguridad sobre los mismos sistemas. En ninguno de los casos los administradores de los sistemas deberán tener el acceso para borrar o alterar la integridad de los sistemas.

			Solución: Instructivo Revisión de registros automáticos (Ver Anexo B Numeral 1.4).
A.12.4.2	Protección de la información de registro	SI	Se recomienda a HECC COURRIER que los controles de protección de la información de registro deben estar dirigidos a proteger contra cambios no autorizados de la información del registro y contra problemas con la instalación de registro donde entra alteraciones a los tipos de mensaje que se registran, archivos editados o eliminados. Para esto los logs deben ser protegidos ya que, si los datos se pueden modificar o borrar, su existencia puede crear una cesación de seguridad débil. Se debe utilizar un copiado de seguridad de los logs en tiempo real para que estos no sean vulnerados.
			Solución: Instructivo Revisión de registros automáticos (Ver Anexo B Numeral 1.4).
A.12.4.3	Registros del administrador y del operador	SI	Las acciones y registros de los coordinadores también son almacenados y protegidos de cualquier transformación, los dueños de las cuentas de usuarios pueden estar en la capacidad de manipular los logs en oficinas de procesamiento de información bajo un control directo. Por esto, es requerido asegurar y revisar los logs para conservar la rendición de cuentas para los usuarios.
			Solución: Instructivo Revisión de registros automáticos (Ver Anexo B Numeral 1.4).
A.12.4.4	Sincronización de relojes	SI	El ajuste correcto de los relojes de los equipos de cómputo es de alto valor para asegurar la exactitud de los logs de auditoría, que pueden ser necesarios para investigaciones o como evidencia legal en casos legales o casos disciplinarios. Los logs de auditoría inexactos pueden dificultar estas investigaciones y afectar la credibilidad de esta evidencia. Se puede usar un protocolo de tiempo de red para conservar todos los servidores sincronizados con el reloj maestro. El área de sistemas debe ser el encargado de asegurar que todos los sistemas están acordes y ajustados en una observación de tiempo única y sincronizada.
			Solución: Instructivo para sincronización de relojes (Ver Anexo B Numeral 1.5).
A.12.5	Control de Software operacional **Objetivo**: Asegurar la integridad de los sistemas operacionales		
A.12.5.1	Instalación de software en sistemas operativos.	SI	La instalación o desinstalación de cualquier elemento software o hardware en los equipos de cómputo de la organización, es responsabilidad del funcionario encargado del manejo de los elementos tecnológicos, y por

			tanto será el único autorizado para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por la institución a través de la Dirección. Debe existir una documentación sobre el proceso de instalación de los sistemas operativos todo esto cumpliendo con las políticas de seguridad de la información.
			Solución: Inventario de software libre autorizado y software base (Ver Anexo B Numeral 1.6).
A.12.6	Gestión de la Vulnerabilidad Técnica **Objetivo**: Prevenir el aprovechamiento de las vulnerabilidades técnicas.		
A.12.6.1	Gestión de las vulnerabilidades técnicas	SI	Para la oportuna evaluación de la información basadas en las vulnerabilidades técnicas de los sistemas de información lo primero que se necesitara será un inventario actualizado de todos los activos de la organización e identificar los responsables de cada activo, lo siguiente es tomar acciones apropiadas y oportunas en respuesta a la identificación de vulnerabilidades técnicas potenciales una vez que se haya identificado una vulnerabilidad técnica potencial, la organización debería identificar los riesgos asociados y las acciones por tomar; esta acción puede involucrar la colocación de parches de sistemas vulnerables o la aplicación de otros controles, se deberían abordar primero los sistemas que están en alto riesgo.
			Solución: Instructivo Para el Monitoreo de Registros Técnicos (Ver Anexo B Numeral 1.7).
A.12.6.2	Restricciones en la instalación de software	SI	La instalación de software es hecha sólo por los empleados autorizados y con software probado y licenciado se le suma el principio del menor privilegio. El procedimiento de instalación es documentado.
			Solución: Inventario de software libre autorizado y software base (Ver Anexo B Numeral 1.6).
A.12.7	Consideraciones sobre auditorías de sistemas de información **Objetivo**: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.		
A.12.7.1	Controles sobre auditorías de sistemas de información	NO	No se poseen auditorias sobre los sistemas de información operacionales
A.13	SEGURIDAD DE LAS COMUNICACIONES		
A.13.1	Gestión de la seguridad de las redes		

	Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.		
A.13.1.1	Controles de redes	SI	HECC COURRIER buscando prevenir y controlar el acceso que tienen los empleados y visitantes; el área de sistemas, realizara un estricto control de contenido en Internet, agrupando perfiles de accesos comunes en los que se administran los permisos de acceso a las páginas necesarias para desempeñar las labores de cada uno de los empleados de la empresa. Se deberían aplicar logging y seguimiento adecuados para posibilitar el registro y detección de acciones que pueden afectar, o son pertinentes a la seguridad de la información.
			Solución: Política de Control y Gestión de los Servicios de Red (Ver Anexo A Numeral 1.2.11).
A.13.1.2	Seguridad de los servicios de red	SI	HECC COURRIER deberá contar con directrices que controlen el uso de servicios de red, administrados principalmente, desde un firewall. La tecnología aplicada a la seguridad de servicios de red debe tener restricciones de acceso a los servicios de red de acuerdo con las reglas de conexión de seguridad de la red. Se deberán bloquear páginas que generan un mayor consumo de ancho de banda, también se bloquean las páginas generadoras de filtraciones de códigos maliciosos y las que podrían perjudicar el correcto funcionamiento de los equipos y dispositivos que se encuentran en la red interna.
			Solución: Política de Control y Gestión de los Servicios de Red (Ver Anexo A Numeral 1.2.11).
A.13.1.3	Separación en las redes	SI	Se le recomienda a la organización como uno de los mecanismos que puede utilizar para controlar la red, es la subdivisión de red interna en dominios, cada dominio se encuentra protegido con políticas de acceso y control de contenido específico, fundamentado en la política de control de acceso, en la clasificación de la información que se realiza conforme a la metodología para el manejo de la información. Se debe también tener en cuenta la segmentación (VLAN) configurar los switch alojados en el centro de cómputo de sistemas.
			Solución: Política de Control y Gestión de los Servicios de Red (Ver Anexo A Numeral 1.2.11).
A.13.2	Transferencia de información		

	Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.		
A.13.2.1	Políticas y procedimientos de transferencia de información	SI	Se tiene que dar garantía que la información se localice segura al ser llevada haciendo uso de diferentes servicios de comunicación. Las responsabilidades del personal externo y cualquier otro usuario no comprometen a la organización. Puede ocurrir transferencia de información mediante el uso de varios tipos diferentes de instalaciones de comunicación, incluido el correo electrónico, voz, fax y video. La transferencia de software puede ocurrir a través de varios medios diferentes, incluida la descarga desde internet y la adquisición de productos en el comercio. Se deberían tener en cuenta las intervenciones para el negocio, y las implicaciones normativas y de seguridad asociadas con el intercambio electrónico de datos, el comercio electrónico y las comunicaciones electrónicas, y los requisitos para los controles.
			Solución: Políticas y procedimientos de transferencia de información (Ver Anexo A Numeral 1.2.12).
A.13.2.2	Acuerdos sobre transferencia de información	SI	Se deben tener los acuerdos de transferencia de información sobre todo con los clientes donde se deben tener las responsabilidades de la alta gerencia y de la dirección para controlar y notificar la transmisión, se debe tener procedimientos para asegurar la trazabilidad y no repudio, las responsabilidades y obligaciones en el caso de incidentes de seguridad de la información, tales como pérdidas de datos, mantener una cadena de custodia para la información mientras está en tránsito. Estos acuerdos deben estar estipulados en contratos formales.
			Solución: Políticas y procedimientos de transferencia de información (Ver Anexo A Numeral 1.2.12).
A.13.2.3	Mensajería electrónica	SI	Se deberá garantizar los mensajes electrónicos mediante niveles fuertes de autenticación desde redes accesibles públicamente, la protección de mensajes garantizando la confiablidad y disponibilidad del servicio de mensajería.
			Solución: Políticas y procedimientos de transferencia de información (Ver Anexo A Numeral 1.2.12).

A.13.2.4	Acuerdos de confidencialidad o de no divulgación	SI	Para HECC COURRIER los acuerdos de confidencialidad o de no divulgación deberían tener en cuenta el requisito de asegurar la información confidencial usando términos ejecutables legalmente. Los acuerdos de confidencialidad o de no divulgación son ejecutables a las partes externas o a empleados de la organización. Se deberían seleccionar o adicionar elementos teniendo en cuenta el tipo de la otra parte y su acceso o manejo permisible de la información confidencial. Estos acuerdos se deben tener a savol la información de la organización e informa a los que se declaran acerca de la responsabilidad para proteger, usar y de transmitir la información de una manera segura. **Solución:** Acuerdos de confidencialidad que la organización deberá realizar.
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS		
A.14.1	Requisitos de seguridad de los sistemas de información **Objetivo:** Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye los requisitos para sistemas de información que presten servicios sobre redes públicas.		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	SI	La empresa actualmente no tiene una política determinada hacia el análisis y especificación de requisitos de seguridad de la información. Tras realizar el análisis de la gestión de seguridad con la identificación de amenazas y riesgos, su impacto en los activos de información y valoración de cada tipo, se tiene que realizar y documentar los requisitos con que debe contar la empresa en sus procesos de seguridad. Habiendo realizado un análisis de estos requisitos se obtiene información capaz de hacer que las áreas encargadas puedan mejorar la estructura de seguridad y los procedimientos en caso de cualquier ataque. Es claro que esto debe ser liderado por los jefes operativos y de sistemas. **Solución:** Política de Gestión de Activos (Ver Anexo A Numeral 1.2.3).
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	SI	El área de sistemas deberá implementar de alguna forma algoritmos correctos de cifrado que certifiquen la confidencialidad e integridad de la información que se envíen a través de las redes públicas. Se debe evitar la pérdida o información repetida de la información de transacciones. Las disposiciones sobre servicio

			de aplicaciones entre socios deberían estar apoyadas por un acuerdo documentado que involucra a ambos lados bajo los términos de los servicios acordados, incluidos los detalles de la autorización.
			Solución: Política de Control y Servicios de Red (Ver Anexo A Numeral 1.2.11).
A.14.1.3	Protección de las transacciones de los servicios de las aplicaciones	SI	El área de sistemas deberá hacer el uso de firmas electrónicas para cada una de las partes involucradas en transacciones por medios de algoritmos fuertes de cifrado que garanticen la confidencialidad e integridad de la información que se transmite a través de las redes. Los protocolos que se usaran para las partes involucradas deben ser seguros. En los casos donde se use una autoridad confiable, la seguridad estará integrada e incluida en todo el proceso de gestión de certificados/firmas de un extremo a otro
			Solución: Política de Controles Criptográficos (Ver Anexo A Numeral 1.2.8) y Política de Transferencia de Información (Ver Anexo A Numeral 1.2.12).
A.14.2	Seguridad en los procesos de desarrollo y soporte **Objetivo:** Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.		
A.14.2.1	Política de desarrollo seguro	NO	La empresa no realiza desarrollos de software ni tiene pensado en el futuro convertirse en una empresa que preste dicho servicio. Los desarrollos utilizados son por adquisición de otras empresas ya que su objetivo y negocio está en el tema de mensajería.
A.14.2.2	Procedimientos de control de cambios en sistemas	NO	Al no aplicar desarrollo de software, este control tampoco es necesario de aplicar.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	SI	No se encuentra una política para la revisión de las aplicaciones al efectuarse cambios en la plataforma, pero si se realizan pruebas para verificar su funcionamiento. La empresa al manipular información sensible requiere que las aplicaciones sean probadas debidamente y revisadas para que no exista fuga de información o que se pueda corromper los datos de alguna manera. Es necesario que exista en las políticas un ítem que determine como obligatorio estas revisiones de las plataformas y aplicaciones.
			Solución: Política de Continuidad en las Operaciones (Ver Anexo A Numeral 1.2.2).
A.14.2.4	Restricciones en los cambios a los paquetes de software	NO	No existe una política que mencione este control ya que los cambios y actualizaciones son realizados por la empresa que provee las

