DISEÑO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA BASADAS EN LA NORMA NTC-ISO-IEC 27001:2013 EN EL ÁREA DE AFILIACIONES DE COOPSEGUROS.

LEIDY VIVIANA YEPES CHACÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ – COLOMBIA
2017

DISEÑO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA BASADAS EN LA NORMA NTC-ISO-IEC 27001:2013 EN EL ÁREA DE AFILIACIONES DE COOPSEGUROS.

LEIDY VIVIANA YEPES CHACÓN

PROYECTO PARA OPTAR EL TÍTULO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA

MSC ING. GABRIEL RAMIREZ
DIRECTOR DE PROYECTO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ – COLOMBIA
2017

CONTENIDO

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

Pág.

INTRODUCCIÓN

Actualmente el mundo está dirigido a las mejoras tecnológicas que facilitan la vida, rápidamente las personas tienen acceso a servicios, bienes, información y comunicación. Aunque las empresas utilizan la tecnología para comunicarse mejorando sus procesos de manera efectiva, no son conscientes de las amenazas a las que están expuestas una vez le abren las puertas a la implementación de tecnología. Por este motivo se han creado leyes, procedimientos y normas diseñadas a la prevención de ataques y mitigación de riesgos informáticos.

La presente investigación se llevó a cabo en COOPSEGUROS, una pyme dedicada a la prestación de servicios de afiliación a salud, pensión y ARP de independientes y empleados que cada día crece a pasos agigantados en donde se hace necesaria la implementación de programas de desarrollo tecnológico para el control y protección de la compañía, cumpliendo las exigencias regulatorias y de ley, que le permitan reducir los riesgos económicos y administrativos.

Este proyecto de investigación se realiza con el fin de valorar los activos informáticos, analizando las vulnerabilidades, amenazas y riesgos existentes a nivel de seguridad informática que pueden afectar el proceso de afiliaciones, los recursos y el prestigio de la organización; en consecuencia para contrarrestar y mitigar los riesgos identificados en Seguridad Informática, se diseñan Políticas de seguridad Informática, acordes a las actividades propias del negocio.

De acuerdo con lo anterior el presente proyecto pretende identificar y establecer políticas de seguridad Informática, que protejan los activos de información, teniendo en cuenta la infraestructura, los aplicativos o procesos establecidos para el manejo de información en el área de afiliaciones, para ello se estudiará el marco teórico referente al tema, se identificaran los activos de información, las vulnerabilidades y amenazas en Seguridad Informática, se realizará el análisis de riesgos el cual le dará las bases a la compañía para diseñar una Matriz de Riesgos que permitirá determinar las acciones que debe tomar para mitigar los riesgos identificados y salvaguardar los activos de información.

1. PLANTEAMIENTO DEL PROBLEMA

La tecnología avanza a pasos agigantados y así mismo aumentan las vulnerabilidades aprovechadas por los delincuentes informáticos. Es una tendencia mundial y los Hackers ya no actúan por un hobbies sino que son organizaciones criminales reconocidas que buscan atentar contra la integridad, disponibilidad y confidencialidad de la información, aprovechando el alcance que tienen las personas a la tecnología.

El internet ha facilitado la vida de las personas a nivel personal y laboral, es así como prefieren realizar búsquedas de cualquier tema a través de esta herramienta sobre cualquier otro medio; a su vez el ser humano ha encontrado la manera de desarrollar diferentes actividades diarias de forma ágil, mediante el uso de los electrodomésticos y aparatos electrónicos, sin embargo con estos avances tecnológicos también se desencadenan una serie de riesgos que las personas no han logrado dimensionar, por lo mismo no buscan mecanismos de protección para sus sistemas de información y sus datos sensibles. [1]

En Colombia el 05 de enero de 2009, el Congreso de la Republica, divulgó la ley 1273 “De la protección de la información y de los datos” modificando el Código Penal. Esta ley normalizó una serie de delitos relacionados con el manejo de los datos personales, lo que implica que las compañías lo incluyan dentro de sus políticas y procedimientos con el fin de evitar incumplimientos legales.[2]

COOPSEGUROS, es una empresa constituida en el año 2008 es de carácter privado y su objetivo principal es prestar servicios de afiliación a seguridad social, pensión y riesgos profesionales para independientes y empresas. Actualmente la compañía ha incrementado su operación y las relaciones comerciales con sus clientes, sin embargo COOPSEGUROS no cuenta políticas de Seguridad

[1] Tecnología del futuro, disponible en: http://nizquierdo3.botot.com.co/2012/12/la-facilidad-de-la-nueva-era.html

[2] Colombia, Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado –denominado "de la protección de la información y de los datos"- y se conservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones, disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html

Informática definidas, los funcionarios del área de afiliaciones desconocen los cuidados que deben tener para proteger la Seguridad informática y sin saberlo realizan acciones que ponen en riesgo a la empresa.

La información de las compañías es procesada, intercambiada o conservada en bases de datos, equipos informáticos o herramientas de almacenamiento que hacen parte de los sistemas informáticos de la organización, estos sistemas están expuestos a riesgos potenciales que pueden atentar contra la seguridad de la compañía. Estos riesgos se pueden clasificar así: los riesgos físico, como desastres naturales, incendios y/o accidentes provocados de manera involuntaria; por otra parte esta los riesgos lógicos, como los producidos por delincuentes informáticos, quienes roban la información, sabotean los sistemas o realizan ataques maliciosos a la compañía, entro otros.[3]

1.2. FORMULACIÓN

¿Cuáles son los riesgos de los activos de información del área de afiliaciones de COOPSEGUROS y cómo mejorar la seguridad de los mismos basados en la norma NTC-ISO-IEC 27001:2013?

1.3. DELIMITACIÓN DEL PROYECTO

De acuerdo con la limitación temática se tiene establecido identificar las políticas de seguridad informática basados en la Norma ISO NTC IEC 27001:2013 que ayuden y orienten al Gerente y funcionarios del área de afiliaciones a mejorar la seguridad de la información en el proceso de afiliaciones de COOPSEGUROS.

[3] Metodología para la gestión de la Seguridad Informática
http://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf

2. OBJETIVOS

2.2. OBJETIVO GENERAL

Diseñar políticas de seguridad informática para el área de afiliaciones de COOPSEGUROS, tomando como referencia la norma NTC-ISO-IEC 27001:2013-

2.3. OBJETIVOS ESPECÍFICOS

- Identificar los activos de información, del área de afiliaciones de COOPSEGUROS

- Analizar las vulnerabilidades, amenazas y riesgos existentes en los sistemas de información basado en la norma NTC –ISO-IEC 27001:2013

- Valorar el impacto de los riesgos de Seguridad Informática identificados en el área de afiliaciones de COOPSEGUROS

- Elaborar un plan de divulgación, sensibilización y capacitación en políticas de Seguridad Informática.

