RESGUARDAR LA INFORMACIÓN DEL SISTEMA DE GESTIÓN DOCUMENTAL DOCUNET EN LA EMPRESA CONTACTAR - PASTO

MARIO ANDRES CHAVES ROSERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”

ESPECIALIZACION EN SEGURIDAD INFORMATICA

BOGOTA D.C.

2017

RESGUARDAR LA INFORMACIÓN DEL SISTEMA DE GESTIÓN DOCUMENTAL DOCUNET EN LA EMPRESA CONTACTAR - PASTO

MARIO ANDRES CHAVES ROSERO

Proyecto de Grado

Metodología para el Aseguramiento de la información del Sistema de Gestión Documental Docunet en la empresa CONTACTAR - Pasto

Director: Martin Camilo Cancelado Ruiz

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”

ESPECIALIZACION EN SEGURIDAD INFORMATICA

BOGOTA D.C.

2017

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

San Juan de Pasto, 26 de Julio de 2017

DEDICATORIA

Dedicado a en primer lugar a Dios quien es el que me ilumina y bendice todos los días en todo lo que realizo, me da la fuerza para seguir adelante, a mi familia por el apoyo y el estar pendientes de mi desarrollo como profesional, a las personas que me alentaron a seguir estudiando y prepararme para lograr muchos éxitos personales y profesionales.

AGRADECIMIENTOS

Agradezco a mi familia en especial a mis padres quienes siempre me apoyaron en los proyectos a realizar tanto personales como profesionales y siempre conté con todos sus buenos consejos y estar presentes en todo momento como guías incondicionales, a mis hermanos quienes se preocuparon porque siguiera adelante con mis estudios profesionales y alcanzar cada uno de mis objetivos en el entorno laboral como profesional.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

RESUMEN

Un sistema de gestión documental es una aplicación o herramienta la cual permite el tratamiento, conservación, publicación y trabajo sobre documentos electrónicos, y estructura de directorios de cada uno de los procesos que se manejan en una empresa (ya sean documentos escaneados o que se hayan creado originalmente en digital). Dentro del entorno de la red se debe asegurar la privacidad de la información y de proteger las operaciones de daños no intencionados como deliberados**.**

La aplicación de nuevas tecnologías, la gestión de los documentos y del conocimiento hace necesario la protección de esta información y la estabilidad del sistema de gestión documental, en cuanto a software, hardware y acceso por parte del administrador del sistema como de los usuarios.

Palabras clave: Riesgos, amenazas, metodologías, seguridad, gestión documental, confidencialidad, integridad, disponibilidad, sistemas de información.

INTRODUCCIÓN

Un Programa de Gestión Documental es un proceso estratégico de largo plazo que busca dar las bases técnicas, administrativas, tecnológicas y normativas necesarias para el adecuado manejo de la documentación que soporta los procesos esenciales, de apoyo y verticales de la compañía, facilitando la consulta, conservación y generación de conocimiento, para mejorar la toma de decisiones y el servicio al cliente.

Las principales actividades de la Gestión Documental son:

- Producción
- Recepción
- Distribución
- Conservación
- Organización
- Consulta y Recuperación
- Trámite
- Disposición Final

La metodología para la Implementación en la seguridad del Sistema de Gestión Documental involucra un componente de consultoría que busca lograr un conocimiento sobre la compañía, el negocio, sus dinámicas, flujos, visión prospectiva y diferentes aspectos de la cultura organizacional. Todo lo anterior con el objetivo de implementar el Sistema de Gestión Documental de una manera transparente que permita una apropiación más sencilla sin que se afecte la operación diaria de la compañía y buscando generar una menor resistencia al cambio por parte de los usuarios de la información y del sistema.

Con el presente proyecto se busca establecer una metodología para resguardar la información del sistema de gestión documental en la empresa Contactar, teniendo como referencia las diferentes técnicas, herramientas y estándares que se encuentran en el medio tecnológico para llevar a cabo la implementación de gestión de seguridad de la Información lo cual, permite garantizar su efectiva implementación y asegurar su debida permanecía y evolución a futuro.

1. DESCRIPCIÓN DEL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

Cómo resguardar un sistema de gestión documental y la información que existe para mantener un sistema estable y proteger la información que se encuentra relacionada en este sistema aplicando los nuevos estándares y tecnologías que se encuentran en el medio informático.

Debido a los diferentes riesgos y amenazas que se generan por el cambio constante en las nuevas tecnologías de la información, es necesario que las organizaciones cuenten con una estrategia o planes de seguridad basado en los riesgos y alineados con las necesidades de la razón de ser del negocio, con el objetivo de contar con un modelo de la Seguridad de la Información en aspectos como la seguridad de la infraestructura que se utiliza en lo que respecta a asegurar que nadie puede acceder a los documentos si no es a través del programa o servicios correspondientes. La gestión de acceso, protección de la confidencialidad, integridad y disponibilidad del sistema, recursos para garantizar que sólo los usuarios autorizados pueden acceder o modificarlos. Implementar políticas y planes de gestión de seguridad de la información. La Gestión de Seguridad de la Información es fortalecer integralmente en la empresa, los pilares fundamentales de la seguridad correspondiente a la Integridad, Confidencialidad y Disponibilidad de la información y garantizar con esto la debida protección de la información y la privacidad de la información de cada una de sus áreas y de sus partes interesadas.

1.2. FORMULACIÓN DEL PROBLEMA

¿Cómo resguardar la información del Sistema de gestión documental Docunet en la empresa Contactar Pasto?

2. JUSTIFICACIÓN

La información se posiciona como uno de los elementos más importantes en las organizaciones, lo cual conlleva a contar con herramientas que les permitan acceder de una manera ágil y eficiente a la gran cantidad de datos que se generan en el día a día y que se articulan como la base para el desarrollo de las diversas actividades que conforman el que hacer de la organización. Dentro de este ambiente, los Sistemas de Gestión Documental cumplen un papel muy destacado al permitir manejar de una forma ordenada y automatizada los diversos tipos de información ya sean electrónicos y físicos a través de las diferentes funcionalidades que presentan estos sistemas los cuales permiten administrar y proteger la información.

Hoy en día las empresas deben considerar dentro de sus planes estratégicos el aseguramiento de la información generando políticas y controles bien sea en busca de garantizar la continuidad del negocio o certificarse frente a otras empresas. La empresa Contactar debe tomar conciencia de la necesidad y se debe alinear sus objetivos institucionales, asegurar el flujo de información, optimizar recursos y garantizar la confidencialidad, disponibilidad e integridad de la misma. Este es uno de los desafíos que debe tomar la empresa para estar acorde a los modelos y estándares actuales, para ello es necesario empezar con la ejecución del análisis de riesgos de la seguridad del sistema de información con el fin de garantizar mayor efectividad y eficiencia dentro de cada uno de los procesos, teniendo en cuenta que al conocer las fortalezas y debilidades se mejora el control y administración de recursos tecnológicos y así proporcionar mecanismos y herramientas para adoptar buenas prácticas de seguridad y lograr objetivos institucionales.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Realizar el análisis del Sistema de Gestión Documental Docunet de la empresa Contactar Pasto a través de nuevas metodologías, lineamientos e instrumentos archivísticos así como tecnologías controles y mecanismos para garantizar la seguridad de la información y componentes del sistema.

3.2. OBJETIVOS ESPECÍFICOS

- ✓ Fortalecer la seguridad y el nivel de tecnología en los sistemas de información de la Empresa Contactar Pasto
- ✓ Establecer lineamientos para la administración, creación, almacenamiento, recuperación, consulta y custodia de la información del sistema de gestión documental
- ✓ Generar políticas de seguridad apropiadas que permitan garantizar la seguridad de la información, el acceso rápido y selectivo a los datos aplicando modelos y estándares establecidos

4. ALCANCE Y DELIMITACIÓN DEL PROYECTO

Este trabajo presenta un análisis, recomendaciones y diseño de una solución para la seguridad de información del Sistema de Gestión Documental Docunet en la empresa Contactar Pasto. El Sistema de Gestión documental está orientado al apoyo o soporte de actividades que realizan las diferentes áreas de la empresa como las siguientes: Radicación, trámite y trazabilidad de las comunicaciones oficiales que se producen en la empresa tanto interna como externa, envío de correos internos a través del sistema de gestión documental. Creación de documentos según la estructura definida en la Tabla de retención documental de cada una de las áreas con sus respectivos archivos adjuntos para su consulta. Brindar a apoyo en la seguridad de la información a través de la estandarización de políticas en los procesos que pueden afectar la integridad, confidencialidad y disponibilidad de la información. Estas políticas se aplican a procesos y procedimientos del sistema de gestión documental a los siguientes elementos: Repositorio de información, clasificación de seguridad del documento, Backups, Credenciales de acceso privilegios de acceso a la información, Servidor de almacenamiento. Para el desarrollo del proyecto se utilizará como guía principal la norma NTC-SGSI basado en ISO27000 e ISO27001, Gestión del riesgo informático, que corresponde a un estándar referente a nivel mundial que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información. Los cual permite definir la funcionalidad del sistema de gestión documental, definiendo el correcto uso y sincronización de las herramientas, tecnologías y estándares utilizados.[1]

[1] ISO 27001: El papel de la alta dirección en un SGSI, https://www.isotools.org/2015/02/04/iso-27001-papel-alta-direccion-sgsi/

5. MARCO REFERENCIAL

5.1. MARCO CONTEXTUAL

5.1.1. Historia de Contactar

La IMF colombiana Contactar (Corporación Nariño Empresa y Futuro) fue creada en 1991. Sus más de 20 años de experiencia en microcréditos para las zonas rurales del sureste de Colombia le permiten lograr un sólido alcance rural. Contactar opera a través de una red de 21 sucursales en los departamentos de Nariño y Putumayo. Corporación Nariño Empresa y Futuro (Contactar) tiene más de 20 años de experiencia en el sector de las micro finanzas, con foco específico en la financiación de actividades agrícolas en áreas rurales (desde hace más de 10 años). En los últimos años se abrieron varias oficinas nuevas, con lo cual la red llegó a 52 oficinas.

Contactar ha adquirido una buena posición rural en las regiones suroeste y central de Nariño, Putumayo, Huila y Tolima. La institución tiene claros objetivos financieros y sociales que persiguen un resultado neto triple. En 2013, Contactar lanzó varios productos nuevos con fuertes componentes sociales y ecológicos; por ejemplo, tiene un programa específico sobre conciencia ambiental y ofrece actividades de asistencia técnica para clientes rurales con un claro enfoque ambiental. Además de su presencia en las zonas rurales, también financia las actividades de producción rural. Contactar atiende a sus clientes mediante préstamos individuales y grupales solidarios, créditos asociativos y banca comunitaria.[2]

Objetivos de la empresa Contactar

Contribuir con el mejoramiento de las condiciones de vida de nuestros clientes

[2] Historia CONTACTAR, http://www.contactar-pasto.org/index.php/microcreditos-conocenos-contactar

Generar conocimiento en los clientes para mejorar la toma de decisiones (financieras, económicas productivas, sociales y ambientales).

Desempeño social y ambiental:

Taller de educación financiera, Fondos auto gestionados de ahorro y crédito,

Taller en prácticas de agricultura sostenible, jornadas de promoción de la salud

Valores: Lealtad, Integridad, Profesionalismo, Solidaridad

Principios: Compromiso, Efectividad, Calidez, Transparencia

5.1.2. Misión

Prestamos servicios micro financieros inclusivos e integrales con calidad, calidez, responsabilidad social y ambiental, a poblaciones prioritariamente rurales, para contribuir a mejorar sus condiciones de vida.[3]

5.1.3. Visión

Contactar será modelo empresarial de micro finanzas prioritariamente rurales con desempeño social y ambiental en Colombia.[4]

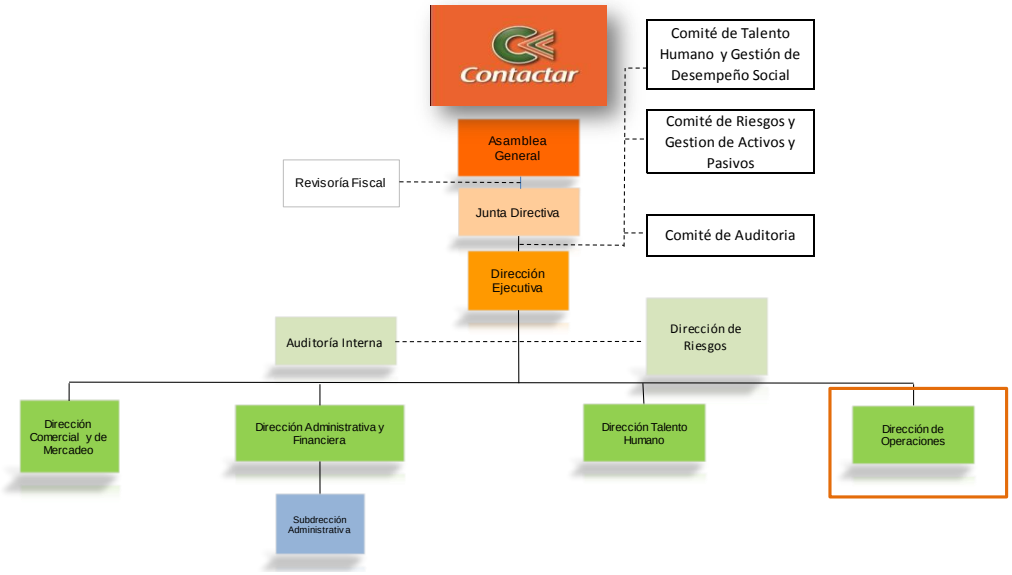
[3] Misión, Tomado de Actas Junta Directiva CONTACTAR
[4] Visión, Tomado de Actas Junta Directiva CONTACTAR

Figura 1 Instalaciones Corporación Nariño Empresa y Futuro- CONTACTAR

Fuente: Subdirección Administrativa CONTACTAR.

5.1.4. ESTRUCTURA ORGANIZACIONAL

Figura 2 Organigrama CONTACTAR



Fuente: Subdirección Administrativa CONTACTAR

5.1.5. DESCRIPCION SISTEMA DE GESTION DOCUMENTAL

Docunet es una solución de GESTION DOCUMENTAL para la gestión electrónica de los documentos, cuenta con una característica y/o fortaleza diferenciadora frente a otros software del mercado: está basado en la normatividad emitida por el Archivo General de la Nación (Ley 594 del año 2.000 del AGN) la cual es de uso obligatorio para entidades públicas, privadas que cumplen funciones públicas y las vigiladas por la Superintendencia de Industria y Comercio[5]

Docunet cuenta con las mejores prácticas para los procesos archivísticos, que pueden ajustarse de forma eficiente a los procesos de las organizaciones de cualquier sector y tamaño.

DOCUNET Cuenta con Tres Módulos:
Archivo

- ✓ Administración y gestión de la información de acuerdo a las TRD y TVD, Transferencias primarias y secundarias, seguridad de la información y reportes.
- ✓ Digitalización, consulta de imágenes e integración con diferentes sistemas propios del negocio de nuestros clientes.
- ✓ Reconocimiento óptico de caracteres OCR.
- ✓ Indexación masiva de Documentos.
- ✓ Prestamos Documentales.
- ✓ Módulo de Importación de Imágenes.

Trámite de Correspondencia y Workflow

- ✓ Implementación Ventanilla Única: Radicación, distribución y manejo de correspondencia entrante y saliente, Código de Barras.