			aplicaciones.
A.14.2.5	Principios de construcción de los sistemas seguros	NO	La empresa no efectúa desarrollos de software, por lo tanto no aplica este control.
A.14.2.6	Ambiente de desarrollo seguro	NO	La empresa no efectúa desarrollos de software, por lo tanto no aplica este control.
A.14.2.7	Desarrollo contratado externamente	SI	No existe política al respecto, pero si se tiene desarrollos contratados externamente para el funcionamiento de la organización. Se debe tener conocimiento de la legalidad del software que se adquiere, tener prácticas y pruebas de funcionamiento seguro. Es clave que todo este documentado y reglamentado para asegurar que en alguna auditoria externa no se encuentren estos fallos que pueden perjudicar a la organización y su funcionamiento.
			Solución: Política de Relación con Proveedores (Ver Anexo A Numeral 1.2.13).
A.14.2.8	Pruebas de seguridad de sistemas	NO	Al no desarrollar software no se requiere tener una política que verifique la realización de pruebas de seguridad en los sistemas y su desarrollo.
A.14.2.9	Pruebas de aceptación de sistemas	SI	Aunque no se tiene una política establecida, los ingenieros de sistemas efectúan pruebas de todo tipo de seguridad en los desarrollos contratados, para poder tener una aceptación de la adquisición realizada. Es clave que la empresa encargada de proveer el desarrollo entregue la documentación de su desarrollo y aplicativo, así mismo los ingenieros de sistemas de HECC COURRIER avalan los procesos, la forma en que lo ejecutaron, las pruebas y su funcionamiento, sin esto no se puede tener el aval de que la plataforma sea implementada en la organización.
			Solución: Política de Continuidad en las Operaciones (Ver Anexo A Numeral 1.2.2).
A.14.3	Datos de prueba **Objetivo:** Asegurar la protección de los datos usados para pruebas.		
A.14.3.1	Protección de datos de prueba	NO	No existe una política que relacione la protección de datos de prueba. La empresa adquiere desarrollo en infraestructura de proveedores, y son ellos quienes deben efectuar dichas pruebas.
A.15	RELACIONES CON LOS PROVEEDORES		
A.15.1	Seguridad de la información en las relaciones con los proveedores **Objetivo:** Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.		

A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	SI	Actualmente no se tiene una política para este caso. La empresa debe tener una política en la cual se especifique los niveles de seguridad a los cuales los proveedores de servicios tendrán acceso en la organización. Dichos proveedores de servicios y de infraestructura van a estar en la organización eventualmente y tendrán acceso a información en algunos procesos ya que de ellos depende que el flujo del proceso continúe. De aquí que se tengan política para no divulgar información, transferencia de información, entre otros. Todo esto debe estar documentado para constatar que las partes están de acuerdo en que los proveedores tendrán contacto con los activos de información y que no perjudicaran los procesos de la organización. **Solución:** Política de Relación con Proveedores (Ver Anexo A Numeral 1.2.13).
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	SI	De acuerdo al anterior punto, se debe determinar el acceso de los proveedores a la organización para que puedan suministrar los elementos o servicios que brindan, permitir la instalación de equipos de infraestructura y de algún tipo de servicio de software que se requiera. Todo esto debe estar documentado y registrado donde las partes se comprometen tanto a permitir el acceso y manejo de los activos de información como de la confidencialidad de los proveedores al no suministrar alguna información a agentes externos, como también en el caso de corromper información en los procesos de instalación de servicios e infraestructura. Los jefes operativos y de sistemas deben estar atentos a todo tipo de procesos que los proveedores efectúen. **Solución:** Política de Relación con Proveedores (Ver Anexo A Numeral 1.2.13).
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	SI	Este control no se aplica actualmente al no haber una política con los proveedores, la cadena de suministro de tecnología de información y comunicación debe estar reglamentada para que los proveedores tengan acceso limitado a la información, y donde los activos no van a ser perjudicados o corrompidos y mucho menos los procesos de la empresa. Hay riesgos que se tienen por agentes externos en cuanto al acceso a la información y es aquí donde un agente externo como lo son los proveedores no deben influir de manera negativa en los procesos del envío de correspondencia cuando se estén

			suministrando servicios y equipos de infraestructura.
			Solución: Política de Relación con Proveedores (Ver Anexo A Numeral 1.2.13).
A.15.2	Gestión de la prestación de servicios de proveedores **Objetivo:** Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.		
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	SI	Los jefes operativos y de sistemas deben estar al tanto y revisar lo que ocurre con los servicios que ofrecen los proveedores, así mismo debe tener como requisito que los equipos de infraestructura funcionen de manera correcta. Cualquier tipo de falla en dichos dispositivos o servicios puede ocasionar perdidas de información en el envío de correspondencia, algo fatal para el funcionamiento de la empresa. Es clave que la empresa tenga una política donde especifique y realice auditorias respecto a los servicios y equipos de infraestructura, lograr monitorear su estado y comportamiento, debe efectuarlas con intervalos de tiempo cortos no mayor a dos meses.
			Solución: Política de Relación con Proveedores (Ver Anexo A Numeral 1.2.13).
A.15.2.2	Gestión de cambios en los servicios de los proveedores	SI	Al realizarse seguimiento, revisión y auditoria a los servicios e infraestructura que ofrecen los proveedores seleccionados, se debe realizar un análisis si es conveniente continuar con dichos proveedores, identificar si se pueden mejorar los acuerdos tanto económicos como de los servicios prestados. Esto lleva tiempo de análisis si se tiene un proveedor de años y confiable donde se puede negociar, o si no se ha tenido un rendimiento que los satisfaga tratar de anular los acuerdos e ir en búsqueda de algún proveedor que mejore su servicio. No solo la parte operativa y de sistemas debe estar al tanto de ello, sino también el área comercial y contable como también la alta gerencia deben llegar a un acuerdo para observar que camino debe tomar la empresa en la relación con sus proveedores.
			Solución: Política de Relación con Proveedores (Ver Anexo A Numeral 1.2.13).
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		
A.16.1	Gestión de incidentes y mejoras de la seguridad de la información		

	Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.		
A.16.1.1	Responsabilidades y procedimientos	SI	La empresa no presenta documentación acerca de que responsabilidades y procedimientos en el manejo de incidentes. Esto se maneja de manera más informal, ya que cada área y cada empleado saben que en caso de presentarse algún fallo debe realizar procesos que mitiguen y resuelvan dicha situación. Es clave que se tengan responsabilidades determinadas en un documento donde haya claridad de que hacer en cada situación, los incidentes se presentan con frecuencia y es necesario saber quién debe resolverlo y como debe hacerlo, todo esto dado por áreas quienes saben cuáles son los problemas con que más se presenta y como debe resolverse. Es claro que allí se debe tener un plan de continuidad de negocio, donde los incidentes deben ser solucionados de inmediato para que no interfiera con los procesos de la empresa. Los jefes de cada área y la alta gerencia deben establecer dichas responsabilidades y deben determinar que procedimientos ejecutar en cualquier situación. Es clave tener una planificación adecuada y unos registros que permitan en un futuro saber cómo resolver cada situación para que al presentarse no tome un tiempo más largo de lo debido.
			Solución: Política para la Gestión de Incidentes de Seguridad de la Información (Ver Anexo A Numeral 1.2.14).
A.16.1.2	Reporte de eventos de seguridad de la información	SI	Los empleados de la organización siempre están enterados de lo que sucede en cada una de las áreas, al ser una organización pequeña se trata de que se colaboren en conjunto y puedan solucionar los incidentes de la manera más rápida posible. Actualmente no se tiene un reporte de dichos eventos o situaciones, es necesario empezar a documentar cualquier problema o incidente para así saber qué hacer y cómo solucionar de manera clara si se llega a presentar en un futuro. Este documento debe ser de conocimiento público para todos los empleados de la empresa, ellos deben estar pendientes de estas situaciones, los jefes de cada área deben también informar cualquier novedad si en algún momento el canal de información no es el adecuado.
			Solución: Política para la Gestión de Incidentes de Seguridad de la Información (Ver

			Anexo A Numeral 1.2.14).
A.16.1.3	Reporte de debilidades de seguridad de la información	SI	No solo los jefes operativos y de cada área deben informar sobre los incidentes o debilidades que se presenten en los procesos de la empresa, es clave que los empleados también entreguen información y la compartan a sus jefes respectivos y compañeros. Al no haber un encargado de la seguridad de la información los jefes operativos son los que deben estar a cargo de recibir la información, analizarla, describirla, documentarla y distribuirla para que toda la organización sepa cuáles son las debilidades encontradas en los procesos y donde se debe solventar de manera rápida y oportuna.
			Solución: Política para la Gestión de Incidentes de Seguridad de la Información (Ver Anexo A Numeral 1.2.14).
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	SI	La empresa no presenta en la actualidad una gestión de riesgos documentada y por ello la evaluación de los eventos de seguridad no se presenta. Es clave realizar un análisis de los riesgos, amenazas y eventos que puedan ocurrir para determinar el impacto que puedan presentarse en los activos de información. Dicha evaluación determina los niveles de los eventos y determina las prioridades para efectuar una gestión adecuada a la hora de solucionarlos o mitigarlos prontamente. Los jefes operativos determinan y aprueban dichas escalas.
			Solución: Política para la Gestión de Incidentes de Seguridad de la Información (Ver Anexo A Numeral 1.2.14).
A.16.1.5	Respuesta a incidentes de seguridad de la información	SI	Debe existir un plan de contingencia al presentarse cualquier tipo de incidente, debe haber documentación al respecto y determinar el proceso a seguir para que el funcionamiento de la empresa no se vea afectado drásticamente. Un plan de continuidad del negocio es clave, debe estar documentado y donde los empleados deben conocerlo para ayudar a efectuarlo en cualquier momento.
			Solución: Política para la Gestión de Incidentes de Seguridad de la Información (Ver Anexo A Numeral 1.2.14).

A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	SI	Como se mencionó en los anteriores controles, todo debe documentarse, tanto al momento de identificar los incidentes como de la manera para solucionarlo. Cada miembro de la empresa debe colaborar en la elaboración de un plan de contingencia de acuerdo al área que maneja, así se tendrá algo muy detallado por áreas para que cualquier empleado tenga esa información y pueda colaborar en cualquier momento. Cada vez que se presente un incidente es una oportunidad de aprendizaje, no solo para aplicar los correctivos necesarios si no para que disminuir el porcentaje de que se vuelva a producir. Una base de conocimiento sobre los incidentes, riesgos, amenazas y vulnerabilidades es demasiado importante para este control, con ello se va a tener una misma documentación para lograr controlarlos, mitigarlos y solucionarlos de manera rápida, oportuna y eficaz.
			Solución: Política para la Gestión de Incidentes de Seguridad de la Información (Ver Anexo A Numeral 1.2.14).
A.16.1.7	Recolección de evidencia	SI	La empresa no registra los incidentes en la actualidad, lo hace de manera informal, pero no con un documento serio que especifique lo que ocurre y lo detalla. Todo debe documentarse y registrarse, eso cuenta como evidencia para lo que se presente en el futuro. Tomar acciones legales por parte de la alta gerencia para determinar por qué se presentan los incidentes, como debe solucionarse e identificar responsabilidades si la afectación a la empresa en cuanto a sus procesos son muy graves hace que los empleados tomen seriedad en sus labores, donde no se debe permitir que haya brechas de seguridad y continúe pasando cualquier anomalía que corrompa los sistemas de seguridad establecidos y los activos se vean frágiles a la hora de cualquier ataque o vulnerabilidad no identificada.
			Solución: Política para la Gestión de Incidentes de Seguridad de la Información (Ver Anexo A Numeral 1.2.14).
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		
A.17.1	Continuidad de seguridad de la información **Objetivo:** La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.		