3. JUSTIFICACIÓN

Este proyecto permite identificar si la empresa cuenta normas o procedimientos sobre la protección de datos personales, privacidad, control y aseguramiento de la información en el área de afiliaciones de COOPSEGUROS basado en la norma NTC-ISO-27001[4] lo cual permitirá hacer un aporte a la metodología que debe utilizar la compañía para el aseguramiento informático.

COOPSEGUROS ha venido demostrando un crecimiento en sus operaciones, sin embargo no se tiene establecido quién es el responsable de determinados activos de información, quién y de qué manera debe otorgar los accesos y permisos a los sistemas de información. Una vez analizados los activos informáticos, redes y los sistemas de comunicación que se tengan implementados en el área de afiliaciones de la compañía se logrará identificar:

Las vulnerabilidades y amenazas existentes en los sistemas de información, aplicabilidad de los estándares de seguridad informática, la funcionalidad de los procedimientos establecidos a nivel de seguridad informática. Con el desarrollo del punto anterior, se consigue: mitigar las vulnerabilidades, amenazas y riesgos encontrados a nivel de Seguridad Informática; asegurar el funcionamiento y calidad de los sistemas de información y optimizar la seguridad de los activos de información y los sistemas de comunicación en el área de afiliaciones de COOPSEGUROS.

El punto inicial para la Gestión de la Seguridad de la Información en una empresa son las políticas de seguridad, mediante el diseño y aplicación de ellas se crea cultura de seguridad la cual debe involucrar a todos los usuarios, clientes, proveedores y directivos de la organización con el fin de luchar para proteger sus activos de información. El objetivo principal de las políticas de seguridad

[4] NTC-ISO/IEC 27001 Tecnología de la Información. Técnicas de Seguridad. Sistemas de la Gestión de la Seguridad de la Información (SGSI) Requisitos. Norma Técnica Colombina. Icontec Internacional

informática es preservar la integridad, confidencialidad y disponibilidad de los sistemas y la información de compañía.[5]

Para realizar un adecuado diseño de políticas de seguridad informática es necesario contar con el compromiso de la alta dirección de la compañía, de esto dependerá el éxito y cumplimiento de las mismas. Se puede definir que la política de seguridad es un documento diseñado por un alto nivel de la organización que busca proteger los sistemas informáticos, estableciendo las bases para definir y limitar responsabilidades en diferentes actividades sobre un sistema.[6]

Por lo anterior se observa la necesidad de diseñar e implementar políticas de seguridad informática, las cuales deben ser documentadas, aprobadas y divulgadas al interior de la organización como cumplimiento regulatorio, legal técnico. Estandarizar actividades que se realicen de forma similar, asignar roles, responsabilidades, al proceso de afiliaciones de la compañía, implementar mejores prácticas de seguridad informática en el trabajo, de acuerdo con la actividad económica de la empresa.

[5] Políticas de seguridad a nivel de TI, disponible en: http://capacityacademy.com/2014/03/17/son-las-politicas-de-seguridad-de-la-tecnologia-de-la-informacion/

[6] Políticas de seguridad de la información, disponible en: http://www.segu-info.com.ar/politicas/polseginf.htm

4. MARCO DE REFERENCIA

4.1. ANTECEDENTES

Caso de Estudio de Seguridad Informática para las Bases de Datos del Campus Virtual de la UNAD, realizado por Carlos Javier Uribe Otálora, en el año 2016.
A nivel de políticas de seguridad se cuenta actualmente con normas en seguridad Informática, como la ISO 27000 que a través de entidades normalizadores británicas como la British Standards Institution.

Dado lo anterior se fueron publicando documentos sobre prácticas de seguridad para las empresas en el año 1995. Desde entonces se empezó a gestar la familia 27000 en el año 2000 como un requisito para un Sistema de Gestión de la Seguridad de Información (SGSI) que puede ser aplicado a nivel internacional, se han presentado cambios o complementos en la misma como la norma ISO 17000.[7]

Propuesta de trabajo de grado en la Universidad EAN en la facultad de Ingeniería de la cuidad de Bogotá presentado por Sandra Milena Daza y Andrés Giraldo Murillo "Aplicación de un sistema de Gestión de Vulnerabilidades para la Infraestructura Informática de ABC Ltda., en la que se plantea el siguiente problema: ABC requiere incorporar buenas practicas aplicadas a sus procesos y procedimientos que garanticen una gestión adecuada de las vulnerabilidades y riesgos a nivel informático para asegurar el cumplimiento contractual de la compañía.

Dado lo anterior, se realiza un análisis de la infraestructura de la compañía identificando las vulnerabilidades y amenazas de seguridad informática y por cada vulnerabilidad identificada realizan recomendaciones, proponiendo planes de acción para mitigar los riesgos y protección de la infraestructura informática de la compañía.[8]

Propuesta de trabajo de grado para obtener el título de Ingeniero Informático de la

[7] UBIRBE Otálora Carlos Javier, Estudiante de Ingeniería de Sistema de la Universidad Nacional Abierta y a Distancia UNAD, presenta proyecto de Seguridad Informática para las Bases de Datos del Campus Virtual de la UNAD, http://www.iso27000.es/iso27000.html

[8] "Daza Sandra Milena Y Giraldo Murillo Andrés, estudiantes de Ingeniería de Sistemas de la EAN realizan investigación de Aplicación de un sistema de Gestión de Vulnerabilidades para la Infraestructura Informática de ABC Ltda.
Minerva.ttp://biblioteca.universia.net/html_bura/ficha/params/title/aplicacion-sistemagestion-vulnerabilidades-infraestructura-informatica-abc-ltda/id/55867643.html
http://tesis.ipn.mx/jspui/bitstream/123456789/8428/1/IF2.52.pdf.

Universidad Autónoma de Occidente en la ciudad de Santiago de Cali, presentado por José Luis Jaramillo Lara, tema: Estandarización de Políticas y controles de seguridad de la información para el proceso “Gestionar la Seguridad Informática y la Continuidad de las Soluciones de TIC” (MP11P4).

Planteamiento del problema presentado, brindar respuesta a la pregunta ¿qué políticas, procedimientos y controles de seguridad de la información con base en la norma ISO /IEC 27001 son aplicables para el proceso “Gestionar la Seguridad Informática y la Continuidad de las Soluciones de TIC” en el Departamento Administrativo de las TIC de la Gobernación del Valle del Cauca? El trabajo se desarrolló a través del análisis de riesgos y la gestión del riesgo de seguridad de la información, estandarización de políticas de Seguridad de la información.[9]

Otro tema investigado fue: “el Modelo de Evaluación de Riesgos en activos Tic´s para pequeñas y medianas empresas del sector automotriz” desarrollado por la Ingeniera Diana Moncayo de la facultad de Ingeniería de Sistemas de la Escuela Politécnica Nacional de la ciudad de Quito- Ecuador, en el cual se plantea un modelo basado en la metodología de Magerit para identificar vulnerabilidades, amenazas, riesgos y la implementación de salvaguardas como apoyo a la evaluación de riesgos realizada. La implementación de este modelo de evaluación de Riesgos es recomendable para las pequeñas y medianas empresas debido a que permite conseguir resultados prácticos a costos y tiempos menores referidos a procesos estándar.[10]

4.2. MARCO DE CONTEXTO

COPSEGUROS, es una compañía especializada y calificada para ofrecer servicios con calidad en afiliación a la Seguridad Social, Pensión y Riesgos profesionales a las empresas e independientes. Trabaja con las más importantes entidades tanto del sector público como privado para brindarles a sus clientes mayor cobertura y calidad del servicio. Actualmente cuenta con un registro amplio de clientes, quienes han depositado su confianza en la compañía; al momento de llevar a cabo su trabajo.