- ✓ WorkFlow nivel 1 (Manual), 2 (Automático), 3 (toma decisiones): Automatización del flujo de Procesos de Registro, permite distribuir la asignación de actividades basados en las cargas de trabajo de los funcionarios involucrados en diferentes áreas y procesos de la organización.
- ✓ Control y seguimiento de tareas y actividades.
- ✓ Sistema de mensajería propio con alertas escalables automáticas.
- ✓ Integración con correos IMAP Y POP.
- ✓ Análisis de procesos.
- ✓ Trazabilidad de la gestión de la documentación.[5]

Normas y Procedimientos:

- ✓ Control de documentación de los sistemas de gestión de calidad.
- ✓ Estructuración de procedimientos por pasos para cada proceso con responsable y tiempos.
- ✓ Control y divulgación de los procedimientos de la organización.
- ✓ Control de listas de distribución, terminología y condiciones generales.
- ✓ Control de versión de documentos y copias controladas.

Otras Características:

- ✓ Múltiples repositorios de Imágenes.
- ✓ Biblioteca.
- ✓ Módulo de Importación de Imágenes.
- ✓ Firmas digitales, Estampado Cronológico.
- ✓ Marca de Agua.
- ✓ Webservices, integraciones con otros aplicativos.
- ✓ Visor de Imágenes.
- ✓ Reportes.

[5] Docunet sistema de gestión Documental , http://innova.com.co/docunet/

5.2. MARCO LEGAL

Cuando se quiere implementar un SGSI, se debe estructurar un Modelo Normativo que incluya cada uno de los dominios de la ISO 27001 e ISO 27002, los cuales pueden ser incluidos por ejemplo, en el Manual de Seguridad que se desarrolle en la implementación del SGSI.

Este modelo normativo puede estructurarse documentando una política por cada dominio, y normas que complementen a la política y que reúnan los objetivos de control que exista en la ISO 27002, para cubrir completamente lo incluido en esta Norma.

5.2.1 La Ley 594 de 2000 en su Artículo 22. Procesos Archivísticos. Establece que la gestión de documentos dentro del concepto de Archivo Total, comprende procesos tales como la producción o recepción, la distribución, la consulta, la organización, la recuperación y la disposición final de los documentos[6].

5.2.2 Acuerdo AGN 060 de 2001 Artículos 4, 6, 9 y 14. Pautas para la administración de comunicaciones oficiales en las entidades públicas y privadas que cumplen funciones públicas. Circular Interna AGN No.13 de 1999, No se deben utilizar micropuntas o esferas de tinta húmeda. NTC 2676 Durabilidad soportes, aplicable a los soportes digitales. “Cartuchos de disco flexible de 90 mm. (3.5 pulgadas), características dimensionales, físicas y magnéticas”. NTC 4436 “Papel para documentos de archivo: requisitos para la permanencia y durabilidad”

Radicación de documentos Asignación de un número consecutivo a los documentos en los términos establecidos en el artículo 2 del Acuerdo AGN 060 de 2001, dejando constancia de[6]

[6] Archivo General de la Nación, normatividad, http://www.archivogeneral.gov.co/normatividad/

la fecha y hora de recibo o de envío. Registro impreso de planillas de radicación y control. Decreto 1382 de 1995. Obligatoriedad de la presentación de las T. R .D.

5.2.3 Acuerdo AGN 042 de 2002. Por el cual se establecen los criterios para la organización de los archivos de gestión en las entidades públicas y las privadas que cumplen funciones públicas, se regula el Inventario Único Documental y se desarrollan los artículos 21, 22, 23 y 26 de la Ley General de Archivos, Ley 594 de 2000. Circular AGN 01 de 2003. Organización y Conservación de los documentos de archivo[7].

Acuerdo AGN 47 de 2000 Acceso a documentos. Acuerdo AGN 56 de 2000 Requisitos consulta. Acuerdo AGN 007 de 1994. "Reglamento General de Archivos". Artículo 23. "Valoración documental" que ordena a las entidades oficiales elaborar la tabla de retención documental a partir de su valoración.

Artículo 60. "Conservación integral de la documentación de archivos." Los archivos deberán implementar un sistema integrado de conservación acorde con el sistema de archivos establecido en la entidad, para asegurar el adecuado mantenimiento de los documentos, garantizando la integridad física y funcional de toda la documentación desde el momento de la emisión, durante su período de vigencia, hasta su disposición final.
Acuerdo AGN 11 de 1996. Criterios de conservación y organización de documentos. Acuerdo AGN 047 de 2000. Acceso a los documentos de Archivo, restricciones por razones de conservación. Acuerdo AGN 050 de 2000. Prevención de deterioro de los documentos de archivo y situaciones de riesgo.
Acuerdo AGN 056 de 2000. Requisitos para la consulta y acceso a los documentos de archivo[7]

[7] Archivo General de la Nación, normatividad, http://www.archivogeneral.gov.co/normatividad/

5.2.4 La Norma ISO 14721:2003 Open archival information system (OAIS) – Reference model10 propone el marco reglamentario de archivos para la conservación y acceso a la información electrónica a largo plazo, planteando el modelo para el tratamiento de los objetos digitales producidos durante la fase de gestión para su conversión en documento de archivo, esto es la preparación para su transferencia, la captura, el almacenamiento, el acceso a la información y la conservación a largo plazo: Este documento no es exhaustivo en relación con los requerimientos para preservación, por lo que se recomienda acudir a las normas ISO 14721 e ISO 32000.

5.3. MARCO TEÓRICO

En la Ley General de Archivos, se define Gestión documental como el conjunto de actividades administrativas y técnicas tendientes a la planificación, manejo y organización de la documentación producida y recibida por las entidades, desde su origen hasta su destino final, con el objeto de facilitar su utilización y conservación. Un programa de gestión documental se puede definir como el conjunto de instrucciones en las que se detallan las operaciones para el desarrollo de los procesos de la gestión documental al interior de cada entidad, tales como producción, recepción, distribución, trámite, organización, consulta, conservación y disposición final de los documentos. Para el desarrollo de éste trabajo es muy importante tener en cuenta los conceptos archivísticos empleados en los programas de Gestión Documental, así como la aplicación de modelos y estándares con el fin de diseñar e implementar el modelo para organizar y controlar los documentos e información generados bien sean análogos o digitales, en cada una de las áreas de la empresa y como administrar y asegurar toda esta información. Los Archivos son centros dinámicos de información, base para la gestión, los cuales conservan el patrimonio documental de las instituciones y de la proporcionan información original y única de las entidades y apoyan la planeación, control de resultados y toma de decisiones. Un SGD (Sistema de Gestión de

Documentos electrónicos) es unsistema informático que, está compuesto de unos elementos físicos (hardware y redes) que constituyen la infraestructura del sistema y otros lógicos (software) que proveen los servicios necesarios para gestionar un documento en la organización y realizar los flujos de información y automatización de los procesos. La Gestión Documental electrónica, ha ganado espacios teniendo en cuenta los múltiples beneficios tales como: bajos costos de almacenamiento, facilidad para recuperar información, posibilidad de consulta simultánea de un mismo documento, protección de documentos y optimización del flujo de información entre las diferentes personas

El análisis del estado inicial de la seguridad informática de la organización es fundamental, dado que con base a él se detectaran todas las vulnerabilidades, riesgos y amenazas a que se está expuesto, lo cual cimentara toda la implementación de su SGSI o auditoria de sistemas y a partir del cual se llevaran a cabo la planeación de las acciones preventivas y correctivas a seguir. Para garantizar la seguridad de la información así como la seguridad de la infraestructura en las organizaciones se debe garantizar que el análisis se realice de manera minuciosa e involucre todas los actores de la organización con el fin de realizar los planes de mejoramiento que correspondan en el menor tiempo posible para mitigar los riesgos informativos detectados durante este análisis[8]. Adicionalmente, con se debe realizar un análisis profundo con el fin de evidenciar el impacto que generan los riesgos ante la alta gerencia y así obtener los recursos necesarios para implementar las medidas que se requieran. La información que se maneja a través del sistema de gestión documental representan un activo muy valioso para la empresa Contactar, el cual puede encontrarse expuesto a diversos riesgos, que de ser explotados causarían un impacto significativo en la continuidad de las funciones normales de la empresa. Por lo anterior es muy importante efectuar acciones que

[8] Archivo General de la Nación, gestion documental, http://archivogeneral.gov.co/gestdocumental-pgd

contribuyan en la seguridad de la información, desarrollando diversas acciones para asegurar la integridad, protección y confiabilidad de la información. Entre las metodologías a resaltar se encuentra MAGERIT la cual está directamente relacionada con el uso de las tecnologías de la información que pretende la minimización de los riesgos de seguridad que puedan afectar la disponibilidad e integridad de la información. ISO 27001 un estándar de calidad internacional, y se encarga de administrar, gestionar e implementar las mejores prácticas para el manejo de la seguridad de la información en las organizaciones, la norma se encarga de proponer unos lineamientos, unas métricas e indicadores que permiten establecer un marco adecuado para implementar un sistema de gestión de seguridad de la información.

5.4. MARCO CONCEPTUAL

5.4.1. Gestión Documental

La Gestión documental se define como el conjunto de actividades administrativas y técnicas tendientes a la planificación, manejo y organización de la documentación producida y recibida por las entidades producida por los diferentes medios, desde su origen hasta su destino o disposición final, con el objeto de facilitar su utilización y conservación. Un Sistema de gestión documental se puede concebir como el conjunto de instrucciones en las que se detallan las operaciones para el desarrollo de los procesos de la gestión documental al interior de cada entidad, tales como producción, recepción, distribución, trámite, organización, consulta, conservación y disposición final de los documentos.

Gestión de base de datos: en la actualidad la aplicación y el uso de la información ofrecen grandes ventajas con el fin de administrar la integridad y calidad de los datos que se genera. Lograr realizar consultas de manera más eficiente, segura con mayor rapidez y fuentes confiables, aspectos importantes a tener en cuenta

en la gestión de datos e información en los diferentes procesos que se deben tener en cuenta dentro de la gestión documental.

5.4.2. Gestión Documental Electrónica

El termino Gestión documental electrónica se utiliza para hacer referencia al control automatizado de documentos electrónicos en las organizaciones a través de su ciclo vital, es decir desde su producción o recepción hasta su disposición final. Un SGD es un sistema informático que está compuesto de unos elementos físicos (el hardware y redes) que constituyen la infraestructura del sistema y otros lógicos (el software) que proveen los servicios necesarios para gestionar un documento en la organización

5.4.3. Workflow

Se refiere a la sistematización de un proceso del negocio el cual describe y automatiza las transacciones o series de actividades, donde los documentos, la información y las tareas son delegadas de un participante a otro de acuerdo a un conjunto de reglas procedimentales.

5.4.4. Almacenamiento

Garantizar a largo plazo la información, acceso rápido y selectivo al contenido del archivo, alto grado de seguridad y protección, empleo de estándares industriales y normas internacionales

5.4.5. Copias de Seguridad y Recuperación

Como parte de una buena planificación de protección de los datos que se generan en una organización, es importante tener en cuenta los mecanismos y métodos

para protegerlos así como cuales se ajustan mejor a las necesidades de la organización. Es un proceso complejo en el cual interviene una buena consecución de análisis y decisiones por parte del área de sistemas para su correcta implementación. Las copias de seguridad se realizan con el fin de contar con medios de respaldo y así recuperarlos en caso de pérdida, cambios de software plataformas, son útiles ante diferentes situaciones y usos como lo es recuperar aplicaciones y sistemas de información, que se presenten ante una catástrofe informática, natural o ataques informaticos.

5.4.6. Análisis de Riesgos Informáticos

El riesgo se define como la posibilidad de que ocurra algún evento negativo para las personas y/o empresas representado en los activos, infraestructura humana y tecnológica. Mediante el análisis de riegos y el adecuado uso de herramientas para el análisis que se presenten en una empresa es posible evaluar los casos que presenten inconsistencias con el fin de tomar medidas y correctivos para reducirlo, y así mantener un balance económico entre el impacto de los riesgos y de las soluciones.

Para un análisis de riesgos, es importante destacar e implementar las siguientes pautas que llevaran a determinar el nivel de amenazas a los cuales se está expuesto:

- ✓ Establecer activos relevantes para la empresa, características con el fin de clasificar y estandarizar valores.
- ✓ Determinar y analizar a qué amenazas estan expuestos.
- ✓ Determinar qué salvaguardas hay dispuestas y eficacia ante riesgos.
- ✓ Evaluar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

- ✓ Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia de la amenaza.

5.4.7. Seguridad de la información

La Seguridad de la Información propende mantener y garantizar la confidencialidad, integridad y disponibilidad de la información, para ello se apoya en políticas, controles y medidas que abarcan lo preventivo y lo reactivo; cabe recalcar que el concepto de información se aplica a nivel global y no se encuentra restringido al tipo de información o medio que lo contenga. La Seguridad Informática, es la seguridad específica aplicada a todos los medios electrónicos que contengan información; por ende cualquier desarrollo humano que se cimente sobre componentes electrónicos, de software y la interacción con estos, seria abarcado por la seguridad informática.

5.4.8. Normas ISO/IEC 27000

Es un estándar de calidad internacional, y se encarga de administrar, gestionar e implementar las mejores prácticas para el manejo de la seguridad de la información en las organizaciones, la norma se encarga de proponer unos lineamientos, unas métricas e indicadores que permiten establecer un marco adecuado para implementar un sistema de gestión de seguridad de la información. La serie de normas ISO con numeración 27000 aglomeran los estándares enfocados a la gestión de la seguridad de la información

La norma técnica ISO/IEC 27000 ofrece información general de las normas que componen la serie ISO27000 aclarando sus alcances y dando la visión de conjunto de estas normas; cuenta con el vocabulario técnico usado en las normas, igualmente contiene una introducción al Sistema Integrado de Seguridad de la Información (SGSI).

La norma técnica ISO/IEC 27001 se considera la norma principal de la serie ISO 27000, donde se plasman los requisitos normativos para establecer el SGSI y su subsecuente operación y mejora; el SGSI girará alrededor de los riesgos y su tratamiento

5.4.9. Ciclo de mejora contínua

El ciclo de mejora continua, reconocido como ciclo PDCA (del inglés plan-do-check-act) o PHVA (planificar-hacer-verificar-actuar) o Ciclo de Deming, es un sistema por medio del cual es posible identifiar y gestionar los procesos organizacionales y asi lograr estandarizar un sistema de mejora contínua, el cual esta conformado por las siguientes fases:

a) (Planear) - Establecer que hacer y cómo para satisfacer la política y objetivos de seguridad de la Información
b) (Hacer) – Poner en práctica lo planeado
c) (Verificar) - Verificar si se ha hecho lo planificado y si lo que se ha hecho es eficiente.
d) (Actuar) – Establecer las acciones de cómo y que mejorar.

La Fase Planear: En esta fase se debe tener claro la organización de ideas el tiempo y los recursos necesarios a emplear para ejecutarlos y asi establecer controles de seguridad, se debe tener en cuenta.

- ✓ Establecer politicas claras de segurdad del SGSI
- ✓ Implementar metodología con el fin de evaluar los riesgos y determinar los criterios para la analizar los riesgos
- ✓ Identificar activos, vulnerabilidades y amenazas
- ✓ Identificar , seleccionar y evaluar controles para el tratamiento de riesgos

La Fase "Do" (Implementación): Implementar y operar, establece una manera adecuada de como se debe operar el sistema,cumplimiento de políticas, controles y procedimientos y asi ejecutar las acciones planificadas, en base a la fase anterior.

- ✓ Documentación y registros del plan de tratamiento del riesgo donde se detalle quién, cómo, cuándo deberían implementar los controles para el tratamiento de riesgos
- ✓ Implementación de un plan de tratamiento del riesgo
- ✓ Implementación de los controles de seguridad correspondientes
- ✓ Determinación de cómo medir la eficacia de los controles
- ✓ Realización de programas de concientización y capacitación de empleados
- ✓ Gestión del funcionamiento normal del SGSI
- ✓ Gestión de los recursos del SGSI
- ✓ Implementación de procedimientos para detectar y gestionar incidentes de seguridad.