A.17.1.1	Planificación de la continuidad de la seguridad de la información	SI	La empresa no tiene documentación al respecto sobre lo que se debe hacer para tener una continuidad de la seguridad de la información. A pesar de ello se tratan los incidentes de acuerdo al conocimiento que se tenga y dependiendo del área en el que labore. La norma ISO 27001 determina como obligatorio que se realice una planificación y se tenga documentado los planes de continuidad del negocio, así mismo entra en esta categoría los planes de recuperación de desastres. El fin de esto es que se pueda reestablecer los servicios con los que cuenta la empresa para que la información no pueda ser comprometida, corrupta o manipulada en alguno de los procesos, así solucionar de manera rápida y efectiva logra evitar cualquier inconveniente y el proceso de envío de correspondencia fluya normalmente. Los jefes operativos y de sistemas suministran dichos planes, los desarrollan y los presentan a la alta gerencia para obtener los avales, así cuando deban entrar en acción las diferentes áreas de la empresa sabrán que realizar en caso de cualquier novedad de seguridad.
			Solución: Política de Continuidad en las Operaciones (Ver Anexo A Numeral 1.2.2).
A.17.1.2	Implementación de la continuidad de la seguridad de la información	SI	Este control implementa lo planeado en el apartado A.17.1.1. Establece una gestión adecuada para mitigar y responder ante cualquier eventualidad en los procesos de seguridad. Así mismo se asignan los roles y se determinan responsabilidades en cada área para que sepan que hacer en caso de algún incidente o problema de seguridad identificado, con ello se logra que la continuidad del negocio no se vea afectada drásticamente y los servicios de la empresa continúen debidamente. Los jefes operativos y de sistemas están al tanto de ello, son quienes deben monitorear cualquier evento que se presente y también colaborar en la resolución de los problemas de seguridad encontrados.
			Solución: Política de Continuidad en las Operaciones (Ver Anexo A Numeral 1.2.2).
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SI	Tras la implementación de los planes de continuidad de seguridad de la información, se debe efectuar análisis de cómo estos han funcionado, si existen mejoras que hacer o si se debe cambiar la forma de ejecución, así se debería hacer de nuevo una planeación que modifique la forma de cómo se están realizando dichos planes. Así mismo sin necesidad de que

			se presenten inconvenientes hay que efectuar pruebas para diagnosticar el funcionamiento de los planes, los ensayos deben ser requisitos para identificar falencias o verificar que se ha establecido correctamente los planes y van por buen camino. Los jefes operativos y de sistemas son los que deben liderar esta parte, efectuar análisis y dar los resultados para saber en qué se debe mejorar.
			Solución: Política de Continuidad en las Operaciones (Ver Anexo A Numeral 1.2.2).
A.17.2	Redundancias **Objetivo:** Asegurar la disponibilidad de instalaciones de procesamiento de información.		
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	SI	De acuerdo al dominio actual, se debe tener un correcto funcionamiento de los planes de continuidad de seguridad de la información y para ello es indispensable que los servicios de infraestructura tengan la disponibilidad adecuada para el procesamiento de la información. La redundancia confirma que las instalaciones deban siempre estar en funcionamiento y que si hay algún problema debe saberse sobrellevar, es el caso de tener plantas eléctricas o cualquier equipo que solucione los temas de electricidad, esto como un ejemplo.
			Solución: Política de Continuidad en las Operaciones (Ver Anexo A Numeral 1.2.2).
A.18	CUMPLIMIENTO		
A.18.1	Cumplimiento de los requisitos legales y contractuales **Objetivo:** Evitar el incumplimiento de las obligaciones legales, estatuarias, de reglamentación o contractuales relacionadas con la seguridad de la información y de cualquier requisito de seguridad.		
A.18.1.1	Identificación de la legislación aplicable a los requisitos contractuales	SI	Para que las organizaciones funcionen correctamente y sobretodo legalmente debe tener todos sus documentos en orden, licencias al día, registros ante el gobierno, etc. Cualquier tipo de negocio con proveedores o la adquisición y disposición de servicios debe estar bajo la ley. Es algo obligatorio para funcionar como organización cumplir los requisitos legales y contractuales que la ley determina, es por ello que la empresa HECC COURRIER a día de hoy cumple con todo lo estipulado por la ley.
			Solución: Política General de Seguridad de la Información determina las sanciones al incumplimiento de los requisitos de seguridad.

A.18.1.2	Derechos de propiedad intelectual	NO	La empresa actualmente no tiene desarrollos o equipos que deban estar registrados como propiedad intelectual. No se plantea en el futuro realizarlos.
A.18.1.3	Protección de registros	SI	Los registros deben estar protegidos, la información debe ser enviada de manera segura por todos los canales de comunicación existentes. La encriptación de las claves da un nivel de seguridad alto para proteger adecuadamente la información que se manipula. Las bases de Datos deben tener una protección segura de acuerdo a los niveles de clasificación de la información, así como la información física que se maneja.
			Solución: Política de Gestión de Activos (Ver Anexo A Numeral 1.2.3) y Política General de Protección de Datos HECC COURRIER (Ver Anexo A Numeral 1.2.15).
A.18.1.4	Privacidad y protección de información de datos personales	SI	Es deber de la empresa mantener la privacidad de la información que maneja de sus clientes, sus datos personales y la información que se envía en el proceso de correspondencia debe estar protegida y salvaguardada para evitar que agentes externos puedan obtenerla, manipularla y modificarla. Los clientes confían en la empresa y entienden la forma en que sus envíos van a llegar al destinatario. La empresa debe determinar una política para este control, ya que es información sensible que la ley está al tanto de ello y por la cual la empresa debe responder y en caso de no hacerlo deberá cumplir con las sanciones impuestas.
			Solución: Política de Gestión de Activos (Ver Anexo A Numeral 1.2.3) y Política General de Protección de Datos HECC COURRIER (Ver Anexo A Numeral 1.2.15).
A.18.1.5	Reglamentación de controles criptográficos	SI	Existen claves criptográficas dentro de los procesos de envíos de correspondencia, esta debe estar reglamentada para que los servicios funcionen correctamente y tengan un nivel de seguridad alto. Al existir dicha reglamentación debe continuar con el proceso de mejora y buscar maneras para que dichos controles funcionen igual o mejor si es posible.
			Solución: Política de Controles Criptográficos (Ver Anexo A Numeral 1.2.8).
A.18.2	Revisiones de seguridad de la información **Objetivo:** Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.		