[9] JARAMILLO Lara Jose Luis, presenta Propuesta de trabajo de grado para obtener el título de Ingeniero Informático de la Universidad Autónoma de Occidente en la ciudad de Santiago de Cali, tema: Estandarización de Políticas y controles de seguridad de la información para el proceso “Gestionar la Seguridad Informática y la Continuidad de las Soluciones de TIC” (MP11P4). presentado por https://red.uao.edu.co/bitstream/10614/5187/1/TIS01570.pdf.

10 MONCAYO Diana, estudiante de Ingeniería de Sistemas de la Escuela Politécnica Nacional de la ciudad de Quito- Ecuador el Modelo de Evaluación de Riesgos en activos Tic´s para pequeñas y medianas empresas del sector automotriz.

El desarrollo del proyecto se realizará únicamente en el área de afiliaciones de la compañía, esta área cuenta con la participación de 7 funcionarios capacitados para atender y cumplir con la prestación de los servicios ofrecidos por la entidad a empresas e independientes.

COOPSEGUROS cuenta actualmente con una sede en la ciudad de Bogotá en Colombia, sus servicios son ofrecidos únicamente en esta ciudad; dentro de los objetivos de la compañía está en expandir sus servicios a zonas aledañas a la ciudad de Bogotá y en un futuro no muy lejano iniciar operaciones en las ciudades de Medellín y Villavicencio.

En el área de afiliaciones de la compañía se centra el gran volumen de la operación, es en este departamento en dónde se recibe la información de los clientes, se verifican los datos y se realizan los trámites para la afiliación a salud, pensión y riesgos profesionales con las más prestigiosas entidades del país, de este proceso dependerá la calidad de servicio ofrecida a los clientes.[11]

A lo largo del desarrollo de este trabajo se van a identificar los activos con lo que dispone el área de afiliaciones de COOPSEGUROS a nivel de software, hardware, comunicaciones, sistemas de vigilancia, medios externos y el personal involucrado en el proceso, con el fin de alertar a la organización de las amenazas a las que se encuentran expuestos, generando impactos negativos en cuanto a la parte financiera, imagen de la empresa, incumplimientos y sanciones legales, entre otras.

4.3. MARCO TEÓRICO

Las organizaciones siempre estarán expuestas a distintos tipos de amenazas, como se ha visto en la fase de Análisis de Riesgos; las amenazas pueden proceder desde varias fuentes y contienen un nivel de peligrosidad distinto, lo cual depende tanto del activo como de la situación específica en que una vulnerabilidad sea explotada.

Cualquier tipo de amenaza, afecta de alguna manera bien sea directa o indirectamente a los Procesos de Negocio de la organización; el nivel en que estos pueden ser afectados es conocido como impacto, y se sabe que, aunque se implementen salvaguardas para reducir estos niveles, es imposible reducir su nivel

[11] COOPSEGUROS, [en línea] [citado el 11 de noviembre de 2017] disponible en internet: https://www.coopseguros.com.co/

a cero.

Dado lo anterior se puede decir, que independientemente a los Sistemas y Estrategias de Control, la naturaleza de una organización es ser vulnerable; por esta razón es importante incluir dentro de la Gestión de Riesgos Políticas de seguridad informática que garanticen el cumplimiento la confiabilidad, disponibilidad e integridad de la información.

El desarrollo de este proyecto está enfocado en el diseño de políticas de seguridad informática en el área de afiliaciones de COOPSEGUROS, teniendo en cuenta la misión, visión y objetivos de la compañía. Recopilando información del proceso ejecutado por los colaboradores, en dónde se identifiquen las vulnerabilidades y riesgos a los cuales está expuesta la compañía.

Norma ISO 27001

La norma ISO ISO/IEC 27000 estructura un marco de gestión de la Seguridad de la información, aplicable a cualquier tipo de empresa (privada, pública, grande o pequeña). En su anexo A enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean analizados y divididos por las organizaciones durante el desarrollo del SGSI, no es necesaria la implementación de todos los controles, sin embargo se debe justificar la no aplicabilidad de los controles que no son tenidos en cuenta.[12]

Este proyecto tiene como marco de referencia la norma ISO27001:2013 toda vez que se plantean temas como la mejora continua en la seguridad de la información en las organizaciones y sobre ella se describen los siguientes temas que son clave al momento de desarrollar este trabajo:

Figura 1. PHVA

[12] Norma ISO ISO/IEC 27000, https://advisera.com/27001academy/es/que-es-iso-27001/

Figura 1 Pasos clave para implementación de un Plan de Continuidad del Negocio

La Figura 1 muestra un breve resumen de la propuesta realizada por la normativa para la implementación del Plan de Continuidad de Negocio. [13]

Sistema de Gestión de la Seguridad de la Información (SGSI)

El (SGSI) es una herramienta que le permite a las empresas implementar estratégicamente políticas, procedimientos y controles de seguridad informática alineados a los objetivos de cada negocio, esto a fin de evaluar el nivel de riesgo e implementar las acciones de mitigación de los mismos, documentando el proceso de forma estructurada, continua, eficiente y flexible que permita adaptarse a los diferentes cambios que se produzcan en la compañía a nivel de riesgos, entorno y las nuevas tecnologías.

Mediante la implementación de un Sistema de Gestión en Seguridad de la Información las compañías mantienen un proceso de mejora continua a través del modelo (PHVA) planear, hacer, verificar y actuar, lo cual permitirá gestionar de manera eficiente el aseguramiento de la información garantizando la confidencialidad, integridad y disponibilidad de los activos de información, asignados roles y responsabilidades a cada uno.

Planear

Se define el alcance que tendrá el plan de continuidad, cuáles son sus objetivos y los incidentes más relevantes a ser atendidos. Algunas de las tareas a desarrollar en esta etapa son: definición de los objetivos del plan, delimitación y alcance, identificación y descripción de escenarios críticos, revisión del Análisis de Riesgos

[13] Plan de Continuidad de Negocio, http://www.iso27000.es/iso27000.html

para estudio de las amenazas, vulnerabilidades, salvaguardas y estado actual de los activos., selección de los incidentes más relevantes para la organización, Identificar los Procesos de Negocio involucrados y atendidos en el plan.