La Fase "Check" (Revisión verificación): Realizar las acciones correspondientes a evaluar el desempeño de los procesos, el cumplimiento de objetivos y lograr la mejora continua del sistema.

- ✓ Implementar procedimientos y controles para determinar incidentes de seguridad, eventos de seguridad y riesgos existentes.
- ✓ Revisiones y controles a los sisitemas de información

- ✓ Estudios y análisis sobre la evaluación de riesgos
- ✓ Auditorias de control con el fin de evaluar y hacer seguimiento a los controles establecidos.

La Fase "Act" Mantenimiento y Mejora: Realizar acciones, planes de mejora a partir de acciones correctivas, preventivas implementadas y asi evaluar el desempeño de los procesos .

- ✓ Implementación de medidas correctivas y preventivas al SGSI por medio de experiencias de seguridad propias y de terceros
- ✓ Comunicación de actividades y mejoras a todos los grupos de interés
- ✓ Asegurarse de que las mejoras cumplan los objetivos previstos.

6. DISEÑO METODOLÓGICO

Área del Conocimiento: Gestión de la Seguridad Informática

Área Específica: Vectorización de amenazas informáticas, SGSI basado en ISO27000 e ISO27001, Gestión del riesgo informático, Plan de contingencia para el negocio, Auditoría en Seguridad Informática

Teniendo en cuenta, los objetivos y el alcance que se plantea en el presente trabajo de investigación. La metodología planteada pretende dar cumplimiento a cada uno de los objetivos específicos que se definieron con el propósito de alcanzar el objetivo general del proyecto, se tendrá en cuenta el marco de referencia de la norma SGSI basado en ISO27000 e ISO27001 que especifica, entre otros aspectos, los requerimientos y actividades que se deben desarrollar para el diseño de un Sistema de Gestión de Seguridad de la Información.

6.1. TIPO DE INVESTIGACIÓN

El presente trabajo corresponde al análisis y desarrollo de una propuesta para la Seguridad del sistema de gestión documental de la empresa Contactar Pasto, de acuerdo al alcance definido, las necesidades de la entidad y tomando como base el modelo de referencia de seguridad de la norma ISO/IEC 27000-27001.

7. METODOLOGÍA MAGERIT (METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE TI)

Magerit es una metodología de análisis y gestión de riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, enfocada a las Administraciones Públicas. Esta metodología es una respuesta a la percepción de que la administración pública depende de forma creciente de los sistemas de información para alcanzar sus objetivos. Actualmente está en su versión 3.

La razón fundamental de MAGERIT está relacionada directamente con la generalización del uso de las tecnologías de la información, la cual supone unos beneficios evidentes para la protección de los activos tecnológicos e información y cuidado de los usuarios; ayudando a analizar y creando procedimientos para prevenir ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza. Este método es interesante y eficaz para nuestra formación como profesionales y para los que trabajamos con información digital y sistemas informáticos para protegerla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT permitirá saber cuánto valor está en juego y nos ayudará a protegerlo. Es importante conocer el riesgo al que están sometidos nuestros elementos de trabajo es imprescindible para poder gestionarlos.

8. RESULTADOS ESPERADOS DEL TRABAJO

8.1. ENTREGABLES DEL TRABAJO

A continuación se detallan los diferentes entregables del presente trabajo:

- Aplicación de una metodología para lograr identificar, clasificar y evaluar cada uno de los activos de información de la empresa para su análisis y valoración de riesgos respecto a la Seguridad de la Información.

- Definir una serie de políticas, alcance y objetivos para la seguridad de la informacion en todos los niveles de la empresa para ser aplicados y estandarizados en conjunto con el sistema de gestion documental.

- Establecer el Plan de tratamiento de riesgos, mediante el cual se logrará aplicar las acciones correctivas para la gestión de los riesgos de seguridad identificados en los procesos que se aplican en la empresa.

- Analizar la estructura organizacional, áreas y ofcinas para determinar la asignación de roles, controles, responsabilidades de la Seguridad de la Información.

- Evaluación y cumplimiento de la empresa con relación a cada uno de los procesos establecidos, los objetivos aplicados,los controles de acuerdo a lo estipulado en norma ISO 27001:2013, así como también los planes de acción a tener en cuenta con el fin de disminuir todos aquellos errores que se encuentren.

8.2. IMPACTO DEL PROYECTO

Con el desarrollo de este proyecto se pretende establecer un adecuado modelo de seguridad de la información para el sistema de gestión documental teniendo como guía la norma ISO/IEC 27001:2013, aplicación de metodologías como Magerit con el propósito de que la seguridad de la información, apoye a las diferentes áreas de la empresa en la consecución de los objetivos estratégicos.

Los objetivos planeados para este proyecto, tienen como fin la seguridad de la Información para la empresa, y asi lograr los siguientes beneficios:

Cumplimiento de la normatividad vigente. Permite establecer como se encuentra la empresa en temas de seguridad informática, analizar las amenazas que puedan suceder, implantar acciones de mejora con el fin de atenuarlas. Una apropiada gestión de riesgos permite garantizar la debida protección, integridad y confidencialidad de la información.

Mejorar la Imagen de la empresa. Proporcionar a la empresa adecuadas metodologías para apoyar la gestión de riesgos de seguridad de la información, lo cual le permite mejorar su imagen frente a otras empresas, ante sus clientes y empleados generando seguridad, respeto, confianza demostrando que se cumple de manera eficiente frente a los riesgos de seguridad.

Reducir costos. Generar impactos efectivos y de reconocimiento en la economía y presupuesto de la empresa, ya que si los empleados toman conciencia de la importancia de conocer todo lo que implica la seguridad de información que se tiene dentro de la empresa y como participes fundamentales de esta deben gestionar responsablemente los riesgos, y así a futuro minimizar inversiones innecesarias en seguridad y tecnología.

8.3. RESULTADOS – DIAGNOSTICO

Esta fase se planteó y desarrollo con el propósito de poder alcanzar los siguientes Objetivos específicos del proyecto:

8.3.1 Fortalecer la seguridad y el nivel de tecnología en los sistemas de información de la Empresa Contactar Pasto.

Para la consecución de este objetivo es pertinente realizar un estudio detallado de los diferentes factores o eventos que afectan la seguridad de la información bien sean por desconocimiento por parte de los colaboradores de la empresa, falta de capacitación en cuanto a la protección y seguridad de la información que se maneja entre oficinas, así como la implantación de nuevas tecnologías para fortalecer los mecanismos de seguridad de la información y así establecer que problemas están asociados a un proceso inadecuado se aseguramiento de la Gestión de la Información. Para este proceso se definen los siguientes métodos de análisis y evaluación de información:

• Evaluación, análisis con base en la experiencia del profesional de gestión documental , quien conoce los procesos establecidos en la empresa y conoce detalladamente el proceso de gestión documental ,sistema de información y TICS en cuanto a la administración y seguridad de la información.

• Consulta y estudio de los documentos que contienen los resultados de las diferentes auditorías, capacitaciones realizadas al proceso de gestión documental y tecnología, don el fin de detallar aspectos como debilidades asociados a la seguridad de la información.

8.3.2 Inventario de activos

Se identifica y relaciona los tipos de activos, descripción que se encuentran en las instalaciones de Contactar en la siguiente tabla:

Tabla 1 Descripción Activos informáticos

Nombre del Activo	Descripción	Tipo de Activo
[HW_SERV1]	SERVIDOR 1: contiene la data de la compañía donde se manejan las ofertas y proyectos de clientes, además se maneja software ERP de la compañía.	[HW] Equipos Informáticos
[HW_SERV2]	SERVIDOR 2: servidor exclusivo de Backup y contingencia.	[HW] Equipos Informáticos
[HW_PC]	Equipos de escritorios y portátiles personales, activos 64.	[HW] Equipos Informáticos
[HW_FW]	1 Router Fortinet corta fuegos	[HW] Equipos Informáticos
[HW_SWITCH]	2 Switch Administrables	[HW] Equipos Informáticos
[HW_RACK]	1 Rack de comunicaciones	[HW] Equipos Informáticos
[COM_WIFI]	1 Red Inalámbrica	[COM] Redes de comunicaciones
[COM_LAN]	1 Red LAN	[COM] Redes de comunicaciones
COM_INTERNET]	1 Acceso a Internet	[COM] Redes de comunicaciones
[SW_ERP]	Software ERP ISOLUCION, FINANCIAL, Docunet para manejo de inventario, financiero, comercial, nómina y compras.	[SW] Aplicaciones (Software)
[OS_WIN7]	Sistema Operativo Windows 7 instalado en 58 equipos	[SW] Aplicaciones (Software)
[OS_WIN8.1]	Sistema Operativo Windows 8.1 instalado en 4 equipos	[SW] Aplicaciones (Software)
[OS_WIN_2008]	Sistema Operativo Windows 2008 Server R2 STD instalado en los dos servidores.	[SW] Aplicaciones (Software)
[WWW]	Servicio hosting para página WEB alquilado	[S] Servicios
[EMAIL]	Servicio de servidor de correo corporativo alquilado	[S] Servicios
[D_CLIENTES]	Archivos que contiene la información de los Clientes, Áreas empresa.	[D] Datos/Información
[D_USUARIOS]	Datos de acceso a los sistemas de información.	[D] Datos/Información

Nombre del Activo	Descripción	Tipo de Activo
[MEDIA_DISK]	2 Discos duros Extraíbles de 2 TB especiales para Backup	[MEDIA] Soporte de Información
[UPS]	2 UPS una de alimentación para el rack de comunicaciones y 1 sistema de circuito regulado.	[AUX] Equipamiento Auxiliar
[UI]	Usuarios Internos	[P] Personal
[ADM]	1 coordinador TICS -Profesional, TICS	[P] Personal
[PROV]	1 Analista de soporte	[P] Personal
[LOCAL]	Cuarto de sistemas	[I]Instalaciones

Fuente El Autor

Definición de activos

D] Datos

- [D_CRESP] Copias de Respaldo
- [D_CLIENTES] Datos del Cliente
- [D_USUARIOS] Datos de Usuarios

[S] Servicios

- [S_INT] Internet
- [EMAIL] Correo Electrónico
- [WWW] Hosting de página WEB

[COM] Comunicaciones

- [COM_CTRL] Central telefónica IP
- [COM_TELIP] Teléfonos digitales
- [COM_WIFI] Red Inalámbrica
- [COM_LAN] Red LAN
- [COM_INTERNET] Acceso a Internet

Para el desarrollo de este objetivo se hace un análisis en la empresa Contactar, lo cual ha permitido generar la matriz de gestión de riesgos en donde se logró identificar de manera clara los activos, riesgos, amenazas y vulnerabilidades con

sus respectivas descripciones y asi tener mayor claridad en cuanto a los activos con los que se cuenta. A continuación se detallan en la la siguiente tabla:

Tabla 2 Matriz Identificación del Riesgo

CODIGO	TIPO ACTIVO	DESCRIPCION	AMENAZA	VULNERABILIDAD	RIESGO
SI	Sistema de Información	Aplicativos, Sistemas de Información	Difusión de software dañino, Errores del administrador, Errores de los usuarios, Errores de monitorización, Errores de mantenimiento / actualización de programas (software), Denegación de servicio.	Falta de control, Falta de capacitación del administrador del sistema, Falta de conocimiento para el uso de la aplicación, Incapacidad de la aplicación, Falta de procedimientos aprobados.	Suspensión de los servicios en las aplicaciones de la Organización debido a la falta de capacitación del administrador o a los usuarios y verificación de los procedimientos.
D	Documentos-datos	Proyectos, Planes, Contratos, Manuales, Registros clientes y administrativos, Informes, Área financiera, comercial, HV talento humano.	Introducción de información incorrecta, Degradación de la información, Robo.	Desconocimiento de la aplicación, Respaldo inadecuado, Falta de protección física.	Afectación a la integridad en la documentación institucional, debido a falta de capacitación de usuarios y acceso libre de personal no autorizado a servidores de almacenamiento de información.

CODIGO	TIPO ACTIVO	DESCRIPCION	AMENAZA	VULNERABILIDAD	RIESGO
HW	Hardware	PC's, Servidores, Switches, Routers, Backup	Incendios, Inundaciones, Contaminación mecánica, Corte del suministro eléctrico,	Falta de protección contra fuego, Falta de protección física adecuada, Falta de mantenimiento, Funcionamiento no confiable del UPS.	Daño masivo de equipamiento tecnológico debido a la falta de plan de contingencia en caso de desastres y debido al no mantenimiento de la UPS que brinda protección a los servidores principales
SW	Software	Sw, Base de Datos, Herramientas	Difusión de software dañino, Errores del administrador, Errores de los usuarios, Errores de monitorización, Errores de mantenimiento / actualización de programas (software), Denegación de servicio.	Falta de control, Falta de capacitación del administrador del sistema, Falta de conocimiento para el uso de la aplicación, Incapacidad de la aplicación, Falta de procedimientos aprobados.	Afectación en la disponibilidad de recursos, debido a utilización de software no licenciado, mal manejo por parte de administrador de aplicación, mal realización de mantenimiento a software o base de datos.
ID	Información Digital	Información en Servidor Archivos, USB, CD, DVD.	Robo, Avería de origen físico, Incendios, Acceso de Personal no autorizado.	Falta de protección física, Falta de mantenimiento, Falta de protección contra fuego.	Robo de información confidencial debido al acceso libre de personal no autorizado a los equipos.

CODIGO	TIPO ACTIVO	DESCRIPCION	AMENAZA	VULNERABILIDAD	RIESGO
STR	Servicios de Terceros	Internet, Telefonía, Energía, Vigilancia	Corte del suministro eléctrico, falla en servidores.	Funcionamiento no confiable del UPS, Manipulación inadecuada del administrador, Configuración errónea en aplicaciones.	Suspensión del servicio interno y externo para el desarrollo de actividades académicas y administrativas, debido a la falta de plan de contingencia como respaldo del canal de red, no verificación permanente de configuración dentro de los servidores principales y mantenimiento a la UPS del centro.
COM	Red de Comunicaciones	Red LAN, Red WAN, Red VPN, Acceso Remoto VPN	Corte del suministro eléctrico, falla en servidores,	Funcionamiento no confiable del UPS, Manipulación inadecuada del administrador, Configuración errónea en aplicaciones.	Daño en el sistema eléctrico que afecte el funcionamiento de los equipos principales que brindan los servicios a los usuarios debido al mal funcionamiento de la UPS, y la falta de capacitación del administrador para dar pronta solución en subir el servicio de las aplicaciones

CODIGO	TIPO ACTIVO	DESCRIPCION	AMENAZA	VULNERABILIDAD	RIESGO
					de los servidores.
S	Servicios	Soporte Técnico, atención de incidentes y requerimientos	Error de mantenimiento, error de asesor, Destrucción la información	Falta de capacitación del administrador del sistema, Falta de procedimientos aprobados	Que los usuarios se vean afectados por la no solución a sus requerimientos e incidentes de tal manera que se suspendan sus actividades académicas y administrativas ocasionando insatisfacción en los servicios prestados por parte del administrador, llevando a obtener una mala aceptación del servicio, lo cual afectara las estadísticas del área de informática.

Fuente El Autor

8.3.3 Determinar los recursos afectados y analizar la causa que origina cada uno de los riesgos encontrados

Actualmente, la información y la tecnología son recursos considerados como activos valiosos dentro de las organizaciones ya que las decisiones apropiadas que tomen o que puedan adoptar los directivos se basan en un alto porcentaje en los datos precisos y veraces. Para lograr que una administración se lleve de una manera eficaz, se debe tener el conocimiento suficiente sobre los riesgos que implica el manejo de las tecnologías de la información, para aplicar los controles necesarios dentro de la organización.