A.18.2.1	Revisión independiente de la seguridad de la información	SI	Actualmente la organización no efectúa auditorías internas. Es necesario realizar auditorías internas para medir el funcionamiento de los procesos, procedimientos y sistemas de seguridad. Tener revisiones periódicas de ello para que los empleados estén preparados y puedan efectuar las correcciones a tiempo para que al efectuar una auditoria externa no se presenten los mismos inconvenientes y se detecten fallas en los procesos. Cada auditoria interna debe documentarse, los registros encontrados deben estar plasmados para que los jefes operativos y de sistemas puedan efectuar cambios en los procesos si son necesarios o hacer recomendaciones a los empleados en su forma de ejecutar los procedimientos de seguridad.
			Solución: Política de Continuidad en las Operaciones (Ver Anexo A Numeral 1.2.2).
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	SI	Al no haber políticas de seguridad en la empresa no se cumple el control definido. Por eso es necesario el desarrollo e implementación de las políticas, así se puede tener auditorias y revisiones de los procesos que allí se deberán describir. Teniendo en cuenta esto, se efectúan las evaluaciones correspondientes, verificando los procesos que cumplen con la normativa y los cuales deberían modificarse o mejorarse para que en el siguiente periodo de evaluación se puedan obtener resultados satisfactorios de las políticas de seguridad de la información.
			Solución: Política de Continuidad en las Operaciones (Ver Anexo A Numeral 1.2.2).
A.18.2.3	Revisión del cumplimiento técnico	SI	Actualmente no hay forma de efectuar una revisión del cumplimiento técnico al no tener desarrolladas las políticas de seguridad de la empresa. Por eso al realizarlas e implementarlas hay que tomar intervalos de tiempo para realizar su análisis correspondiente y desarrollar pruebas o test que permitan verificar el funcionamiento de la seguridad, como por ejemplo hackeos internos, intentos de penetración a los sistemas, etc. Todo esto con el fin de que los empleados a cargo de las áreas y de verificar, solucionar y corregir los incidentes o eventos encontrados puedan determinar cómo al implementar las políticas estas fueron de utilidad o hay que adicionar más requisitos para que la falla sea mitigada de inmediato.
			Solución: Política de Continuidad en las Operaciones (Ver Anexo A Numeral 1.2.2).

Tabla 20. Análisis de Controles aplicables

Fuente: Los Autores

Después de haber realizado el análisis correspondiente a los controles del Anexo A de la ISO 27001:2013, se ha determinado realizar una tabla asociando los riesgos identificados durante el proyecto junto a su dominio correspondiente:

No Riesgo	Riesgo	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18
1	Riesgos de Fraude o Corrupción.	X	X	X	X	X		X	X	X			X	X	
2	Riesgos con el recurso humano.	X		X					X	X					
3	Riesgos Operativos y de procesos	X		X					X					X	
4	Riesgo de contratación externa	X				X						X			X
5	Riesgos Tecnológicos y de Infraestructura	X			X	X	X	X		X			X	X	X
6	Riesgos de Información	X			X	X			X	X					
7	Riesgos externos, (de entorno)	X			X			X					X	X	
8	Riesgos Naturales, ambientales y antrópicos	X			X									X	
9	Riesgos legales o regulatorios	X	X											X	X
10	Riesgos de Acceso	X				X			X						X
11	Riesgos Estratégicos	X							X					X	X

Tabla 21. Asociación de riesgos con los controles ISO 27001:2013. Fuente: Los Autores

5. POLÍTICAS DE SEGURIDAD

La norma ISO/IEC 27001 establece que se deben crear políticas basado en los controles que se deben implementar para tal fin, se establece una Política de la Seguridad de la Información, como marco de trabajo de la organización en lo referente al uso adecuado de los recursos tecnológicos, buscando niveles adecuados de protección y resguardo de la información, definiendo sus lineamientos, para garantizar el debido control y minimizar los riesgos asociados.

En el "**Anexo A: Políticas de Seguridad de la Información**" (Disponible en el CD) se ha detallado cada una de las políticas que se han desarrollado de acuerdo a todo el análisis de gestión de riesgos, vulnerabilidades y amenazas.

6. GUÍA DE IMPLEMENTACIÓN

De acuerdo a las políticas de seguridad de la información y a la gestión de los riesgos detallados anteriormente, se ha determinado realizar una guía de implementación como sugerencia para implementar el presente sistema de gestión de seguridad de la información descrito. Los autores han efectuado un análisis que permite describir los pasos que la empresa HECC COURRIER debería efectuar para que este diseño SGSI sea efectivo.

Teniendo en cuenta la gestión de los riesgos y la valoración de cada uno de ellos se ha realizado una gráfica que determina cuales deberían ser los que necesitan ser tratados prioritariamente. Identificando la escala de valoración se ha determinado que el Riesgo R1 (Riesgos de Fraude o Corrupción.) como de alto impacto y por el cual encabeza la lista. Aunque algunos riesgos sean demasiado importantes hay que tener en cuenta otra variable como lo es el tiempo de ejecución que este conlleve para realizar.