Creación de estrategias para dar contingencia y mitigación a los incidentes seleccionados, estimación de medidas de tolerancia, cuánto tiempo y costos puede (como máximo) llevar a cabo el plan (Concepto de RTO y RPO). Identificación de Recursos y Tareas y delegación de tareas e identificación de actores.

Hacer.

En esta etapa se implementan las estrategias que han sido planteadas anteriormente. Algunas de las tareas a desarrollar en esta etapa son: implementación de estrategias para dar contingencia y mitigación, a los Procesos de Negocio involucrados, creación del plan piloto de continuidad de negocio, identificación de mejoras de las estrategias, corrección e implementación de las mejoras a las estrategias.

Verificar.

Se toma la última versión del plan piloto anteriormente definido, procediendo a realizar una verificación del mismo. Algunas de las tareas a desarrollar en esta etapa son: definición de los simulacros para recrear escenarios críticos, ejecución de simulacros para la verificación del plan piloto, medición de niveles de tolerancia estimados en la fase de verificación; medir RTO y RPO entre otros, definir en qué nivel ha sido cumplido o incumplido el plan de continuidad, teniendo en cuenta las medidas de tolerancia y aplicación de correctivos o mejoras, si es necesario se puede repetir la etapa de Hacer.

Actuar.

Al final debe ejecutarse el plan de continuidad y establecerse dentro de los planes de Gestión de Riesgo de la organización. Algunas de las tareas realizadas en este punto son: implementación de las estrategias en ambientes reales, supervisión de las tareas y pasos realizados, medición de niveles de tolerancia estimados en la fase de verificación; medir RTO y RPO entre otros y establecer una reevaluación del plan, si es necesario.

Como se puede observar, los pasos se encuentran en función a todo flujo de un plan de mejora continua; siendo un proceso cíclico en constante evolución, encontrándose actualizado según los nuevos requerimientos y procesos de la organización, es importante que se involucre a todos los funcionarios de la compañía con el fin de hacer un proceso ágil y eficiente.

Cabe aclarar que un Plan de Continuidad de Negocio, no se encuentra específicamente dirigido hacia la Seguridad de la Información; sin embargo, al tener en cuenta que los Sistemas de Información juegan un papel crítico dentro del ámbito de las organizaciones es usual encontrar muchas referencias entre un Plan de Continuidad de Negocio y la implementación de Sistemas de Gestión de la Seguridad de la Información o manejos de Incidentes de Seguridad.[14]

Seguridad informática en bases de datos

Las bases de datos son las que almacenan la información sensible de las compañías, contiene datos personales de los clientes, información financiera, comercial, de la gestión de los servicios ofrecidos, de los empleados, entre otras, por lo anterior se considera que la seguridad informática en las bases de datos es altamente critica.

Las empresas hoy en día deben necesariamente contemplar un plan de seguridad informática en el que involucre la participación de los funcionarios de la compañía, a través de la divulgación y capacitación con el fin de generar compromiso, así mismo se tendrá en cuenta la disponibilidad de recursos económicos, técnicos y tecnológicos, la implementación de controles y la evaluación de los mismos periódicamente, identificando las debilidades y fortalezas de la organización.[16]

Una vez identificados los riesgos a los que están expuestas las bases de datos, es importante implementar medidas de aseguramiento con el fin de asegurar los servidores que contienen estas bases de datos, buscando siempre proteger la información sensible de la compañía de posibles amenazas, mitigando las vulnerabilidades y minimizando los riesgos.

Plan de contingencia

Un plan de contingencia se define como el proceso alternativo que tiene una organización para realizar su funcionamiento normal, en caso de ocurrir una eventualidad de carácter externa o interna. La implementación del Plan de continencia le va a permitir a las compañías reducir las pérdidas económicas, productivas, de información, de personal, clientes, entre otras, ocasionadas por las

[14] Norma ISO ISO/IEC 27000, https://advisera.com/27001academy/es/que-es-iso-27001/

[16] Seguridad en bases de datos, https://msdn.microsoft.com/esco/library/cc434708%28v=vs.71%29.aspx?f=255&MSPPError=-2147217396

eventualidades que puedan parar el flujo normal de actividades de la organización.

Para elaborar un plan de contingencia se deben considerar las siguientes etapas, que van a dar una orientación a la empresa a nivel de prevención y ejecución del plan en caso de presentarse un siniestro, a continuación se describen las etapas en las que se basa el plan de contingencia (Evaluación, planificación, pruebas de viabilidad y la ejecución):[17]

Etapa de Evaluación: Es necesario que exista un equipo responsable de monitorear periódicamente la efectividad de los planes creados por la compañía, evaluando todas las situaciones que se puedan presentar.

Planificación: Mediante la evaluación de los riesgos y el impacto que pueda tener la ocurrencia del evento, se deben plantear las acciones que se implementarían para mitigar el riesgo o minimizar el daño que puede causar-

Pruebas de viabilidad: Es la metodología establecida para documentar los procedimientos que se utilizaron para realizar las diferentes pruebas de las vulnerabilidades identificadas, los cuales deben contar con especificaciones técnicas, tecnológicas, financieras, de personal, esta documentación debe reposar en una parte visible y conocida al interior de la organización, con el fin de tener una respuesta oportuna en caso de presentarse una eventualidad.

Ejecución: En esta etapa se deben tomar con inmediatez los planes de contingencia elaborados por el equipo encargado de asegurar las pruebas y documentar el procedimiento a seguir en caso de materializarse un riesgo, esto para responder a la operación normal del negocio y a los servicios informáticos de la compañía.

Análisis de riesgos

El incremento de la tecnología y la manera como las personas y las empresas se han venido involucrando más en estos temas, han hecho que los riesgos a los que están expuestos sean cada día de mayor complejidad lograr protegerse, la puerta es más grande para dejar entrar el avance tecnológico y todos los beneficios que trae consigo, pero a su vez el incremento de las vulnerabilidades.

El análisis de riesgos surge a partir de la necesidad de organizar datos con el fin de entregar información confiable a las organizaciones, es un proceso que se puede aplicar a cualquier tipo de organización bien sea de carácter público o

[17] Ciclo PHVA del SG-SST, Plan de contingencia, http://www.bdigital.unal.edu.co/57426/42/43092659.2017.ANEXO%202.pdf

privado. El objetivo del análisis de riesgos es hacer una proyección hacia el futuro basados en un pasado seguro y una metodología de análisis definida de los acontecimientos.

Dado lo anterior, se evalúan los controles de seguridad físicos y técnicos de una organización, priorizando acciones para reducir la probabilidad de ocurrencia de los riesgos a nivel de sistemas de información. Es necesario seguir una metodología que involucre a los diferentes funcionarios de las distintas áreas de la compañía, debido a que nadie mejor para identificar los posibles riesgos a los que están expuestos y llevar a una solución para mitigar los mismos.[18]

Determinación de los activos

Un activo es un bien que representa un valor o una utilidad para la organización, es por esto que se debe valar por su protección asegurando la operación y continuidad del negocio, de acuerdo con lo dispuesto en la norma ISO 17799:2005 (Código de práctica para la gestión de la Seguridad de Información) le da una clasificación a los activos así:

Activos de información como: las bases de datos, documentación del sistema, archivos de datos, manuales de usuarios, procedimientos internos, de capacitación o continuidad del negocio.