Como primera medida los activos son identificados y clasificados de acuerdo a su criticidad (integridad, confidencialidad y disponibilidad) y a su vez los recursos críticos son agrupados de acuerdo a sus funciones dentro de los procesos de la organización, para posteriormente ser revisados a través de un ciclo continuo de valoración de riesgos para determinar las amenazas relevantes, las consecuencias de su materialización y la existencia y efectividad de controles implementados que disminuyen el impacto o la probabilidad de concretar la amenaza.

Activos más relevantes:

- ✓ Los equipos informáticos que permiten hospedar datos, aplicaciones y servicios.
- ✓ Las aplicaciones informáticas (software) que permiten manejar los datos.
- ✓ Los servicios que se pueden prestar gracias a aquellos datos.
- ✓ Los servicios que se necesitan para poder gestionar dichos datos.
- ✓ Los dispositivos de soporte para el almacenamiento de datos.
- ✓ El equipamiento auxiliar que complementa el material informático.
- ✓ Las redes de comunicaciones que permiten intercambiar datos.
- ✓ Las instalaciones de equipos informáticos y de comunicaciones.

Para cada activo identificado se determinaron las características que lo definen tales como:

- ✓ Propietario del Activo
- ✓ Unidad responsable (Custodio del activo)
- ✓ Nombre y Tipo de activo (Qué caracterizan el activo)
- ✓ Descripción de funcionalidad y/o Servicios soportados
- ✓ Datos o Información comprendido
- ✓ Ubicación del Activo
- ✓ Una vez se identificaron las características que componen los activos se especifican bajo la siguiente clasificación:
- ✓ Equipos Informáticos (Servicios / Información)
- ✓ Redes de Comunicaciones
- ✓ Soportes de Información
- ✓ Instalaciones

Es fundamental el buen uso y la protección de la información y también que la tecnología de la información desempeñe una función cumpliendo sus objetivos de negocios por esto las organizaciones deben blindarse con el objetivo de proteger sus activos informáticos de las nuevas amenazas de seguridad que afecten el negocio. Las empresas algunas veces presentan falencias al momento de enfrentar este tipo de amenazas, por esto se han diseñado algunas metodologías que conducen de forma útil al análisis del riesgo, estos métodos ofrecen procedimientos los cuales deben ser implementados para la minimización de cualquier tipo de riesgo existentes.

Entre estas metodologías se encuentra MAGERIT la cual está directamente relacionada con el uso de las tecnologías de la información la cual pretende la

minimización de los riesgos de seguridad que puedan afectar la disponibilidad e integridad de la información.

Valoración de Equipos Informáticos:

Tabla 3 Criterios de Valoración

Criterios de Valoración		
Valor		**Criterio**
10	Extremo	daño extremadamente grave
9	Muy alto	daño muy grave
6-8	Alto	daño grave
3-5	Medio	daño importante
1-2	Bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Fuente: 2012_Magerit_v3_libro2_catálogo de elementos_es_NIPO_630-12-171-8

Tabla 4 Valoración de Equipos Informáticos

Metodología MAGERIT					
Código Grupo de Activo	Nombre Grupo de Activo	Código Activo-Entidad	Nombre Activo - Entidad	Dimensiones	Criterio
[mid]	Equipos Medios (Conectados a red inalámbrica)	[PC_Empleados]	Equipos Escritorio	**Confiabilidad**	7
				Integridad	6
				Autenticidad	6
				Disponibilidad	5
				Trazabilidad	6

Metodología MAGERIT					
Código Grupo de Activo	Nombre Grupo de Activo	Código Activo-Entidad	Nombre Activo - Entidad	Dimensiones	Criterio
[pc]	Equipos fácilmente transportados	[PC_Portatiles]	Equipos Portátiles	**Confiabilidad**	8
				Integridad	8
				Autenticidad	7
				Disponibilidad	7
				Trazabilidad	6
[router]	Enrutadores	[Enrutadores]	Router Fortinet corta fuegos	**Confiabilidad**	8
				Integridad	8
				Autenticidad	8
				Disponibilidad	8
				Trazabilidad	8
				Integridad	8
				Autenticidad	8
				Disponibilidad	8
				Trazabilidad	8
[lp]	Swich	[Swich_Interconexion]	Switch Administrable	**Confiabilidad**	8
				Integridad	8
				Autenticidad	8
				Disponibilidad	8
				Trazabilidad	8
[arch]	Punto de Acceso al Servicio	[Sap_Acceso]	Puntos de Acceso	**Confiabilidad**	6
				Integridad	7
				Autenticidad	8

Metodología MAGERIT					
Código Grupo de Activo	Nombre Grupo de Activo	Código Activo-Entidad	Nombre Activo - Entidad	Dimensiones	Criterio
			Inalámbrico	**Disponibilidad**	7
				Trazabilidad	6

Fuente: El Autor

Tabla 5 Valoración de Servicios

Código Grupo de Activo	**Nombre Grupo de Activo**	**Código Activo-Entidad**	**Nombre Activo - Entidad**	**Dimensiones**	**Criterio**
[www]	Wold Wide Web	[Internet]	Servicio de Internet Hosting Pagina WEB	**Confiabilidad**	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	5
				Trazabilidad	5
[email]	Correo Electrónico	[S_Correo]	Servicio de Servidor de Correo Corporativo	**Confiabilidad**	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	6
				Trazabilidad	6

Fuente: El Autor

Tabla 6 Valoración Redes de Comunicaciones

Código Grupo de Activo	Nombre Grupo de Activo	Código Activo-Entidad	Nombre Activo - Entidad	Dimensiones	Criterio
[wifi]	Red Inalámbrica	[R_wifi]	Red Inalámbrica	**Confiabilidad**	8
				Integridad	8
				Autenticidad	8
				Disponibilidad	7
				Trazabilidad	7
[LAN]	Red Local	[R_Local]	Red LAN	**Confiabilidad**	8
				Integridad	8
				Autenticidad	7
				Disponibilidad	7
				Trazabilidad	6
[Internet]	Internet	[Internet]	Acceso a Internet	**Confiabilidad**	6
				Integridad	6
				Autenticidad	7
				Disponibilidad	6
				Trazabilidad	6
[Intranet]	Intranet	[Intranet]	Acceso a Intranet	**Confiabilidad**	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	7
				Trazabilidad	6

Fuente: El Autor

Tabla 7 Aplicaciones Informáticas

Código Grupo de Activo	Nombre Grupo de Activo	Código Activo-Entidad	Nombre Activo - Entidad	Dimensiones	Criterio
[app]	Servidor Aplicaciones	[Server_App]	Win Server 2008	**Confiabilidad**	8
				Integridad	8
				Autenticidad	8
				Disponibilidad	7
				Trazabilidad	7
[os]	Sistemas Operativos	[OS_Win7_Win8.1_Win10]	Sistemas Operativos Windows 7, 8.1, 10.	**Confiabilidad**	8
				Integridad	8
				Autenticidad	7
				Disponibilidad	7
				Trazabilidad	6
[erp]	Software	[SW_ERP]	Software Docunet ERP Financial,Isolucion	**Confiabilidad**	6
				Integridad	6
				Autenticidad	7
				Disponibilidad	6
				Trazabilidad	6

Fuente: El Autor

Tabla 8 Valoración Datos/Información

Código Grupo de Activo	Nombre Grupo de Activo	Código Activo-Entidad	Nombre Activo - Entidad	Dimensiones	Criterio
[files]	Clientes	[Internet]	Archivos de Información de Clientes	**Confiabilidad**	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	8
				Trazabilidad	5
[int]	Datos de Gestión Interna	[D_Gestion]	Datos de Acceso a Sistemas de Información	**Confiabilidad**	8
				Integridad	6
				Autenticidad	6
				Disponibilidad	8
				Trazabilidad	6
[usuarios]	Copias de Respaldo	[D_Usuarios_Backup]	Copia de Respaldo (Backup)	**Confiabilidad**	8
				Integridad	8
				Autenticidad	8
				Disponibilidad	8

Fuente: El Autor

Tabla 9 Valoración Soporte de Información

Código Grupo de Activo	Nombre Grupo de Activo	Código Activo-Entidad	Nombre Activo - Entidad	Dimensiones	Criterio
[media]	Soporte de Información	[Disk]	Discos Duros (Backup)	**Confiabilidad**	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	5
				Trazabilidad	5

Fuente: El Autor

Tabla 10 Valoración Redes de Comunicación

Código Grupo de Activo	Nombre Grupo de Activo	Código Activo-Entidad	Nombre Activo - Entidad	Dimensiones	Criterio
[wifi]	Red Inalámbrica	[R_wifi]	Red Inalámbrica	**Confiabilidad**	8
				Integridad	8
				Autenticidad	8
				Disponibilidad	7
				Trazabilidad	7
[LAN]	Red Local	[R_Local]	Red LAN Correo Corporativo	**Confiabilidad**	8
				Integridad	8
				Autenticidad	7
				Disponibilidad	7

Código Grupo de Activo	Nombre Grupo de Activo	Código Activo-Entidad	Nombre Activo - Entidad	Dimensiones	Criterio
				Trazabilidad	6
[Internet]	Internet	[Internet]	Acceso a Internet	**Confiabilidad**	6
				Integridad	6
				Autenticidad	7
				Disponibilidad	6
				Trazabilidad	6
[Intranet]	Intranet	[Intranet]	Acceso a Intranet	**Confiabilidad**	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	7
				Trazabilidad	6
[PSNT]	Red Telefónica	[Red]	Red Telefónica Analógica	**Confiabilidad**	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	7
				Trazabilidad	6
				Disponibilidad	7
				Trazabilidad	6

Fuente: El Autor

Tabla 11 Valoración Equipamiento Auxiliar

Código Grupo de Activo	Nombre Grupo de Activo	Código Activo-Entidad	Nombre Activo - Entidad	Dimensiones	Criterio
[Aux]	Maquinas Centrales	[AC_Maquinas]	Máquinas centrales de Aires acondicionados	**Confiabilidad**	8
				Integridad	8
				Autenticidad	8
				Disponibilidad	7
				Trazabilidad	7
[ups]	Sistema Ininterrumpido de Potencia	[U_Computadores]	UPS	**Confiabilidad**	8
				Integridad	6
				Autenticidad	6
				Disponibilidad	5
				Trazabilidad	5

Fuente: El Autor

Tabla 12 Valoración de personal

Código Grupo de Activo	Nombre Grupo de Activo	Código Activo-Entidad	Nombre Activo - Entidad	Dimensiones	Criterio
[ui]	Usuarios Internos	[E_Funcionarios]	Usuarios Internos	**Confiabilidad**	6
				Integridad	7
				Autenticidad	8
				Disponibilidad	8
				Trazabilidad	6
				Confiabilidad	7

Código Grupo de Activo	Nombre Grupo de Activo	Código Activo-Entidad	Nombre Activo - Entidad	Dimensiones	Criterio
[adm	Adminsitradores de Sistemas	[A_Sistemas]	Analista, Profesional Tics	**Integridad**	6
				Autenticidad	6
				Disponibilidad	5
				Trazabilidad	5
[op]	Aux. Operacionales	[U_Computadores]	Aux. Operacionales	**Confiabilidad**	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	5
				Trazabilidad	5

Fuente: El Autor

Tabla 13 Valoración Instalaciones

Código Grupo de Activo	Nombre Grupo de Activo	Código Activo-Entidad	Nombre Activo - Entidad	Dimensiones	Criterio
[Local]	Cuarto de Sistemas	[Local]	Cuarto de Sistemas	**Confiabilidad**	8
				Integridad	8
				Autenticidad	8
				Disponibilidad	7
				Trazabilidad	7
				Integridad	6
				Autenticidad	6

Código Grupo de Activo	Nombre Grupo de Activo	Código Activo-Entidad	Nombre Activo - Entidad	Dimensiones	Criterio
				Disponibilidad	5
				Trazabilidad	5

Fuente: El Autor

Tabla 14 Vulnerabilidades

Activo	Vulnerabilidad	Nivel del Riesgo								
		[D]	[C]	[A]	[T]	**MA**	**A**	**M**	**B**	**MB**
[Server_App] Servicior de Aplicaciones	Errores de Administradores	8	8	8	6	MA				
[PC_Empleados] Equipo de cómputo conectados a red	Errores de Usuarios	4	5	5	5		A			
Equipos de Comunicaciones	Poco mantenimiento Correctivo	7	5	5	3		A			
Soporte de la Información	Existen varios administradores de los mismos equipos de computo	8	8	8	5	MA				
[R_wifi], Redes [Internet], [Intranet], [Inalambrica]	Mal funcionamiento por eventos climáticos	8	4	4	5			M		

Activo	Vulnerabilidad	Nivel del Riesgo								
		[D]	[C]	[A]	[T]	MA	A	M	B	MB
[S_A_Bases de datos] Almacenamiento de información en el servidor	Varios usuarios	8	8	8	7	MA				
[A_Copias de Seguridad]	Varios administradores	5	5	5	5				B	
[D_ConfiguracionSer] Servidor Local	Errores de Administradores	6	5	5	6			M		
[E_entidad] Infraestructura Física y de Comunicaciones	Muchos equipos de cómputo no cuenta con ups	6	4	4	4				B	
[Pass_Usuarios] Políticas de Seguridad	Conexión a Internet, sin permisos	5	5	5	5			M		
[S_Internet] Acceso del Servicio Internet	Virus, Fraudes, Ataques, etc.	8	8	8	6	MA				
Sistemas Operativos	Directorios Compartidos y Puertos abiertos	8	8	8	6	MA				
Personas (Servicios)	Abuso de Privilegios	4	4	5	4				B	

Fuente: El Autor

8.3.4 Identificación de amenazas a que están expuestos los activos de información.Se identifican y evalúan las amenazas que sufren los activos de información. Se realizó la identificación de amenazas basándose en la clasificación de MAGERIT:

Tabla 15 Valoración de las amenazas

<table>
<tr><th colspan="2">Valoración amenazas</th></tr>
<tr><td colspan="2">[N.1] Fuego</td></tr>
<tr><td>Tipo de Activos:

[HW] equipos informáticos (hardware)

[AUX] equipamiento auxiliar

[L] instalaciones</td><td>Dimensiones:

[D] disponibilidad</td></tr>
<tr><td colspan="2">Descripción:

Incendios: Posibilidad de que el fuego acabe con recursos del sistema.</td></tr>
<tr><td colspan="2">[N.1] Daños por Agua</td></tr>
<tr><td>Tipo de Activos:

• [HW_SERV1], [HW_SERV2], [HW_FW]
• [MEDIA_DISK]
• [UPS]
• [LOCAL]</td><td>Dimensiones:

[D] disponibilidad</td></tr>
<tr><td colspan="2">Descripción: Inundaciones: Posibilidad de que el Agua acabe con los recursos del sistema</td></tr>
<tr><td colspan="2">[N.*] Desastres Naturales</td></tr>
<tr><td>Tipo de Activos:</td><td>Dimensiones:</td></tr>
</table>

<table>
<tr><th colspan="2">Valoración amenazas</th></tr>
<tr><td>[HW_SERV1], [HW_SERV2], [HW_FW]
[MEDIA_DISK]
[UPS]
[LOCAL]</td><td>[D] disponibilidad</td></tr>
<tr><td colspan="2">Descripción:

Otros incidentes que se producen sin intervención humana como: contaminación, siniestro mayor, fenómeno climático, fenómeno sísmico, fenómeno de origen volcánico y fenómeno meteorológico.</td></tr>
<tr><td colspan="2">[I.6] Corte del Suministro Eléctrico</td></tr>
<tr><td>Tipo de Activos:

[HW] equipos informáticos (hardware)
[Media] soportes de información

[AUX] equipamiento auxiliar</td><td>Dimensiones:

[D] disponibilidad</td></tr>
<tr><td colspan="2">Descripción:

Cese de la alimentación de potencia

Origen: Entorno (accidental) Humano (accidental o deliberado)</td></tr>
<tr><td colspan="2">[I.*] Desastres Industriales</td></tr>
<tr><td>Tipo de Activos:

[HW] equipos informáticos (hardware)
[Media] soportes de información</td><td>Dimensiones:

[D] disponibilidad</td></tr>
</table>

Valoración amenazas	
[AUX] equipamiento auxiliar [L] instalaciones	
Descripción: Otros desastres debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico, **Origen:** Entorno (accidental) Humano (accidental o deliberado)	
[I.3] Contaminación Mecánica	
Tipo de Activos: [HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar	**Dimensiones:** [D] disponibilidad
Descripción: Vibraciones, polvo, suciedad, **Origen:** Entorno (accidental) Humano (accidental o deliberado).	
[I.8] Fallo de Servicios de Comunicaciones	
Tipo de Activos: [COM] Redes de Comunicaciones	**Dimensiones:** [D] disponibilidad
Descripción: Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción	

<table>
<tr><th colspan="2">Valoración amenazas</th></tr>
<tr><td colspan="2">física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.