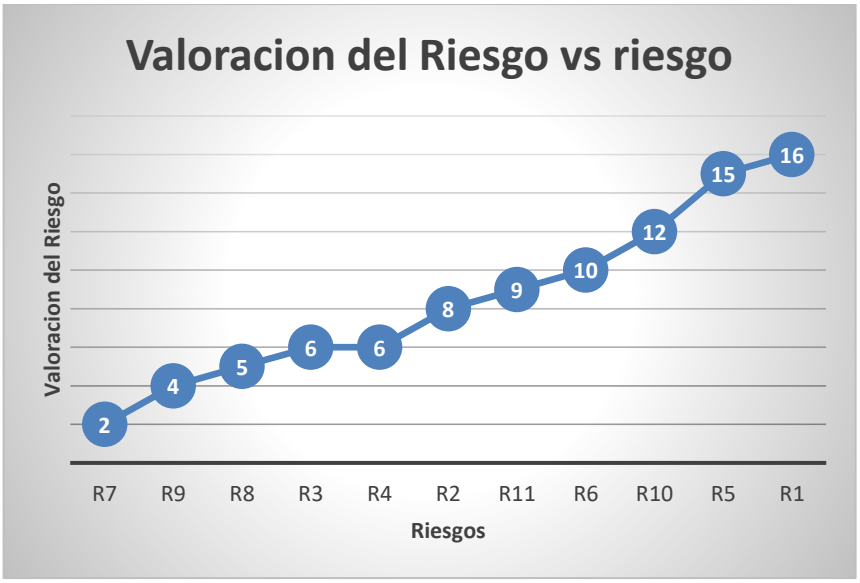


Ilustración 8. Valoración del Riesgo vs Riesgo
Fuente: Los Autores

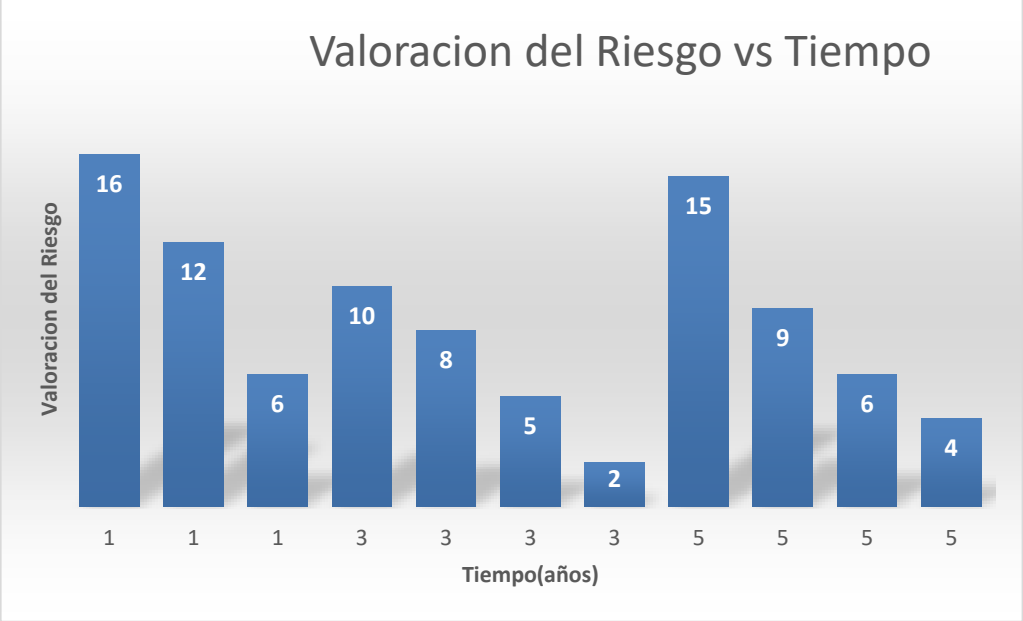


Ilustración 9. Valoración del Riesgo vs Tiempo
Fuente: Los Autores

De acuerdo a las gráficas se creará la guía de implementación abarcando primero la mitigación de los riesgos con valoración más alta pero que llevan menos tiempo de implementación. Se aclara que la guía de implementación es el paso a seguir después establecer y hacer cumplir las políticas antes mencionadas, la guía es complemento y sustento de las políticas desarrolladas. Partiendo del principio que lo primero que se debe hacer es desarrollar las normas y directrices que se mencionan en las políticas.

La guía de Implementación se ha detallado en el "**Anexo B: Guía de Implementación**" (Disponible en el CD) donde se ha descrito cada uno de los pasos a realizar para tener un óptimo proceso de seguridad de la información.

7. MÓDULO WEB

Como valor agregado del presente Proyecto se escogió la propuesta de realizar un módulo web que pudiera gestionar el control de incidentes durante el proceso de implementación de las políticas de seguridad. Este módulo web es un desarrollo establecido por los autores como solución tecnológica para la serie de documentos que se realizaron durante el proyecto, con ello la empresa HECC COURRIER tendrá la capacidad de gestionar sus incidentes, determinar los usuarios o grupos de trabajo a quienes se les asigne realizar las pertinentes acciones para solucionar dichos inconvenientes y por supuesto tener una base de conocimientos capaz de proveer soluciones a temas que ya se hayan solventado efectivamente.

Para efectuar este módulo web para la gestión de control de incidentes se pensó en metodologías agiles de desarrollo que pudieran efectuarse rápidamente y por supuesto que permitiera trabajar estructuradamente obteniendo los resultados esperados. Teniendo en cuenta que lo más importante para el diseño de un sistema de gestión de seguridad de la información es definir las políticas de seguridad de la empresa, así como también su guía de implementación, se determinó un tiempo corto de trabajo para este módulo web, por ello se definió el uso de la metodología RAD (Desarrollo Rápido de Aplicaciones) con la cual se ajustaba por tiempos y por estructura un desarrollo efectivo, ágil y rápido.

En el "**Anexo C: Desarrollo del Módulo Web**" (Disponible en el CD) se ha detallado la metodología RAD efectuada y todo el proceso necesario para implementar adecuadamente dicho desarrollo.

8. CONCLUSIONES

- La identificación y diagnóstico de las amenazas y vulnerabilidades permitió verificar el grado de seguridad con el que la empresa HECC COURRIER se encontraba en el momento de su análisis. Al no tener definidas unas políticas de seguridad, sus activos se encontraban expuestos a cualquier tipo de afectación que se pudiera presentar, que de ocurrir esto hubiera sido catastrófico para el funcionamiento normal de la empresa al demostrar el alto impacto con el que los activos se verían afectados.

- El análisis de riesgos de seguridad determinó los altos niveles de impacto con que los procesos de la empresa pueden verse afectados, así mismo la probabilidad media de que dichos riesgos puedan presentarse. Teniendo esta información se pudo comprender los controles del anexo A de la norma ISO27001 que deben aplicarse para reducir los niveles de impacto en los activos de la entidad, ya que riesgos de fraude o corrupción y tecnológico y de infraestructura tienden a afectar la continuidad del negocio de manera catastrófica.

- Se elaboraron las políticas de seguridad de la empresa teniendo en cuenta el análisis de la gestión de los riesgos gracias a la identificación de los niveles de impacto y probabilidad de ocurrencia de los riesgos. En estas políticas se describen en detalle el propósito por lo cual se debe implementar, el alcance de la política, los responsables de que se cumpla y por supuesto la explicación de cómo debe ejecutarse para mantener los niveles de seguridad apropiados para proteger la confidencialidad, disponibilidad e integridad de la información de HECC COURRIER.

- Con base en lo establecido por las políticas de seguridad de la empresa se logró definir una guía de implementación que permite estructuralmente desarrollar los ítems de acuerdo al criterio de los autores definidos por escalas de valoración de impacto y tiempo con respecto a los riesgos identificados. Esta guía se debe tomar como sugerencia para desarrollarse, no es de carácter obligatorio para la empresa seguir la estructura definida.

- El módulo web para gestionar el control de incidentes se ha desarrollado de acuerdo a los requisitos establecidos utilizando metodologías de desarrollo rápido y ágil, así como frameworks como Laravel para que pudiera ser estructurado y escalable. Hay que destacar que como valor agregado al SGSI, la empresa HECC COURRIER podrá contar con un sistema amigable y fácil de usar para dicho control de incidentes.