Documentos impresos: Normas, contratos, procedimientos, lineamientos, políticas de la compañía.

Activos de Software: Software de aplicación, software del sistema y/o herramientas de desarrollo.

Activos físicos: Todos los equipos electrónicos, de computación, comunicación y todos los equipos técnicos de la compañía.

Personas: Clientes internos, funcionarios, clientes externos, proveedores, socios. Imagen y reputación de la empresa

Servicios: Todos los servicios de tecnología y sistemas, entre otros servicios técnicos.

Dependencias entre los activos

[18] Guía de Administración del Riesgo, http://www.dafp.gov.co/

La dependencia de los activos hace referencia a la afectación o en las implicaciones que puede incurrir un activo superior por la vulnerabilidad de la seguridad de un activo inferior, esto se presenta por la sinergia de los procesos de la compañía, en dónde se involucran varias áreas para el desarrollo de una actividad específica.

Lo anterior se puede definir como una dependencia de los activos superiores al buen funcionamiento y seguridad de los activos inferiores, por lo que es necesario implementar medidas de prevención y aseguramiento que no generen conflicto entre los activos superiores e inferiores. En cada caso hay que aplicar a la organización que sea objeto de análisis el conjunto de activos en capas en donde las capas superiores dependen de las inferiores.[19]

Valoración de los Activos

Luego de realizar el proceso de identificación de activos, se procede a realizar el proceso de valoración, esto hace referencia a la asignación de un valor de acuerdo con el grado de importancia, manteniendo las bases de la Seguridad de la Información: integridad, disponibilidad, confiabilidad de cada uno de los activos. Esta valoración puede hacerse de manera cuantitativa (escala de valor numérico) o cualitativa (escala por niveles).

Para realizar el proceso de valoración es necesario contar con la experiencia de los dueños de proceso o las personas que ejecutan el proceso, debido a que será una ventaja para la identificación de los activos y una realidad de la probabilidad de ocurrencia de un posible riesgo y valorar el impacto que tendría la materialización del mismo en la organización.

La valoración de activos debe ser realizada por un grupo de profesionales que de acuerdo con su experiencia aporten una visión objetiva y razonable al análisis realizado, generando un valor a la organización. De acuerdo con la metodología seleccionada es necesario conocer la organización y los procesos, adicionalmente recolectar información para valorar los activos de acuerdo con entrevistas, encuestas realizadas a los funcionarios involucrados.[20]

Criterios de valoración

[19] PADILLA PACHA Cristina, Análisis de riesgos Informáticos para la protección de los Sistemas de Información en el área de Tecnologías de Información del Gobierno Tunguragua.2012 p.79
[20] Activos de Seguridad de la Información, http://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-7.pdf

Es importante identificar el grado de afectación que tendría la materialización del riesgo, por lo anterior es indispensable definir criterio para la identificación del impacto sobre el activo y la organización. Las siguientes definiciones pueden ayudar a establecer conceptos claros de valoración e impacto:

Autenticidad, ¿Cuáles podrían ser las consecuencias si se llegara a descifrar las claves de los equipos informáticos en una organización? La pregunta responderá el nivel de riesgo al que está expuesta la organización a nivel de autenticación y seguridad de cada usuario en los equipos a los que tienen acceso.

Confidencialidad, ¿Qué podría pasar en el caso que personal no autorizado tuviera acceso a los sistemas de información en la compañía? La respuesta a esta pregunta dará a la organización una valoración de la materialidad de un riesgo de fuga o pérdida de información confidencial de la compañía.

Disponibilidad, ¿Cómo responder ante un ataque al sistema de información de la compañía que impide el acceso al personal autorizado? La respuesta a este interrogante permitirá valorar los riesgos asociados a la continuidad del negocio y el funcionamiento de la operación.

Integridad, ¿Qué nivel de protección tiene establecido la organización para evitar vulnerabilidades de sus bases de datos, y para la información de la compañía y de sus clientes internos y externos que circula por los diferentes medios de comunicación? La respuesta al anterior cuestionamiento le permitirá a la organización valorar los riesgos asociados a garantizar la veracidad de la información.

Identificación de amenazas

Una amenaza es la probabilidad de ocurrencia de un incidente que pueda implicar afectaciones negativas para la compañía, de la materialización de una amenaza podría tener afectaciones a nivel de integridad, confidencialidad, autenticidad y la disponibilidad de los activos de la organización. Las amenazas se pueden presentar en un activo en particular o en un proceso que incluya la participación de varios activos, se pueden clasificar en consideradas o accidentales de acuerdo con el nivel de intencionalidad que se identifique.

Consideradas: Son las amenazas que han sido planificadas por la organización en las que se estima un valor de perdida y afectación, pero que también se

establecen mecanismos para disminuir el impacto de las mismas, como hurto, fraude, sabotaje, entre otros.

Accidentales: Son las amenazas que no deberían "existir" ocurren sin intención de dañar a la organización pero que terminan en implicaciones negativas para la misma. Estas amenazas pueden ocurrir en cualquier momento y predecirlas no es fácil pero deben ser consideraras dentro de la evaluación, algunas de estas amenazas son: averías en hardware, software, desastres naturales, entre otros.

Para determinar el grado de afectación y la probabilidad de ocurrencia de cada amenaza sobre cada activo de la compañía, se evalúa conforme la siguiente tabla de valoración:[21]

Criterios de Valorización			
MA	100	Muy frecuente	A diario
A	10	Frecuente	Mensualmente
M	1	Normal	Una vez al año
B	1/10	Poco frecuente	Cada varios años
MB	1/100	Muy poco frecuente	Siglos

Tabla 1. Probabilidad de Ocurrencia
Fuente: Magerit versión 3 p.28

El grado de afectación se debe realizar para cada activo, esto se hace con referencia a la amenaza y la dimensión; se mide entre el 0% y 100%.

Estimación del impacto

Producto de la materialización de una amenaza sobre un activo, se calcula el daño causado bien sea al activo o a la cadena del proceso que de él dependía. Una vez se tiene la valoración de los activos y el porcentaje de afectación de la materialización de las amenazas, se puede identificar el impacto que esto tiene sobre los sistemas de información de la compañía. La consecuencia de esta materialización podría traer a la compañía pérdidas cualitativas o cuantitativas que de acuerdo al nivel de afectación podrían parar completamente el funcionamiento de los procesos.