Origen: Entorno (accidental)

Humano (accidental o deliberado)</td></tr>
<tr><td colspan="2">[E.1] Errores de Usuarios</td></tr>
<tr><td>Tipo de Activos:

[D] datos / información

[keys] claves criptográficas

[S] servicios

[SW] aplicaciones (software)

[Media] soportes de información</td><td>Dimensiones:

[I] integridad

[C] confidencialidad

[D] disponibilidad</td></tr>
<tr><td colspan="2">Descripción: Equivocaciones de las personas cuando usan los servicios, datos, etc.

Origen: Entorno (accidental), Humano (accidental o deliberado)

Ver: EBIOS: 38 - ERROR DE USO</td></tr>
<tr><td colspan="2">[E.1] Errores del Administrador</td></tr>
<tr><td>Tipo de Activos:

[D] datos / información

[keys] claves criptográficas

[S] servicios</td><td>Dimensiones:

[D] disponibilidad

[I] integridad

[C] confidencialidad</td></tr>
</table>

<table>
<tr><th colspan="2">Valoración amenazas</th></tr>
<tr><td>[SW] aplicaciones (software)

[Media] soportes de información

[HW] equipos informáticos (hardware) [COM] redes de comunicaciones [Media] soportes de información</td><td></td></tr>
<tr><td colspan="2">Descripción: Equivocaciones de personas con responsabilidades de instalación y operación

Origen: Entorno (accidental), Humano (accidental o deliberado)</td></tr>
<tr><td colspan="2">[E.9] Errores de [re-]encadenamiento</td></tr>
<tr><td>Tipo de Activos:

[S] servicios

[SW] aplicaciones (software)

[COM] redes de comunicaciones</td><td>Dimensiones:

[C] confidencialidad</td></tr>
<tr><td colspan="2">Descripción: Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera</td></tr>
<tr><td colspan="2">[E.15] Alteración Accidental de la Información</td></tr>
<tr><td>Tipo de Activos:

[D] datos / información</td><td>Dimensiones:

[I] integridad</td></tr>
</table>

Valoración amenazas	
[keys] claves criptográficas [S] servicios [SW] aplicaciones (software) [COM] redes de comunicaciones [Media] soportes de información [L] instalaciones	
Descripción: Alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	
[E.18] Destrucción de Información	
Tipo de Activos: [D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (software) [COM] redes de comunicaciones [Media] soportes de información [L] instalaciones	**Dimensiones:** [D] disponibilidad
Descripción: Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas	

<table>
<tr><th colspan="2">Valoración amenazas</th></tr>
<tr><td colspan="2">específicas.</td></tr>
<tr><td colspan="2">[E.20] Vulnerabilidades de los Programas (Software)</td></tr>
<tr><td>Tipo de Activos:

[SW] aplicaciones (software)</td><td>Dimensiones:

[[I] integridad

[D] disponibilidad

[C] confidencialidad</td></tr>
<tr><td colspan="2">Descripción: Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.</td></tr>
<tr><td colspan="2">[E.23] Errores de Mantenimiento / Actualización de Equipos (Hardware)</td></tr>
<tr><td>Tipo de Activos:

[HW] equipos informáticos (hardware)
[Media] soportes electrónicos

[AUX] equipamiento auxiliar</td><td>Dimensiones:

[D] disponibilidad</td></tr>
<tr><td colspan="2">Descripción: Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.</td></tr>
<tr><td colspan="2">[E.25] Perdida de Equipos</td></tr>
<tr><td>Tipo de Activos:

[HW] equipos informáticos (hardware)
[Media] soportes electrónicos</td><td>Dimensiones:

[D] disponibilidad</td></tr>
</table>

Valoración amenazas	
[AUX] equipamiento auxiliar	[C] confidencialidad
Descripción: La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.	
[A.4] Manipulación de la Configuración	
Tipo de Activos: [D.log] registros de actividad	**Dimensiones:** [I] integridad [C] confidencialidad [A] disponibilidad
Descripción: Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	
[A.7] Uso No Previsto	
Tipo de Activos: [S] servicios [SW] aplicaciones (software) [HW] equipos informáticos (hardware) [COM] redes de comunicaciones [Media]	**Dimensiones:** [D] disponibilidad [C] confidencialidad [I] integridad

<table>
<tr><th colspan="2">Valoración amenazas</th></tr>
<tr><td>soportes de información

[AUX] equipamiento auxiliar

[L] instalaciones</td><td></td></tr>
<tr><td colspan="2">Descripción: Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.</td></tr>
<tr><td colspan="2">[A.8] Difusión de Software Dañino</td></tr>
<tr><td>Tipo de Activos:

[SW] aplicaciones (software)</td><td>Dimensiones:

[D] disponibilidad

[I] integridad

[C] confidencialidad</td></tr>
<tr><td colspan="2">Descripción: Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.</td></tr>
<tr><td colspan="2">[A.18] Destrucción de Información</td></tr>
<tr><td>Tipo de Activos:

[D] datos / información

[keys] claves criptográficas

[S] servicios (acceso)

[SW] aplicaciones (SW)</td><td>Dimensiones:

[D] disponibilidad</td></tr>
</table>

Valoración amenazas	
[Media] soportes de información [L] instalaciones	
Descripción: Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.	
[A.30] Ingeniería Social (Picaresca)	
Tipo de Activos: [P] Personal Interno	**Dimensiones:** [C] confidencialidad [I] integridad [D] disponibilidad
Descripción: Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.	

Fuente: El Autor

Tabla 16 Escala del Rango porcentual de impactos

Impacto	Valor Cuantitativo
Muy Alto	100%
Alto	75%
Medio	50%
Bajo	20%
Muy Bajo	5%

Fuente: El Autor

Tabla 27 Relación de Amenazas por Activo Identificando su Frecuencia e Impacto

RELACION DE AMENAZAS POR ACTIVO IDENTIFICANDO SU FRECUENCIA E IMPACTO							
AMENAZA	**ACTIVO**	**FRECUENCIA**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[N.1] Fuego	[HW_SERV1]	5				100	
	[HW_SERV2]	5				100	
	[HW_FW]	5				75	
	[MEDIA_DISK]	5				75	
	[UPS]	5				50	
	[LOCAL]	5				100	
[N.2] Daños por Agua	[HW_SERV1]	5				100	
	[HW_SERV2]	5				100	
	[HW_FW]	5				75	
	[MEDIA_DISK]	5				75	
	[UPS]	5				50	
	[LOCAL]	5				100	
[N.*] Desastres Naturales	[HW_SERV1]	5				100	
	[HW_SERV2]	5				100	
	[HW_FW]	5				100	
	[MEDIA_DISK]	5				100	
	[UPS]	5				100	
	[LOCAL]	5				100	
[I.1] Fuego	[HW_SERV1]	5				100	
	[HW_SERV2]	5				100	
	[HW_FW]	5				75	
	[MEDIA_DISK]	5				75	
	[UPS]	5				50	
	[LOCAL]	5				100	
[I.2] Daños por Agua	[HW_SERV1]	5				100	

RELACION DE AMENAZAS POR ACTIVO IDENTIFICANDO SU FRECUENCIA E IMPACTO							
AMENAZA	**ACTIVO**	**FRECUENCIA**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
	[HW_SERV2]	5				100	
	[HW_FW]	5				75	
	[MEDIA_DISK]	5				75	
	[UPS]	5				50	
	[LOCAL]	5				100	
[I.*] Desastres Naturales	[HW_SERV1]	5				100	
	[HW_SERV2]	5				100	
	[HW_FW]	5				100	
	[MEDIA_DISK]	5				100	
	[UPS]	5				100	
	[LOCAL]	5				100	
[I.3] Contaminación Mecánica	[HW_SERV1]	5				50	
	[HW_SERV2]	5				50	
	[HW_FW]	10				50	
	[MEDIA_DISK]	10				75	
	[UPS]	5				20	
[I.4] Contaminación Electromagnética	[HW_SERV1]	5				100	
	[HW_SERV2]	5				75	
	[HW_FW]	5				100	
	[MEDIA_DISK]	5				75	
	[COM-LAN]	50				50	
	[UPS]	5				20	
[I.5] Avería de Origen Físico o Lógico	[SW_ERP]	5				100	
	[OS_WIN_2008]	10				75	
	[HW_SERV1]	5				100	

RELACION DE AMENAZAS POR ACTIVO IDENTIFICANDO SU FRECUENCIA E IMPACTO							
AMENAZA	**ACTIVO**	**FRECUENCIA**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
	[HW_SERV2]	5				75	
	[HW_FW]	5				50	
	[MEDIA_DISK]	5				50	
	[UPS]	5				20	
[I.6] Corte del Suministro Eléctrico	[HW_SERV1]	10				75	
	[HW_SERV2]	10				75	
	[HW_FW]	10				75	
	[MEDIA_DISK]	10				75	
	[UPS]	50				100	
	[LOCAL]	10				100	
[I.7] Condiciones Inapropiadas de temperatura y humedad	[HW_SERV1]	50				75	
	[HW_SERV2]	50				75	
	[HW_FW]	50				50	
	[MEDIA_DISK]	50				50	
	[UPS]	50				50	
	[LOCAL]	50				75	
[I.8] Fallos de servicio de comunicaciones	[COM_LAN]	10				75	
[I.10] Degradación de los soportes de almacenamiento de la información	[MEDIA_DISK]	10				75	
[I.11] Emanaciones Electromagnéticas	[HW_SERV1]	5		100			
	[HW_SERV2]	5		50			
	[HW_FW]	50		100			
	[MEDIA_DISK]	5		100			
	[COM_LAN]	50		100			

RELACION DE AMENAZAS POR ACTIVO IDENTIFICANDO SU FRECUENCIA E IMPACTO							
AMENAZA	**ACTIVO**	**FRECUENCIA**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
	[UPS]	5		20			
[E.1] Errores de los Usuarios	[D_USUARIOS]	70		100	100	100	
	[D_CLIENTES]	70		100	100	100	
	[UI]	70		100	100	100	
	[PROV]	5		100	100	100	
	[SW_ERP]	10		75	75	75	
	[OS_WIN_2008]	10		50	50	50	
	[MEDIA_DISK]	10		50	50	50	
[E.2] Errores del Administrador	[D_USUARIOS]	70		100	100	100	
	[D_CLIENTES]	70		100	100	100	
	[ADM]	70		100	100	100	
	[PROV]	5		100	100	100	
	[SW_ERP]	50		75	75	75	
	[OS_WIN_2008]	50		75	75	75	

RELACION DE AMENAZAS POR ACTIVO IDENTIFICANDO SU FRECUENCIA E IMPACTO							
AMENAZA	**ACTIVO**	**FRECUENCIA**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
	[MEDIA_DISK]	50		50	50	50	
	[COM_LAN]	50		50	50	50	
	[HW_SERV1]	50		100	100	100	
	[HW_SERV2]	50		50	50	50	
	[HW_FW]	50		50	50	50	
[E.7] Deficiencias de la Organización	[ADM]	5				100	
	[PROV]	10				75	
	[UI]	50				20	
[E.8] Difusión de Software Dañino	[SW_ERP]	70		100	100	100	
	[OS_WIN_2008]	70		100	100	100	
[E.9] Errores de Re encaminamiento	[SW_ERP]	50		75			
	[OS_WIN_2008]	50		75			
	[D_USUARIOS]	50		75			
	[D_CLIENTES]	50		75			
	[COM_LOCAL]	50		75			
[E.15] Alteración accidental de la información	[D_USUARIOS]	70			75		
	[D_CLIENTES]	70			75		

RELACION DE AMENAZAS POR ACTIVO IDENTIFICANDO SU FRECUENCIA E IMPACTO							
AMENAZA	**ACTIVO**	**FRECUENCIA**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
	[SW_ERP]	70			75		
	[OS_WIN_2008]	50			50		
	[COM_LAN]	10			50		
	[MEDIA_DISK]	5			50		
	[LOCAL]	5			50		
[E.18] Destrucción de Información	[D_USUARIOS]	5				100	
	[D_CLIENTES]	5				100	
	[SW_ERP]	5				100	
	[OS_WIN_2008]	5				100	
	[COM_LAN]	5				100	
	[MEDIA_DISK]	5				100	
	[LOCAL]	5				100	
[E.19] Fuga de Información	[D_USUARIOS]	5		100			
	[D_CLIENTES]	5		100			
	[SW_ERP]	5		100			
	[OS_WIN_2008]	5		100			
	[COM_LAN]	5		100			
	[MEDIA_DISK]	5		100			
	[LOCAL]	5		100			
	[ADM]	5		100			

RELACION DE AMENAZAS POR ACTIVO IDENTIFICANDO SU FRECUENCIA E IMPACTO							
AMENAZA	**ACTIVO**	**FRECUENCIA**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
	[PROV]	50		100			
	[UI]	70		100			
[E.20] Vulnerabilidades de los programas de Software	[SW_ERP]	50		100	100	100	
	[OS_WIN_2008]	50		75	75	100	
[E.21] Errores de Mantenimiento / Actualización de Software	[SW_ERP]	50			100	100	
	[OS_WIN_2008]	50			75	75	
[E.22] Errores de Mantenimiento / Actualización de Hardware	[HW_SERV1]	10				100	
	[HW_SERV2]	10				75	
	[HW_FW]	10				75	
	[MEDIA_DISK]	10				75	
	[UPS]	5				50	

Fuente: El Autor

8.3.5 Método de análisis de riesgo

Para el análisis de riesgos, es importante realizar los siguientes pasos los cuales nos llevaran a determinar el nivel de amenazas al cual estamos expuestos:

- ✓ Determinar los activos relevantes para la empresa, su interrelación y su valor, dependiendo del costo supondría su degradación.
- ✓ Determinar a qué amenazas están expuestos aquellos activos.
- ✓ Determinar qué salvaguardas hay dispuestos y cuán eficaces son frente al riesgo.

- ✓ Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- ✓ Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia de la amenaza.

Es de vital importancia hacer el estimado de riesgos antes de llevar a cabo los pasos para el análisis de riesgos, además podemos seguir los siguientes pasos:

Activos: en una organización y su sistema de información siempre existen dos cosas esenciales, la información y los servicios que presta la compañía. Estos serían los activos que dan la pauta para los requisitos de seguridad para los demás componentes los cuales podemos clasificar como:

- ✓ Datos
- ✓ Servicios
- ✓ Aplicaciones
- ✓ Equipos informáticos
- ✓ Redes
- ✓ Infraestructura humana y tecnológica

Para poder llevar a cabo un estudio y saber de qué forma que nivel de seguridad aplicar para la protección eficaz de los activos es importante tener en cuenta la valoración de los activos, la dimensión las cuales se pueden calibrar dependiendo de su confidencialidad, integridad y disponibilidad, valoración cualitativa y cuantitativa la cual nos permite tener un valor estimado tanto del activo hardware como de la información y software, cuánto vale la interrupción del servicio si un ataque puede detenerlos.