9. RECOMENDACIONES

- Principalmente se recomienda a la empresa HECC COURRIER implementar el presente Sistema Gestión de Seguridad de la Información para que los activos que tienen dentro de la organización tengan el tratamiento adecuado y no se vean afectados de sobre manera en su funcionamiento diario. Así mismo se recomienda a los empleados de la empresa en todas sus áreas seguir las normas y lineamientos que se establecen en las políticas de seguridad, de igual forma seguir paso a paso la guía de implementación.

- Es necesario hacer efectiva la implementación del Sistema de Gestión de Seguridad de la Información para poder iniciar a un proceso auditor en la empresa que conlleve a realizar en algunos procesos la certificación de la ISO 27001, con ello la empresa ganará credibilidad en el sector, brindará confianza a sus clientes y podrá mejorar no solo en la parte de seguridad sino en un tema económico, ya que los procesos podrían funcionar de una mejor manera aumentando la productividad y ganancias de paso.

- Aunque el presente trabajo haya hecho un análisis exhaustivo de los procesos de la empresa, con enfoque en el proceso de correspondencia, es clave destacar que HECC COURRIER debería darle más interés en los temas de seguridad de la información, efectuar capacitaciones e informarse de una mejor manera, para así complementar el presente SGSI con algunos procesos que en un futuro vayan a desarrollar.

- Aunque el modulo web para gestionar el control de incidentes no solo se enfoca en ello y tiene módulos para gestionar usuarios, enviar mensajes y administrar grupos de trabajo, se recomienda que se amplíe la funcionalidad agregando nuevos módulos que vean pertinentes para la implementación de la guía o de procesos que estén actualmente dentro de la empresa. El modulo web actualmente permite que sea escalable aprovechando el manejo que hace Laravel con su modelo MVC, de allí que se permita la adición de módulos para la empresa HECC COURRIER y su gestión de procesos.

10. BIBLIOGRAFÍA E INFOGRAFÍA

- Calder, Alan. (2017). ISO 27001-ISO27002: Una guía de bolsillo. Reino Unido. IT Governance Publishing.
- Alexander, Alberto G. (2007). Diseño de un sistema de gestión de seguridad de información (Spanish Edition). AlfaOmega.
- Andres, Ana. Gomez, Luis. (2009). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. España. AENOR.
- ICONTEC. (2006). Norma Técnica NTC-ISO/IEC colombiana 27001. Colombia. ICONTEC.
- Ministerio de Tecnologías de la Información y Comunicaciones de Colombia. Sistemas de Gestión de Seguridad de la Información SGSI. 2017. Colombia. Recuperado de http://www.mintic.gov.co/gestionti/615/w3-article-5482.html
- Advisera. ¿Qué es la Norma ISO 27001?. 2017. Recuperado de https://advisera.com/27001academy/es/que-es-iso-27001/
- El Portal de ISO27001 en español. Que es un SGSI. Julio 2015. Recuperado de http://www.iso27000.es/sgsi.html
- Blog especializado en Sistemas de Gestión de Seguridad de la Información. Julio 2015. Que es SGSI. 2017. Recuperado de http://www.pmg-ssi.com/2015/07/que-es-sgsi/
- Duque Ochoa Blanca Rubiela. Metodologías de Gestión de Riesgos (Octave, Magerit, Dafp). 2017. Recuperado de https://auditoriauc20102mivi.wikispaces.com/file/view/Metodolog%C3%ACas+deGesti%C3%B2n+de+Riesgos.pdf
- Agenda ISOTools Excelence. Metodología para realizar el diseño e implementación de un SGSI basado en la norma ISO 27001:2013 e ISO 27002:2013. 2017. Recuperado de https://www.isotools.org/evento/metodologia-implementacion-sgsi-pe7ago/
- Sanchez Moreno, Yuli Paola. 2014. Ciclo PHVA. 2017. Recuperado de https://www.gerencie.com/ciclo-phva.html
- ISOTools Colombia. Mayo 2016. OHSAS 18001: La importancia del ciclo PHVA (Planificar-Hacer-Verificar-Actuar). 2017. Recuperado de http://www.isotools.com.co/ohsas-18001-la-importancia-del-ciclo-phva-planificar-hacer-verificar-actuar/
- Meneses, Alexander. Camargo, Alberto. Febrero 2017. Diseño Del Sistema De Gestión De Seguridad De La Información Sgsi Basado En El Estándar Iso 27001, Para Los Procesos Soportados Por El Area De Sistemas En La Cámara De Comercio De Aguachica, Cesar. 2017. Recuperado de http://repositorio.ufpso.edu.co:8080/dspaceufpso/handle/123456789/1434
- Avella, Julian. Calderon, Leonardo. Mateus, Cristian. Guía metodológica para la gestión centralizada de registros de seguridad a través de un siem.

Universidad Catolica de Colombia. 2015. Recuperado de: http://repository.ucatolica.edu.co/bitstream/10983/2847/1/GU%C3%8DA%20METODOL%C3%93GICA%20PARA%20LA%20GESTI%C3%93N%20CENTRALIZADA%20DE%20REGISTROS%20DE%20SEGURIDAD%20A%20TRAV%C3%89S%20DE%20UN%20SIEM.pdf

- Acosta, David. Controles técnicos de PCI DSS parte VI: Registro de eventos (logs). PCI Hispano. 2016. Recuperado de: https://www.pcihispano.com/controles-tecnicos-de-pci-dss-parte-vi-registro-de-eventos-logs/
- Rouse, Margareth. Gestión de eventos e información de seguridad (SIEM). Search DataCenter en Español. 2017. Recuperado de: http://searchdatacenter.techtarget.com/es/definicion/Gestion-de-eventos-e-informacion-de-seguridad-SIEM

11. ANEXOS

Los anexos desarrollados durante el presente proyecto “DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA EMPRESA HECC CURRIER BASADO EN ISO 27001” se muestran a continuación:

- Anexo A: Políticas de Seguridad
- Anexo B: Guía de Implementación
- Anexo C: Modulo Web
- Anexo D: Diccionario de Datos
- Anexo E: Manual de Usuario

Todos estos anexos se encuentran detallados en cada uno de los archivos que se encuentran en el CD.