[21] GAONA VASQUEZ Karina, Aplicación de la metodología MAGERIT para el análisis y gestión de riesgos de la seguridad de la información en la empresa Persquera e Industria Barvito S.A, Cuenca octubre 2013

Identificación de riesgos

Este proceso le permitirá a las organizaciones identificar los riesgos potenciales a los que están expuestos para cada activo, mediante alguna de las siguientes técnicas de identificación: árboles de fallos, árboles e eventos, método Delphi, análisis probabilístico de Seguridad, entrevistas, encuestas, o mediante un análisis DOFA.

MAGERIT.

Metodología de Análisis y Gestión de los Sistemas de Información, permite medir la vulnerabilidad por la frecuencia cuantitativa de la materialización de una amenaza sobre el activo, cuando sea factible o por la afectación cualitativa que pueda tener dicha materialización, que llevará a utilizar una tabla de acuerdo al nivel de amenaza.

Valoración de riesgos

Una vez se tiene la identificación de los activos, la identificación de las amenazas y la probabilidad de ocurrencia de una amenaza sobre cada uno de los activos de la compañía, se realiza la evaluación de los riesgos. El nivel de riesgo se divide en los siguientes niveles:

Bajo: la probabilidad de ocurrencia es baja, es necesario implementar salvaguardas adicionales que mitiguen este riesgo.

Medio: El nivel de probabilidad es medio y es necesario evaluar por parte de los implicados en el proceso que salvaguardas se deben implementar para evitar la materialización del riesgo.

Alto: La probabilidad de ocurrencia es alta y se hace obligatorio implementar salvaguardas para mitigar la materialización de los riesgos.

Crítico: El nivel de probabilidad de ocurrencia es crítico y se hace obligatorio implementar salvaguardas adicionales que minimicen el impacto de la materialización de los riesgos.[22]

A continuación se presenta la forma de evaluar los riesgos:

Figura 2. Cálculo del nivel de riesgo

[22] El análisis de riesgos, base de la Gestión Empresarial. http://www.criptored.upm.es/intypedia/video.php?id=introduccion-gestion-riesgos&lang=es

PROBABILIDAD DE OCURRENCIA	
Bajo	1
Medio	2
Alto	3

IMPORTANCIA DEL RIESGO	
Bajo	1
Normal	2
Alto	3
Crítico	4

NIVEL DE RIESGO	
Bajo	1
Bajo	2
Bajo	3
Medio	4
Medio	5
Medio	6
Alto	7
Alto	8
Alto	9
Critico	10
Critico	11
Critico	12

Fuente: el autor

4.4 MARCO CONCEPTUAL

SEGURIDAD INFORMÁTICA

En la actualidad el mundo está atravesando un auge en tecnología, en donde se hace fundamental la aplicación de buenas prácticas dentro de las organizaciones para el manejo de la seguridad informática, debido a que si no se manejan de forma adecuada resultan generando un impacto negativo para la compañía, afectando su imagen, sus finanzas, relaciones con los clientes, entre otros.

La seguridad informática es el conjunto de normas, procedimientos, políticas implementados para proteger un sistema de información de los riesgos a los que se encuentran expuestas las organizaciones en la actualidad, permitiendo adoptar una cultura se seguridad informática, orientada a proteger los activos informáticos y estratégicos que a su vez estarán alineados con los objetivos y estándares establecidos en cada compañía[23]

La seguridad informática se divide en dos disciplinas de acuerdo con el nivel de riesgo al que se encuentren expuestos: Seguridad Lógica; Es la implementación de procedimientos que aseguren que únicamente podrán tener acceso a los datos

[23] Guía de estudios ETS seguridad informática, http://www.buenastareas.com/ensayos/Horario-Voca-8-Segundo-Semestre/1513007.html

y la información las personas autorizadas. Seguridad Física: Es la implementación de controles y barreras físicas como medidas de prevención ante posibles amenazas que pueda sufrir una compañía a nivel de instalaciones o físico.

Las principales amenazas que se trata de evitar a nivel de seguridad física son:

Los desastres naturales: como terremotos, inundaciones, entre otros.

Amenazas ocasionadas por las personas: incendios, pérdidas de información por funcionarios o clientes externos.[24]

Para tener un mejor nivel de seguridad física, es necesario tener claridad sobre los siguientes conceptos:

Actores de seguridad: Son todas las personas que están involucradas en el proceso de manejo de información bien sea de forma física o electrónica en una compañía

Vulnerabilidades: Hace referencia a una debilidad presentada en un sistema informático perimiendo a un delincuente informático acceder a la información, a las aplicaciones y al sistema de la compañía.

Amenazas: Toda acción que o actividad que atente contra la seguridad de la información. Las empresas y las personas están expuestas a amenazas que al materializarse pueden provocar daños que resulten en pérdidas significativas para la organización.

Riesgos: Es la probabilidad de ocurrencia de un evento o amenaza dentro de la organización, generando pérdidas o daños significativos. El riesgo involucra: Incertidumbre y pérdida potencial.

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Es un proceso continuo que busca identificar los riesgos a nivel de seguridad de la información, mediante la valoración, gestión y documentación de los mismos apoyados en la participación de todos los funcionarios de la organización. Entendiéndose como información a todos los datos estructurados que tiene una

[24] Conceptos de seguridad informática, http://www.fcca.umich.mx/descargas/apuntes/Academia%20de%20Informatica/Adm%C3%B3n%20de%20Centros%20de%20Computo%20%20%20R.C.M/UNIDAD%20IV.pdf

compañía y que genera valor para la misma, independientemente del modo en el que se guarde o transmita.[25]

De acuerdo con lo establecido por la ISO 27001 la seguridad de la información consiste en preservar su confidencialidad, integridad y disponibilidad, así como los sistemas en los que se trata y almacena dentro de la compañía. La base sobre la cual se establece la seguridad de la información está compuesta por:[26]

Confidencialidad.

Es todo lo relacionado con los accesos a la información y a los sistemas de información de las organizaciones sin autorización. Esto quiere decir, que la información solo pueda ser accedida por el personal autorizado, es por esto que las empresas deben velar por mantener actualizados los perfiles de acceso de acuerdo con la función desempeñada cada funcionario, establecer acuerdos de confidencialidad entre los empleados y la compañía para el manejo de la información.

Integridad.

En este aspecto se habla fundamentalmente de confiabilidad y autenticidad de la información, esta es la base para la toma de decisiones en las organizaciones. Lo que quiere decir, es que la información no haya sido modificada, copiada, alterada desde su origen hasta la salida. La integridad de la información permitirá entregar confiadamente la información, asegurando que no ha tenido modificaciones durante su trayecto.[27]

Disponibilidad.