Amenazas: debemos determinar qué tipo de amenazas estamos propensos a recibir, estas podrían ser naturales, del entorno, defectos de las aplicaciones,

accidentales causadas por los mismos usuarios y las causadas por personas buscando el apoderamiento forzoso de la información. Estas amenazas se pueden clasificar como altas, media, baja y muy baja lo cual nos puede llevar a determinar el impacto del riesgo al que estamos expuestos.

Seguridad o salvaguardas: es necesario proteger de la mejor manera los activos tecnológicos, para poder escoger o saber de qué forma puedo salvaguardar la información, debemos tener en cuenta los siguientes puntos:

- ✓ Tipo de activos a proteger, pues cada tipo se protege de una forma específica.
- ✓ Dimensión o dimensiones de seguridad que requieren protección.
- ✓ Amenazas de las que necesitamos protegernos.
- ✓ Si existen protección alternativa.

Es prudente establecer un principio de proporcionalidad y tener en cuenta:

- ✓ El mayor o menor valor propio o acumulado sobre un activo, centrándonos en lo más relevante y omitiendo lo irrelevante.
- ✓ La mayor o menor probabilidad de que una amenaza ocurra, centrándonos en los riesgos más importantes.
- ✓ Cobertura del riesgo que proporcionan las protecciones alternativas

Caracterización de los activos: para cada activo hay que determinar una serie de características que lo definen:

- ✓ Código, típicamente procedente del inventario
- ✓ Nombre, descripción, tipo
- ✓ Unidad responsable. A veces hay más de una unidad.
- ✓ Persona responsable
- ✓ Ubicación, cantidad

Valoracion de riesgos

A continuación, se realiza la identificación de los riesgos teniendo en cuenta la tabla sugerida en la guía de actividades.

Tabla 18 Valoracion riesgos

Probabilidad			**Impacto**	
Alta	A		Catastrófico	C
Media	M		Moderado	M
Baja	B		Leve	L

Fuente: El Autor

Tabla 19 Riesgo - Valoración

COMUNICACIÓN							
Riesgo/Valoración		**Probabilidad**			**Impacto**		
		A	**M**	**B**	**L**	**M**	**C**
R1	Sistema telefónico no funciona adecuadamente		X			X	
R2	Información sobre teléfonos de emergencias			X	X		
HARDWARE							
Riesgo/Valoración		**Probabilidad**			**Impacto**		
		A	**M**	**B**	**L**	**M**	**C**
R3	Falta de mantenimiento correctivo		X			X	
R4	Instalación de equipos de cómputo de manera incorrecta		X				X
INFORMACION							
Riesgo/Valoración		**Probabilidad**			**Impacto**		

		A	M	B	L	M	C
R5	Perdida de información de respaldo			X		X	
R6	Deterioro de la información por incorrecto almacenamiento		X				X
INFRAESTRUCTURA DE RED							
Riesgo/Valoración		**Probabilidad**			**Impacto**		
		A	**M**	**B**	**L**	**M**	**C**
R7	Falta documentación que facilite la administración de los dispositivos de rd			X		X	
R8	No existe un procedimiento que indique como restaurar la interconexión			X		X	
SEGURIDAD FISICA							
Riesgo/Valoración		**Probabilidad**			**Impacto**		
		A	**M**	**B**	**L**	**M**	**C**
R9	El sistema de cámaras de seguridad no funciona correctamente			X		X	
R10	Se identifican puntos “ciegos” en el sistema de seguridad		X			X	
ELECTRICOS							
Riesgo/Valoración		**Probabilidad**			**Impacto**		
		A	**M**	**B**	**L**	**M**	**C**
R11	No existe conexión de polo a tierra		X			X	
R12	No existe instalación de sistema eléctrico regulado		X			X	
R13	UPS en mal estado o mal funcionamiento			X		X	
Riesgo/Valoración		**Probabilidad**			**Impacto**		
		A	**M**	**B**	**L**	**M**	**C**
R14	No existen copias de seguridad de las aplicaciones utilizadas en la institución que permita recuperar un sistema a su normalidad			X			X

R15	No se cuenta con un plan de actualización de antivirus		X				X
R16	No se cuenta con la documentación de los usuarios y perfiles de acceso a las diferentes aplicaciones			X		X	

Fuente: El Autor

Tabla 20 Matriz de clasificación de riesgos:

	Leve	**Moderado**	**Catastrófico**
Alto			
Medio		**R1, R3, R10, R11, R12**	**R4, R6, R15**
Bajo	**R2**	**R7, R8, R9, R13, R16**	**R5, R14**

Fuente: El Autor

8.3.6 Establecer lineamientos para la administración, creación, almacenamiento, recuperación, consulta y custodia de la información del sistema de gestión documental

Para este objetivo se debe tener en cuenta la estructura organizacional, con los procesos que se lideran en cada área y los respectivos roles y responsabilidades a la seguridad de la información para cada una de las áreas y oficinas, aplicando la estructura de manejo y producción de información establecer políticas documentales apoyándose en las nuevas disposiciones y normas establecidas para el manejo y disposición final de la información, teniendo en cuenta los siguientes aspectos relevantes:

- Responsables de la seguridad de la información y seguridad informática
- Responsable del cumplimiento de la normatividad vigente
- Responsables y encargado del tratamiento de los datos personales.

Para el análisis de esta información se utilizaron los siguientes instrumentos de

recolección de información:

• El organigrama de la entidad.

•La caracterización de los procesos documentada en el sistema de gestión de calidad de la entidad.

•Las funciones específicas de cada uno de los colaboradores dentro de la estructura organizacional del área de sistemas.

Responsables de la seguridad de la información y seguridad informática:

Coordinador de TICS Generar e implementar soluciones de Tecnologías de la Información (TI) que garanticen que la información este acorde al cumplimiento de los criterios de la organización y la seguridad de la información en cuanto a su disponibilidad, integridad y confidencialidad.
Planear, organizar, dirigir y controlar las actividades de mantenimiento y soporte en hardware, software, redes y comunicaciones.

Profesional de TICS: Administrar eficientemente las tecnologías de información y comunicación poniendo los recursos informáticos a disposición de los usuarios, velando por su adecuado uso y liderando proyectos tecnológicos; así como elaborar y supervisar las políticas de uso de la tecnología de información, mediante el desarrollo de sistemas y el soporte técnico a los usuarios para contribuir al logro de los objetivos organizacionales.

- ✓ Responder por el mantenimiento, control, actualización y disposición final del hardware y software de la empresa, buscando el óptimo funcionamiento de la empresa.

- ✓ Apoyar a las otras áreas de la empresa en la logística informática para la realización de reuniones, conferencias y otras.
- ✓ Administrar el software de la empresa, asignando los usuarios, perfiles y copias necesarias para que se conserve la información de la empresa.
- ✓ Implementar y supervisar políticas y normas para el aseguramiento de los activos tecnológicos
- ✓ Solucionar los impases tecnológicos y de equipos que se presenten en la organización para evitar pérdidas de tiempo y de productividad.

- ✓ Liderar proyectos de mejora o modernización de los procesos de la empresa buscando las mejores opciones para la empresa, cumpliendo los requerimientos de la Gerencia y/o departamento solicitante.

- ✓ Verificar y controlar los trabajos o servicios prestados por contratistas o proveedores del área de informática, garantizando que se cumplan los requerimientos y se satisfagan las necesidades de la empresa.
- ✓ Investigar y evaluar permanentemente los productos y servicios de tecnología de la información, así como los riesgos de seguridad en la infraestructura informática.

- ✓ Administrar y controlar los accesos a internet, asegurando una navegación óptima a los usuarios y aplicando medidas para asegurar los activos tecnológicos.

Auxiliar de soporte y mantenimiento: Mantener en condiciones óptimas la infraestructura tecnológica de la empresa y dar soporte e usuarios e ingeniero residente.

- ✓ Mantenimiento de hardware y software a servidor, estaciones de trabajo y red interna.
- ✓ Alistar y asignar los equipos de computación requeridos por los empleados, garantizando que se cumplan los procedimientos y los requisitos legales.
- ✓ Mantener los equipos informáticos, de sistemas y audiovisuales de la empresa para prestar el mejor servicio a las labores de la compañía.
- ✓ Realizar los backup a servidores, equipos locales y gerencia.
- ✓ Dar soporte eventual físico y online a ingeniero de planta.

En una empresa se debe proteger la confidencialidad, integridad y disponibilidad de la información con el fin de seguir afianzando la continuidad del negocio. Para proteger esta información de riesgos y amenazas la Empresa Contactar, se debe tener en cuenta la metodología Magerit que los clasifica en los siguientes grupos.

- Datos o información
- Las aplicaciones de software.
- Equipos informáticos
- Personal
- Redes de Comunicación
- Soportes de Información

La razón fundamental de MAGERIT está relacionada directamente con la generalización del uso de las tecnologías de la información, la cual supone unos beneficios evidentes para la protección de los activos tecnológicos e información y cuidado de los usuarios; ayudando a analizar y creando procedimientos para prevenir ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

8.3.7 Lineamientos para la información del sistema de gestión documental

Planeación documental: Relacionado con todas aquellas actividades orientadas a la producción, procesos, funciones con el fin de lograr valor a los documentos tanto análogos como digitales de la empresa, cumpliendo con lo estipulado en la ley general de archivos y legalmente, para su posterior registro y consulta en el sistema de gestión documental.
Objetivo: Considerar la normatividad en materia de gestión documental leyes y decretos actuales con referencia al programa de gestión documental impartidas por el Archivo general de la nación.

Alcance: identificación necesidades a nivel de Gestión Documental, estipular todas aquellas políticas, definición de planes y programas que contribuyan a mejorar el Sistemas de información. Aplicación y formulación de cuadros de clasificación documental-CCD, aplicación de Tablas de Retención Documental el cual es un instrumento base fundamental para la parametrizacion de todos aquellos documentos e información que se maneja en la empresa y así definir su conservación y disposición final.

Producción Documental: Comprende el estudio y análisis de todos aquellos documentos que se generan y tramitan tanto internos como externos en cada una de las oficinas resultado de cada uno de los procesos establecidos en la empresa ya sean análogos o digitales y la aplicación de normas y procedimientos establecidos en el proceso de gestión documental.

Objetivo: Tener en cuenta los principios de producción y racionalidad, de acuerdo las funciones y procesos que se manejan en las oficinas, generación de la información en sus diferentes medios y su conservación.

Alcance: Se origina con la recepción de los documentos en Ventanilla única, en el sistema de gestión documental continua con la radicación, digitalización y trámite

de documentos a los responsables, validación de la información en las oficinas y disposición final de los documentos.

- Se debe garantizar que la Documentación cumpla con estándares establecidos como validar la confidencialidad, seguridad control de folios para su trámite respectivo.
- El personal de gestión documental debe cumplir con cada uno de los instructivos, procedimientos y guías establecidos dentro del proceso de gestión documental y servir de apoyo para cada uno de los procesos que se gestionan en la empresa.
- Gestión y trámite de los documentos: Acciones necesarias a tener en cuenta para el registro e ingreso y trámite, distribución, la descripción, la disponibilidad, recuperación y control de acceso para consulta de documentos, workflow (control, seguimiento a los trámites de un proceso) hasta su disposición final y almacenamiento).

Objetivo: Resguardar la disponibilidad, recuperación, trazabilidad y acceso a la información que se genera, para así brindar y certificar respuestas oportunas a las solicitudes de los usuarios tanto internos como externos.

Alcance: surge con la consulta de información, a través del Sistema de Gestión Documental, la cual está compuesta por correspondencia interna, externa flujos de información, producción documental de las diferentes oficinas, búsqueda, recuperación y control de información.

Preservación a largo plazo: Establecer las acciones, modelos y estándares que aplican a los documentos y tipos de información durante su gestión con el fin de garantizar su preservación, consulta y protección a futuro, independiente del medio, forma de registro, producción o almacenamiento, algunas consideraciones a tener en cuenta:

- Actualización y aplicación del cuadro de clasificación de acuerdo a las funciones y procesos de las áreas, clasificación de las Tablas de retención documental con sus fases correspondientes
- Selección documental para aquellas series y subseries documentales contenidas en las TRD Tablas de retención documental
- Custodia de inventarios documentales correspondientes a cada una de las transferencias realizadas por las oficinas
- Establecer los tiempos de conservación y controles de acceso a los documentos generados
- Garantizar la consulta y reproducción de la información contenida en el sistema de gestión documental

Programa de Gestión de Documentos Electrónicos- PGDE

Establecer las normas, criterios y especificaciones técnicas necesarias para, administrar, relacionar, parametrizar, almacenar, digitalizar, consultar, proteger y conservar los archivos electrónicos de la empresa. Garantizar la autenticidad, integridad, confidencialidad y la conservación a largo plazo de los documentos así como su disponibilidad, legibilidad e interpretación, aplicando las tecnologías existentes así como mecanismos y dispositivos adecuados.

Responsabilidad sobre las políticas de la gestión electrónica de documentos

- La Subdirección administrativa, Coordinación de organización y métodos, el área de sistemas y Gestión Documental tienen como responsabilidad establecer, procedimientos y buenas prácticas que permitan una adecuada gestión electrónica de documentos en las areas de la empresa.

- El área de Sistemas, es responsable de evaluar, elegir y aplicar los mecanismos y procedimientos informáticos más adecuados para la gestión de la información y los documentos, relacionada a la implementación de nuevas

tecnologías de información, así como trabajar en conjunto con gestión documental aquellos temas relacionados con la seguridad, integridad, protección, confidencialidad de la información.

- Es responsabilidad del proceso de Gestión Documental el capacitar ,diseñar, documentar, implementar controles sobre temas de gestión documental, gestión de información, políticas y controles dentro de los procesos relacionados a cada una de las áreas.

Repositorio documental. Administrar y respaldar, toda la información que está centralizada y organizada en directorios contenida dentro del servidor dispuesto para el sistema de gestión documental.

Actualización de la información, es de vital importancia, puesto que la última versión de un documento debe ser la que se respalde en el repositorio, y así no generar copias locales de documentos con modificaciones.

Todo esto requiere la implantación de parámetros adecuados en el proceso de ir almacenando la información, la creación del repositorio y estructura de directorios según la clasificación de la información.

Asignar un espacio predeterminado al repositorio documental. Al igual que se contempla con el manejo del archivo físico soportes en papel, en cuanto a tamaño de los archivos de información megas, gigas, teras se debe prever y pensar en el crecimiento futuro, así como tener en mente las previsiones de crecimiento de información, copias de seguridad que están contenidas en el repositorio.

Tabla 21 Información y datos de activos

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[files]	Ficheros	[A_proyectos]	Archivos de Facturas,recibos, Contratos, proyectos
		[A_Clientes]	Archivos de Expedientes Clientes, historias laborales
		[A_Area Financiera]	Archivo de tesoreria,Contabilidad,presupuesto
		[A_Informes Area Administrativa]	Archivos de Informes y pólizas,
[backup]	Copias de Respaldo	[A_Copias de Seguridad]	Archivo de Copias de seguridad de la información
[conf]	Datos de configuración	[D_Configuracion_ser]	Datos de configuración de
[int]	Datos de gestión interna	[D_GestionProyectos]	Datos de Gestión de proyectos, contratos radicados y relacionados en Docunet
[password]	Credenciales	[Pass_usuarios]	Contraseñas de acceso de

Fuente: El Autor

Soportes de Información almacenamiento electrónico**.** Se considera dispositivos físicos de almacenamiento electrónico

Tabla 22 Dispositivos almacenamiento

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[cd]	Discos	[A_CD]	Almacenamientos en Disco Duro
[cd]	CDrom (CD_ROM)	[A_CD]	Almacenamiento en
[USB]	Memorias, DD	[A_Memorias]	Almacenamiento en Memorias
[dvd]	DVR	[A_DVD]	Almacenamiento en

Fuente: El Autor

Tabla 23 Software y aplicaciones

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la	Nombre activo de acuerdo a la
[app]	Servidor de aplicaciones	[Server_App]	Servidor de aplicacione
[dbms]	Sistema de gestión de bases de datos	[S_BaseDeDatos]	Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la
[Oficce]	Ofimática	[Oficce]	Office 2010
[av]	Antivirus	[Antivirus]	Kasperskyoriginal con actualizaciones
[os]	Sistema operativo	[OS_Win7]	Sistema operativo Windows 7, en su versión professional

Fuente: El Autor

Tabla 24 Redes comunicaciones

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[wifi]	Red inalámbrica	[R_wifi]	Red Inalámbrica
[LAN]	Red local	[R_Local]	Red local
[Internet]	Internet	[Internet]	Internet

Fuente: El Autor

8.3.8 Generar políticas de seguridad apropiadas que permitan garantizar la seguridad de la información, el acceso rápido y selectivo a los datos aplicando modelos y estándares establecidos

Para el desarrollo de este objetivo se debe documentar, revisar y actualizar periódicamente la producción de información dentro de la empresa, esta información ya sea en medio físico o electrónico producida a través de las diferentes herramientas y tecnologías con que se cuenta en cada una de las areas, con el fin de lograr clasificar la información que se está produciendo y así

hacer un seguimiento detallado de cada tipo de información. Una vez realizado este análisis definir una Estructura de Directorios en la cual se encontrara almacenada y clasificad la información asignando las medidas de protección correspondientes para cada nivel de información de las áreas que componen la empresa. Así como Controlar el acceso a la información se debe aplicar a todas los procesos o formas de acceso a los sistemas de información, bases de datos o servicios de información de la empresa.

Responsables de controles de acceso: Coordinador de Tics, profesional de sistemas y profesional gestión documental coordinador de OYM, esto con el fin de definir normas, pautas y procedimientos para los accesos a los sistemas, bases de datos y servicios de información (acceso a los PC, acceso a la red, acceso a los servidores, acceso a internet, acceso a claves de seguridad, acceso a transacciones etc.). Así como estandarizar los perfiles, realizar un control de los privilegios de los usuarios y concientizar a los usuarios de la importancia de la no divulgación de las contraseñas y control de acceso.

Control de Acceso a las aplicaciones: Controlar los derechos el acceso de los usuarios, restringir la información, controlar el acceso a las funciones de los sistemas, revisar las salidas de información es decir que solo se envié la información solicitada.

Monitoreo de acceso y uso de los sistemas: Revisar y monitorear que los usuarios solo estén realizando actividades que hayan sido autorizadas previamente, se debe monitorear, el acceso, la identificación de usuarios, fecha y hora de eventos, archivos accedidos, se debe supervisar el inicio y cierre del sistema, las operaciones con privilegios, cambios de configuración del sistema, intentos de acceso no autorizado, alertas fallas del sistema etc.

Definición de controles políticas y procedimientos para mitigar los riesgos:

Se realiza el estudio de las causas que originan los hallazgos, se define los controles apropiados de acuerdo a la norma ISO/IEC 27002 se establece su tratamiento, y se diseñan las políticas y procedimientos dentro de las cuales se incluyen los controles, y que finalmente irán en el diseño de acuerdo a la información y controles detallados en la empresa. Se establecen los controles de seguridad como políticas y procedimientos de acuerdo a la norma ISO/IEC 27002, se definen los más apropiados para disminuir los riesgos y se analizan de acuerdo a la empresa. Luego se determina el tratamiento de los riesgos para aceptarlos, transferirlos a terceros o aplicar los controles y posteriormente éstos se integran a las políticas y a los procedimientos institucionales si existen. Dentro de los resultados generales más importantes de la aplicación de la metodología de análisis y evaluación de riesgos, y los instrumentos diseñados están:

Algunos de los problemas de seguridad están relacionados principalmente con: el desconocimiento sobre aplicación de las normas de seguridad de la información y las limitaciones en la administración de seguridad informática. Las posibles causas origen de los problemas están: mínima cultura en el tema de seguridad de información, la organización no formal del área de Sistemas y Tics, la no existencia de responsables de la seguridad, no existencia o falta de cumplimiento de políticas y procedimientos de seguridad dentro de la empresa, fallas en el manejo de los inventarios de activos informáticos, en general la competencia limitada del personal para proteger los activos de información.

A continuación se presentan los Dominios y controles con los cuales se realiza el análisis de buenas prácticas aplicado a cada uno de los procesos y actividades que se realizan e implementan en la empresa, esta información dada por porcentaje teniendo en cuenta el conjunto de medidas, acciones y documentos planteados según ISO 27001

Tabla 25 Análisis Dominios y controles según ISO 27001

Dominio	Sección	Control	Controles Actuales		Susceptible a Mejoras	
			SI	NO	SI	NO
Política de Seguridad	5.1.1	Documento de Política de Seguridad de la Información		X	X	
Aspectos organizativos de la seguridad de la información	6.1.1	Compromiso de la Dirección con la Seguridad de la Información		X	X	
	6.1.3	Asignación de responsabilidades relativas a la seguridad de la información.	X		X	
	6.1.5	Acuerdos de Confidencialidad		X	X	
	6.2.1	Identificación de riesgos derivados del acceso de terceros		X	X	
	6.2.3	Tratamiento de la seguridad en contratos con terceros.		X	X	
Gestión de Activos	7.1.1	Inventario de Activos	X		X	
	7.1.2	Propiedad de los Activos	X		X	
	7.1.3	Uso Aceptable de los Activos	X		X	
Seguridad Ligada a los Recursos Humanos	8.1.1	Funciones y Responsabilidades	X		X	
	8.1.2	Investigación de antecedentes	X		X	
	8.1.3	Términos y condiciones de contratación	X		X	
	8.2.1	Responsabilidades de la Dirección	X		X	
	8.2.2	Concienciación, formación y capacitación en seguridad de la información		X	X	
	8.2.3	Proceso disciplinario	X		X	
Seguridad Física y Del Entorno	9.1.2	Controles físicos de entrada		X	X	
	9.1.3	Seguridad de oficinas, despachos e instalaciones		X	X	
	9.2.1	Emplazamiento y protección de equipos		X	X	
	9.2.3	Seguridad del cableado		X	X	
	9.2.4	Mantenimiento de los equipos	X		X	
Gestión de	10.2.1	Provisión de servicios	X		X	

Dominio	Sección	Control	Controles Actuales		Susceptible a Mejoras	
			SI	NO	SI	NO
Comunicaciones y Operaciones	10.4.1	Controles contra el código malicioso	X		X	
	10.4.2	Controles contra el código descargado en el cliente	X		X	
	10.5.1	Copias de seguridad de la información		X	X	
	10.6.1	Controles de red		X	X	
	10.6.2	Seguridad de los servicios de red	X		X	
	10.7.3	Procedimientos de manipulación de la información		X	X	
	10.7.4	Seguridad de la documentación del sistema		X	X	
	10.10.3	Protección de la información de registros		X	X	
	10.10.5	Registros de fallos		X	X	
Control de Acceso	11.1.1	Política de control de acceso		X	X	
	11.2.1	Registro de usuario		X	X	
	11.2.2	Gestión de Privilegios		X	X	
	11.2.3	Gestión de Contraseñas de usuario		X	X	
	11.2.4	Revisión de los derechos de acceso de usuario		X	X	
	11.3.1	Uso de contraseña		X	X	
	11.3.3	Política de puesto de trabajo despejado y pantalla limpia		X	X	
	11.4.1	Política de uso de los servicios en red		X	X	
	11.4.3	Identificación de equipos en las redes	X		X	
	11.4.6	Control de la conexión a la red	X		X	
	11.5.1	Procedimientos seguros de inicio de sesión		X	X	
	11.5.2	Identificación y autenticación de usuario	X		X	
	11.5.3	Sistema de gestión de		X	X	

Dominio	Sección	Control	Controles Actuales		Susceptible a Mejoras	
			SI	NO	SI	NO
		contraseñas				
	11.5.4	Uso de los recursos del sistema	X		X	
	11.5.5	Desconexión automática de sesión		X	X	
	11.5.6	Limitación del tiempo de conexión		X	X	
	11.6.1	Restricción del acceso a la información	X		X	
Adquisición, desarrollo y mantenimiento de los sistemas de información	12.2.3	Integridad de los mensajes	X		X	
	12.4.1	Control de software en explotación		X	X	
	12.6.1	Control de vulnerabilidades técnicas		X	X	
Gestión de Incidentes en la seguridad de la información	13.1.1	Notificación de los eventos de seguridad de la información		X	X	
	13.1.2	Notificación de los puntos débiles		X	X	
	13.2.1	Responsabilidades y procedimientos	X		X	
	14.1.2	Continuidad del negocio y evaluación de riesgos		X	X	
	14.1.3	Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información		X	X	
	14.1.5	Pruebas, mantenimiento y reevaluación de planes de continuidad		X	X	
Cumplimiento	15.1.3	Protección de los documentos de la organización		X	X	
	15.1.5	Prevención del uso indebido de los recursos de tratamiento de información		X	X	
	15.2.1	Cumplimiento de las políticas y normas de seguridad		X	X	

Fuente: El Autor

Implementación de buenas prácticas:

Cuando se estima llegar a la aplicación de los controles para mitigar los riesgos de la organización es importante tener en cuenta como primera medida la implementación de política de seguridad de la información con la cual conlleve a tener una ejecución viable que garantice la aplicabilidad del control interno informático.

Política de seguridad de la información:

La Política de Seguridad se puede definir como un conjunto de reglas, normas y procedimientos que se establecen en una empresa con el fin de administrar y dar un manejo adecuado a la información y a los sistemas de información, y de esta manera disminuir los riesgos que afecten el normal funcionamiento y continuidad de los procesos y continuidad del negocio.

Política

El propósito de esta política es proteger los activos de información de todas las amenazas, ya sean internas o externas, deliberadas o accidentales. Es política de la Empresa Contactar asegurar que:

- ✓ La información será protegida ante el acceso no autorizado
- ✓ La confidencialidad de la información estará asegurada; la información está accesible solo a aquellas personas autorizadas para tener acceso a la misma.
- ✓ La integridad de la información será mantenida, salvaguardado la precisión y la completitud de la información de los métodos de procesamiento.
- ✓ La disponibilidad de la información será asegurada así como lo requiera la organización.
- ✓ Los planes de continuidad de negocio serán producidos, mantenidos y aprobados.

- ✓ Todos los jefes de dependencias tienen responsabilidad directa en la implementación de la política en los diferentes puestos de trabajo.
- ✓ Es responsabilidad de cada funcionario acatar la política e informar inmediatamente algún incidente de seguridad.

Acceso al Sistema de gestion documental Docunet, personal de las diferentes áreas que integra la la empresa Contactar, que realice, genere documentos ya sean comunicados, oficios, facturas, cuentas, contratos, PQRS, etc, debe tener asignado un usuario y contraseña de Docunet, sera su responsabilidad su correcta administración y control documental.

Administración de cuentas de usuario del sistema de gestion documental Docunet. La creación y actualizacion corresondientes a datos de usuarios, corresponde al administrador del sistema quien será el encargado de asignar los roles de acceso de acuerdo al área que pertenezca dentro de la empresa.

Responsabilidades del personal de la empresa Contactar el personal de las oficinas de acuerdo a las funciones y tareas que realice debe cumplir con los acuerdos, términos y condiciones que regulan el uso de recursos de TI y las reglas y perfiles que autorizan el uso de la información de la empresa. Los procedimientos para estos controles y asignacion de perfiles y las características de acuerdo al área que pertenece, de acuerdo a los lineamientos dados por el área de sistemas, tanto a la información como la Red de Datos, dispositivos hardware y elementos software.

Seguridad Física y del entorno el acceso debe ser controlado y restringido a los cuartos de servidores principales, cuartos de comunicaciones. El área de Sistemas realizará y mantendra las normas, controles y registros de acceso a dichas áreas.

La Seguridad en equipos servidores que contengan información confidencial restringida deben ser mantenidos en un ambiente seguro y protegido mediante: Controles de acceso y seguridad física. Detección de incendio y sistemas de extinción de conflagraciones. Controles de humedad y temperatura. Sistemas eléctricos regulados y respaldados por fuentes UPS.

Protección contra software malicioso y hacking. los sistemas informáticos deben estar debidamente protegidos teniendo en cuenta controles humanos, físicos técnicos y administrativos. El área de sistemas debe cumplir con un conjunto de políticas, normas, estándares, procedimientos establecidos que garanticen disminuir y aplacar aquellos riesgos relacionados con amenazas de software malicioso y técnicas de hacking.

Copias de Seguridad la información que se genera en las áreas o resultado de los diferentes procesos debe estar respaldada por copias de seguridad tomadas de acuerdo a los instructivos y manuales documentados por el area de sistemas. Debe incluir las actividades de almacenamiento de las copias en sitios seguros,realizar pruebas controladas para asegurar que las copias de seguridad funcionen correctamente para luego ser leídas y restauradas sin ningun inconveniente. Se debe cumplir con un registro o historial de copias de seguridad y ser guardados en una base de datos creada para este fin.

Administración y Configuraciones de Red . La configuración de enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red; debe ser documentada, respaldada por copia de seguridad. Es responsabilidad del personal de sistemas revisar, registrar y autorizar la conexion de cualquier dispositivo a la Red de comunicaciones y datos de la empresa.

9. RECURSOS NECESARIOS PARA EL DESARROLLO

9.1 RECURSOS HUMANOS.

Tabla 26 Definición de recursos humanos.

RECURSO	Cantidad	Tiempo Horas
Responsable de realizar el proyecto	1	N/A
Análisis y estudio en cuanto a riesgos, seguridad, normatividad del sistema de información y tecnología aplicada.	N/A	120
Reuniones, asesorías con personal de oficinas sobre temas referentes a seguridad en sistemas de información.	N/A	30
Implementar controles de seguridad de la información en la empresa.	N/A	150
	TOTAL	**300**

Fuente: El Autor

9.2 RECURSOS FINANCIEROS.

Tabla 27 Definición de Recursos Financieros.

RECURSO	VALOR EN PESOS
Acceso a INTERNET	$ 70000
Compra de materiales insumos para implementar la seguridad del sistema y la información	$ 1000000
TOTAL	**$ 1.070.000**

Fuente: El Autor

9.3 RECURSOS TECNOLÓGICOS.

Tabla 28 Definición de recursos Tecnológicos.