En este caso, permite a las organizaciones tomar decisiones y acciones ante posibles eventualidades o ataques en sus Sistemas de Información. Las organizaciones junto con sus sistemas de información están expuestas a amenazas cada vez mayores, aprovechando las vulnerabilidades existentes, abusando de los directivos o dueños de la compañía, sometiéndolos a fraude,

[25] Ernst &Young Calidad en todo lo que hacemos, http://www.ey.com/mx
[26] Análisis y gestión del riesgos Tecnológicos http://www.mnet.com.mx/analisis.html

[27] NARANJO Bertha, Diseño de un plan estratégico de seguridad de información en una empresa del sector comercial, Universidad Superior Politécnica de Litoral, Guayaquil.

espionaje, sabotaje, extorsión, entre otros. Los ataques realizados por Hackers mediante virus informáticos o denegando el servicio al sistema, robo de contraseñas son entre otros, riesgos a considerar por las compañías hoy en día.

Autenticación.

Los mecanismos de seguridad que tienen los equipos que se utilizan para la comunicación, con el fin de validar que el origen de los datos es el correcto, quien los envió, cuando fueron enviados y recibidos. Una de las herramientas utilizadas para garantizar la autenticación es la criptografía, la cual se encarga de brindar legitimidad de los mensajes y la exactitud de los datos.

El sistema de Gestión de la Seguridad de la información (SGSI) permite establecer políticas y procedimientos en relación a los objetivos de cada negocio, con el objeto de mantener un mínimo nivel de exposición del riesgo que la misma compañía ha decido asumir.[28] A continuación se presenta de forma gráfica un SGSI.

Figura 3. SGSI

Fuente http://www.iso27000.es/download/doc_sgsi_all.pdf

Un sistema de información realiza cuatro actividades básicas:

[28]Sistema de gestión de la Seguridad de la Información (SGSI) http://www.iso27000.es/download/doc_sgsi_all.pdf

Entrada de información (INPUT): Es la técnica mediante la cual el sistema obtiene los datos que necesita para procesar la información, mediante de teclados, códigos de barras, medios magnéticos, entre otros.

Almacenamiento de la información: Es la tarea más importante, a través de ella el sistema puede recolectar la información tomada en procesos anteriores para modificarla, almacenarla, agregarla, eliminarla.

Salida de información (OUTPUT): Mecanismo mediante el cual se saca la información procesada, a través de impresiones, USB, discos duros, videos, medios magnéticos, entre otros.

POLITICA DE SEGURIDAD

Se puede decir que es el conjunto adecuado de controles que abarcan prácticas, procedimientos, estructuras organizacionales, funciones de software plasmado en un documento que apoyado en la alta Gerencia demuestra el compromiso de la organización con la seguridad de la información. De forma general a continuación se presentan los pasos para la elaboración de la política general de Seguridad de la información, teniendo en cuenta los principios básicos[29]:

Fase de desarrollo

Es la planificación, investigación y redacción de la política o la creación de la misma. Esto implica identificar que se necesita la política, por ejemplo los requerimientos legales, regulaciones técnicas, contractuales u operacionales. Determinar el alcance y la aplicabilidad de la política, los roles y las responsabilidades inherentes a la política y garantizar la factibilidad de la aplicación dentro de la organización.

Revisión de la política

Una vez ha sido creada la política, esta debe ser remitida a un grupo o individuo independiente para su evaluación antes de la aprobación final. Si la política es revisada por miembros independientes permite obtener una opinión más certera

[29] Elaboración de la política general de seguridad y privacidad de la información, https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

frente a las personas que la crearon, dando mayor credibilidad a la misma ya que se recibe retroalimentación de especialistas para la creación de la política. La exposición de la política a los revisores es de vital importancia en este punto ya que se explicara el objetivo, e contexto y la justificación de la misma lo que llevara a que sea necesaria para la organización.

Aprobación de la política.

El objetivo principal de esta etapa es tener el apoyo de la Administración y alta Gerencia de la organización, mediante la firma del representante legal de la compañía. Una vez aprobada se inicia con la implementación de la política, es de vital importancia que la Administración reconozca y nombre a un funcionario quien presentará las recomendaciones emitidas durante la etapa de revisión e implementación.

Importancia de las Políticas de Seguridad de la información

Para las compañías es muy importante contar con políticas de seguridad, debido a que a través de estas se establecerá la guía de comportamiento personal y profesional de los empleados, contratistas, proveedores, clientes sobre el manejo de la información obtenida, generada, entregada por la compañía, a su vez le darán a la organización los lineamientos para trabajar bajo mejores prácticas de seguridad y cumplir con los requisitos legales.

Fases de implementación de las Políticas de Seguridad de la Información

Desarrollo de las políticas: En esta fase la compañía debe identificar a todas las áreas con el fin de involucrar a todos los funcionarios de la organización, estableciendo responsabilidades para la creación, estructuración, redacción, revisión y aprobación de las políticas, en esta fase es necesario realizar actividades de verificación e investigación.[30]

Cumplimiento: En esta fase se implementan los controles de seguridad de la información atendiendo a las políticas diseñadas, a fin de tener coherencia y consistencia entre el diseño de las políticas versus la implementación de controles de Seguridad de información establecidos y aprobados en la organización.

Comunicación: Corresponde a la divulgación que se haga al interior de la organización de las políticas establecidas, estas deben ser conocidas por los contratistas, proveedores, funcionarios, clientes y todas las personas que hacen parte indirecta o directamente en la compañía, el cumplimiento de las políticas dependerá en gran medida del conocimiento que se tenga sobre las mismas, esto debe ser de carácter obligatorio y de cumplimiento.

[30] Implementación de políticas de Seguridad de la Información, https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

Monitoreo: Esta fase es muy importante debido a que las políticas deben ser evaluadas periódicamente con el fin de identificar el cumplimiento y efectividad, es necesario que las empresas establezcan mecanismos de medición como indicadores que le permitan mantener un dato real del funcionamiento, aplicabilidad y cumplimiento de las políticas.

Mantenimiento: Es necesario que se mantenga actualizada la política de acuerdo con la realidad de cada negocio y las actualizaciones que se realicen de los procesos, teniendo políticas actualizadas que se ajusten a las modificaciones que se requieran de acuerdo con el permanente monitoreo de las mismas.

A fin de dar un mayor concepto de la seguridad de la información, a continuación se presentan algunos términos relevantes dentro de esta materia:

Criptografía: Es un tipo de escritura oculta, que permite enviar documentos o datos a través de redes locales o Internet de forma secreta a través de códigos de cifrado. A través del área de informática se estudian los métodos, procesos y técnicas que se utilizan con el fin de transmitir información en formato digital. La Criptografía busca proteger los datos y la información contra el acceso no autorizado, su alteración, robo o pérdida de la misma, conservando la integridad, confidencialidad y autenticidad de la misma.[31]

Función Hash: Permite transformar cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independiente de la longitud de los datos de entrada, el valor hash de salida siempre tendrá la misma longitud.

Cryptosec RKL: Este dispositivo permite realizar la actualización de sistemas ATMs y Pin Pads de una manera automatizada, desasistida, eliminando los procesos manuales, siendo además cómplice con las normas definidas por VISA-PCI.