RECURSOS	Cantidad
Video Beam	1
Memorias USB	2
PC Portátil líder desarrollador del proyecto	1
Scanner	1
TOTAL	5

Fuente: El Autor

CRONOGRAMA DE ACTIVIDADES

Tabla 29 Cronograma Proyecto

TAREAS	Productos	Técnicas y Prácticas	SEMANAS																					
			Julio		Agosto			Septiembre				Octubre				Noviembre				Diciembre				
Análisis de la necesidad del Sistema	- Descripción general del Sistema:	- Sesiones de trabajo																						
Identificación del alcance	- Descripción general:	- Factores críticos																						
	o Objetivos estratégicos relacionados con el Sistema	- Sesiones de trabajo																						
Determinación de responsables	- Descripción general del PSI:	- Sesiones de trabajo																						
	Responsables del Sistema																							
Especificación del Ámbito y Alcance	- Descripción general de procesos de la organización afectados	- Catalogación																						
	o Objetivos generales																							
	o Objetivos específicos de cada proceso (si los hubiera)																							
Organización del Sistema	- Catálogo de usuarios	- Catalogación																						
	- Equipos de trabajo	- Sesiones de trabajo																						
Definición del Plan de Trabajo	- Plan de trabajo	- Planificación																						
		- Estimación																						
Comunicación del Plan de Trabajo	- Plan de trabajo:																							
	o Aceptación del Plan de Trabajo por parte de los colaboradores																							
Estudio de los Procesos	- Modelo de procesos de la organización	- Modelado de Procesos de la Organización																						
		- Sesiones de trabajo																						
Análisis de las Necesidades de la Información	- Necesidades de información	- Modelo Entidad/Relación																						
	- Modelo de información	- Diagrama de clases																						
		- Sesiones de trabajo																						
Diagnóstico de la Situación Actual	- Diagnóstico de la situación actual:	- Matricial																						
	o Relación de sistemas de información que se conservan y mejoras																							
Definición del Modelo de Sistemas de Información	- Modelo de sistemas de información	- Matricial																						
		- Diagrama de representación																						
		- Sesiones de trabajo																						
Identificación de las necesidades de Infraestructura Tecnológica	- Alternativas de arquitectura tecnológica	- Diagrama de representación																						
		- Sesiones de trabajo																						
Informe final																								

Fuente: El Autor

CONCLUSIONES

El control del riesgo informático requiere de una planeación exhausta, para lo cual se cuenta con metodologias y estándares que ayudan a organizar la información a evaluar y a controlar, como el caso de MAGERIT e ISO/IEC 27001

Una vez identificados los riesgos y aplicada la matriz con estos, se sigue la ejecución del Sistema de Gestión de la Información, la cual suministra a la dirección información para la planificación, el control y la toma de decisiones, colaborar a la consecución de los objetivos de la empresa, lograr ventajas competitivas, generar confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad.

Se puede concluir que el analisis realizado para los riesgos identificados, el definir una metodologia, políticas de seguridad, y aplicación de los diferentes controles para la empresa Contactar teniendo como guia la ISO/IEC 27001 cumple con el objetivo principal que es garantizar la integridad, confidencialidad, disponibilidad, de la información.

Contar con un Sistema de gestion documental en una empresa garantiza la conservación de los documentos a largo plazo, redución de costos e insumos, agilizar los diferentes procesos, búsqueda y trámite oportuno de la información.

RECOMENDACIONES

Mejorar la eficacia y controles del Sistema de gestión documental.

Revisión y actualización de procedimientos y controles que afecten la seguridad de la información.

Realizar capacitaciones y brindar orientación y soporte, en temas de seguridad de la información, en cada una de las áreas de la empresa.

MEDIOS DE DIVULGACIÓN DEL PROYECTO

Para la divulgación del presente proyecto se realizara una publicación y socialización ante los empleados de las diferentes áreas de la empresa Contactar, a través de reuniones y capacitaciones, también por los medios de comunicación que cuenta la empresa como la intranet, en el menú del Proceso de Gestión Documental. Para ser publicado en internet a través de servicios como: SlideShare, Scribd enfocados al sector educativo y laboral.

BIBLIOGRAFIA

ARCHIVO GENARAL DE LA NACION, Política Archivística, Disponible en internet: http://www.archivogeneral.gov.co/

ARCHIVO GENERAL DE LA NACION, Programa de gestión documental, Disponible en: internet http://www.archivogeneral.gov.co/Internet

ISO 27000.ES. ¿Qué es un SGSI?, 2012. Disponible en: http://www.iso27000.es/sgsi.html

ISO 27001: El papel de la alta dirección en un SGSI, Disponible en: https://www.isotools.org/2015/02/04/iso-27001-papel-alta-direccion-sgsi/

MAGERIT v.3, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WD31jrLhDIU

RESUMEN ANALITICO EDUCATIVO
RAE

Título del texto	RESGUARDAR LA INFORMACIÓN DEL SISTEMA DE GESTIÓN DOCUMENTAL DOCUNET EN LA EMPRESA CONTACTAR - PASTO
Nombres y Apellidos del Autor	Mario Andrés Chaves Rosero
Año de la publicación	2017

Resumen del texto:

Un sistema de gestión documental es una aplicación o herramienta la cual permite el tratamiento, conservación, publicación y trabajo sobre documentos electrónicos, y estructura de directorios de cada uno de los procesos que se manejan en una empresa (ya sean documentos escaneados o que se hayan creado originalmente en digital). Dentro del entorno de la red se debe asegurar la privacidad de la información y de proteger las operaciones de daños no intencionados como deliberados.

La aplicación de nuevas tecnologías, la gestión de los documentos y del conocimiento hace necesario la protección de esta información y la estabilidad del sistema de gestión documental, en cuanto a software, hardware y acceso por parte del administrador del sistema como de los usuarios.

Palabras Claves	Riesgos, amenazas, metodologías, seguridad, gestión documental, confidencialidad, integridad, disponibilidad, sistemas de información

Problema que aborda el texto:

¿Cómo resguardar un sistema de gestión documental y la información que existe para mantener un sistema estable y proteger la información que se encuentra relacionada en este sistema aplicando los nuevos estándares y tecnologías que se encuentran en el medio informático?

Objetivos del texto:

- Fortalecer la seguridad y el nivel de tecnología en los sistemas de información de la Empresa Contactar Pasto
- Establecer lineamientos para la administración, creación, almacenamiento, recuperación, consulta y custodia de la información del sistema de gestión documental
- Generar políticas de seguridad apropiadas que permitan garantizar la seguridad de la información, el acceso rápido y selectivo a los datos aplicando modelos y estándares establecidos

Hipótesis planteada por el autor:

Resguardar el Sistema de gestión documental basado en ISO2700 y MAGERIT que permita preservar la integridad, confidencialidad y disponibilidad de la información en la Empresa Contactar Pasto

Tesis principal del autor:

Resguardar la información del Sistema de gestión documental Docunet en la Empresa Contactar - Pasto

Argumentos expuestos por el autor:

La metodología para la Implementación en la seguridad del Sistema de Gestión Documental involucra un componente de consultoría que busca lograr un conocimiento sobre la compañía, el negocio, sus dinámicas, flujos, visión prospectiva y diferentes aspectos de la cultura organizacional. Todo lo anterior con el objetivo de implementar el Sistema de Gestión Documental de una manera transparente que permita una apropiación más sencilla sin que se afecte la operación diaria de la compañía y buscando generar una menor resistencia al cambio por parte de los usuarios de la información y del sistema.

Debido a los diferentes riesgos y amenazas que se generan por el cambio constante en las nuevas tecnologías de la información, es necesario que las organizaciones cuenten con una estrategia o planes de seguridad basado en los riesgos y alineados con las necesidades de la razón de ser del negocio, con el objetivo de contar con un modelo de la Seguridad de la Información en aspectos como la seguridad de la infraestructura que se utiliza en lo que respecta a asegurar que nadie puede acceder a los documentos si no es a través del programa o servicios correspondientes. La gestión de acceso, protección de la confidencialidad, integridad y disponibilidad del sistema, recursos para garantizar que sólo los usuarios autorizados pueden acceder o modificarlos. Implementar

políticas y planes de gestión de seguridad de la información. La Gestión de Seguridad de la Información es fortalecer integralmente en la empresa, los pilares fundamentales de la seguridad correspondiente a la Integridad, Confidencialidad y

Disponibilidad de la información y garantizar con esto la debida protección de la información y la privacidad de la información de cada una de sus áreas y de sus partes interesadas.

Con el presente proyecto se busca establecer una metodología para resguardar la información del sistema de gestión documental en la empresa Contactar, teniendo como referencia las diferentes técnicas, herramientas y estándares que se encuentran en el medio tecnológico para llevar a cabo la implementación de gestión de seguridad de la Información lo cual, permite garantizar su efectiva implementación y asegurar su debida permanecía y evolución a futuro

Conclusiones del texto:

El control del riesgo informático requiere de una planeación exhausta, para lo cual se cuenta con metodologias y estándares que ayudan a organizar la información a evaluar y a controlar, como el caso de MAGERIT e *ISO*/IEC *27001*

Una vez identificados los riesgos y aplicada la matriz con estos, se sigue la ejecución del Sistema de Gestión de la Información, la cual suministra a la dirección información para la planificación, el control y la toma de decisiones, colaborar a la consecución de los objetivos de la empresa, lograr ventajas competitivas, generar confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad.

Se puede concluir que el analisis realizado para los riesgos identificados, el definir una metodologia, políticas de seguridad, y aplicación de los diferentes controles para la empresa Contactar teniendo como guia la ISO/IEC 27001 cumple con el objetivo principal que es garantizar la integridad, confidencialidad, disponibilidad, de la información.

Contar con un Sistema de gestión documental en una empresa garantiza la conservación de los documentos a largo plazo, reducción de costos e insumos, agilizar los diferentes procesos, búsqueda y trámite oportuno de la información.

Bibliografía citada por el autor:

ARCHIVO GENARAL DE LA NACION, Política Archivística, Disponible en internet:

http://www.archivogeneral.gov.co/

ARCHIVO GENERAL DE LA NACION, Programa de gestión documental, Disponible en: internet http://www.archivogeneral.gov.co/Internet

ISO 27000.ES. ¿Qué es un SGSI?, 2012. Disponible en: http://www.iso27000.es/sgsi.html

ISO 27001: El papel de la alta dirección en un SGSI, Disponible en: https://www.isotools.org/2015/02/04/iso-27001-papel-alta-direccion-sgsi/

MAGERIT v.3, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WD31jrLhDIU

Nombre y apellidos de quien elaboró este RAE	Mario Andrés Chaves Rosero
Fecha en que se elaboró este RAE	28/07/2017

Imagen (mapa conceptual) que resume e interconecta los principales conceptos encontrados en el texto:

Comentarios finales:

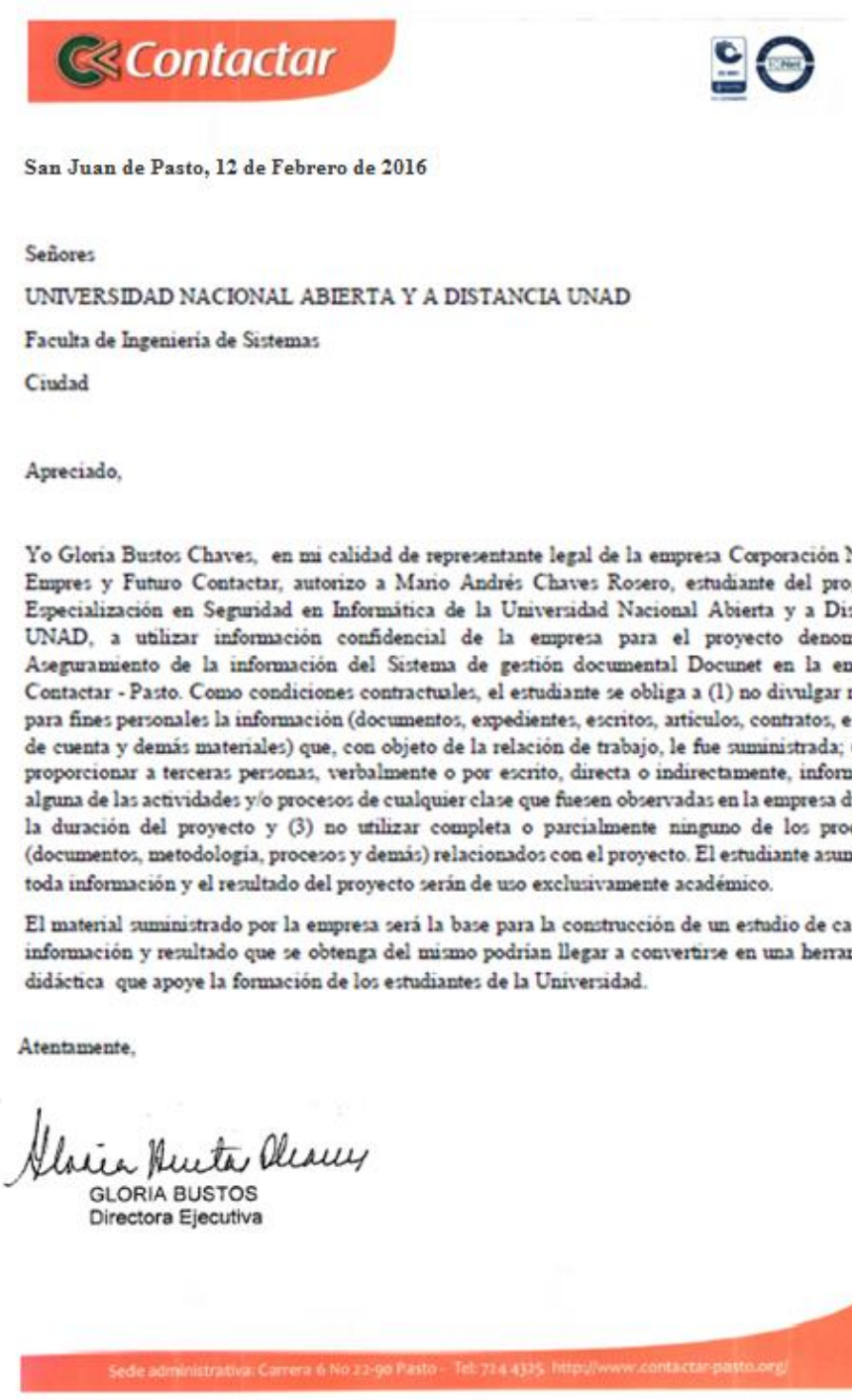
Mejorar la eficacia y controles del Sistema de gestión documental.

Revisión y actualización de procedimientos y controles que afecten la seguridad de la información.

Realizar capacitaciones y brindar orientación y soporte, en temas de seguridad de la información, en cada una de las áreas de la empresa.

ANEXOS

ANEXO A
(Carta Autorización para realizar trabajo grado en la Empresa Contactar)



Contactar

San Juan de Pasto, 12 de Febrero de 2016

Señores

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

Faculta de Ingeniería de Sistemas

Ciudad

Apreciado,

Yo Gloria Bustos Chaves, en mi calidad de representante legal de la empresa Corporación Nariño Empres y Futuro Contactar, autorizo a Mario Andrés Chaves Rosero, estudiante del programa Especialización en Seguridad en Informática de la Universidad Nacional Abierta y a Distancia UNAD, a utilizar información confidencial de la empresa para el proyecto denominado Aseguramiento de la información del Sistema de gestión documental Docunet en la empresa Contactar - Pasto. Como condiciones contractuales, el estudiante se obliga a (1) no divulgar ni usar para fines personales la información (documentos, expedientes, escritos, artículos, contratos, estados de cuenta y demás materiales) que, con objeto de la relación de trabajo, le fue suministrada; (2) no proporcionar a terceras personas, verbalmente o por escrito, directa o indirectamente, información alguna de las actividades y/o procesos de cualquier clase que fuesen observadas en la empresa durante la duración del proyecto y (3) no utilizar completa o parcialmente ninguno de los productos (documentos, metodología, procesos y demás) relacionados con el proyecto. El estudiante asume que toda información y el resultado del proyecto serán de uso exclusivamente académico.

El material suministrado por la empresa será la base para la construcción de un estudio de caso. La información y resultado que se obtenga del mismo podrían llegar a convertirse en una herramienta didáctica que apoye la formación de los estudiantes de la Universidad.

Atentamente,

GLORIA BUSTOS
Directora Ejecutiva

Sede administrativa: Carrera 6 No 22-90 Pasto - Tel: 724 4335. http://www.contactar-pasto.org/