H3P: Aprueba personalizar la información que queremos introducir en una tarjeta segura, independientemente del sistema que utilice de lectura como cotactless, EMV. Permite desde introducir certificados electrónicos y claves, hasta introducir fotos, datos clínicos de pacientes de riesgo, entre otros datos confidenciales, ofreciendo seguridad en los datos.

Ransomware: son programas creados por delincuentes informáticos que ingresan al PC a través de un adjunto en el correo electrónico o un link que lo conecta a

[31] Criptografía https://www.genbetadev.com/seguridad-informatica/tipos-de-criptografia-simetrica-asimetrica-e-hibrida,

una página web infectada con este malware, para secuestrar la información, restringiendo el acceso al sistema y pidiendo rescate para liberar el acceso. Cryptowall, conocido como el mayor ransomware y el más peligroso su ataque más conocido fue a Telefónica en Madrid, España y se aprovecha del desconocimiento de las personas para atacar, secuestrando la información y pidiendo rescate de la misma a través de Bitcoins. [32]

Mediante Herramientas de seguridad se pueden identificar vulnerabilidades en un sistema. Pueden ser una amenaza si un intruso las utiliza en el sistema y detecta fallas en la seguridad de las que el administrador no está enterado. Así como los Firewall: Dispositivo que se coloca entre una red local e Internet y cuyo objetivo es asegurar que todas las comunicaciones entre los usuarios de dicha red o Internet se realicen conforme a las normas de seguridad de la compañía que lo instala.[33]

Backup: Copia de los datos de un archivo automatizado en un soporte que posibilite su recuperación.

Contraseña: Información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.

Por ultimo las compañías deben contemplar un Plan de Continuidad debido a que es una estrategia planificada con una serie de procedimientos que facilitan u orientan a tener una solución alternativa que permita restituir rápidamente los servicios de la organización ante una eventualidad que podría paralizar parcial o totalmente la compañía.

4.5. MARCO LEGAL

En el tema de políticas de seguridad informática, actualmente se cuenta con normas y estándares definidos como lo son la ISO 27000, desde el año 1995 entidades normalizadoras británicas como (British Standards Institution) fueron los pioneros en publicar documentos sobre prácticas en Seguridad para empresas. A partir de esto se dio inicio a la familia 27000 en el año 2000 como un requisito para la implementación de un Sistema de Gestión de la Seguridad de Información (SGSI). Para la realización de este proyecto se tendrán en cuenta los siguientes estándares normativos para la implementación de seguridad informática.[34]

---

[32] Ransomware protéjase, https://www.avast.com/es-es/c-ransomware

[33] Firewalls Work https://computer.howstuffworks.com/firewall.htm

34 Sistema de Gestión de Seguridad de la Información (SGSI) http://repositorio.utp.edu.co/dspace/bitstream/11059/4117/1/0058A284.pdf

Norma ISO27001:2013

Es la norma principal, la cual contiene los requisitos del Sistema de Gestión de Seguridad de la información. Enmarca temas como la mejora continua en la seguridad de la información en las organizaciones y sobre ella se describen temas que permiten hacer un análisis detallado del estado actual de los procesos de la organización. En su anexo A, enumera en forma resumida los objetivos de control y los controles que desarrolla la norma ISO 27002:2005 para que sean tomados por las organizaciones como guía en la implementación del SGSI; aunque no es obligatorio la implementación de todos los controles del anexo A, la empresa deberá sustentar sólidamente la no aplicabilidad de los controles no implementados.

Ley 1273 de 2009

A través del cual se modifica el código penal, el cual indica "la protección de la información y de los datos" y se conserven integralmente los sistemas que utilicen las tecnologías de información y las comunicaciones, entre otras disposiciones. Es de vital importancia esta ley, ya que castiga los atentados contra la confidencialidad, la integridad y la confidencialidad de los datos y de los sistemas de información.[35]

Ley 1341 de 2009

Determina el marco general para la implementación de políticas públicas que rigen el sector de las Tecnologías de la Información y las Comunicaciones, a su vez indica las potestades del Estado con relación a la Planeación, gestión y la administración eficiente de los recursos, la regulación y vigilancia del mismo, facilitando el acceso libre y sin discriminación alguna para el acceso de la información desde cualquier punto del país.[36]

Circular 052 de 2012

A través del cual el Gobierno Nacional expidió la ley Estatutaria 1581 de 2012, esta dicta disposiciones generales para la protección de datos personales, regula el derecho fundamental del habeas data.[37] Establece los requisitos mínimos de seguridad informática en cuanto al manejo de información, bajo los siguientes criterios de información: confidencialidad, integridad y disponibilidad.

[35] CIRCULAR EXTERNA 052 DE 2012 La Súper Intendencia Financiera de Colombia. Capitulo Décimo Segundo: Requerimientos Mínimos De Seguridad y Calidad en el Manejo de Información a Través de Medios y Canales de Distribución de Productos y Servicios.

[36] Ley 1341 de 2009 https://www.enticconfio.gov.co/ley-1341-de-2009

[37]: CERTICAMARA. ABC para proteger los datos personales Ley 1273 de 2009 https://www.certicamara.com

En el año 2012 la Superfinanciera de Colombia publica el proyecto el cual presenta modificaciones en las definiciones y criterios de seguridad y calidad de la información, como el tema de la autenticación, mecanismos fuertes de autenticación, banca móvil, proveedor de telecomunicaciones, obligaciones adicionales por tipo de canal, cajeros automáticos, sistemas de audio respuesta, centro de atención telefónica, internet. Es deber de las organizaciones conocer y aplicar la ley establecida.

5. METODOLOGÍA

Para la elaboración de este trabajo se tomará como referencia la norma ISO/IEC 27001:2013, la cual hace énfasis en las actividades y requisitos que se deben tener en cuenta para el desarrollo de un diseño de políticas de seguridad informática; el enfoque de la metodología empleada es Cualitativo.

5.1. TIPO DE INVESTIGACIÓN

La presente investigación es de carácter descriptivo debido que aborda la seguridad informática y los principales riesgos de seguridad informática que tiene el área de afiliaciones de COOPSEGUROS; Así mismo es una investigación orientada a la gestión de los sistemas en busca de generación de soluciones a los problemas que se identifican en esta área de la compañía y también se puede considerar como propositiva toda vez que se genera como producto el diseño de políticas de seguridad informática.

5.2. DISEÑO DE INVESTIGACIÓN

La metodología empleada en el desarrollo de este proyecto se basó en la observación y análisis descriptivo de los hallazgos encontrados. No se empleó una metodología de tipo transaccional o transversal, los resultados presentados no incluyen el seguimiento a la aplicación de las políticas de seguridad informática propuestas para el área de afiliaciones de COOPSEGUROS.

5.3. POBLACIÓN Y MUESTRA

Población: Se determina con el personal de COOPSEGUROS involucrados en el proceso de afiliaciones de la compañía. Muestra: Dado que en el proceso de afiliaciones intervienen funcionarios, la recolección de la información se hizo sobre el 100% de la población. Esta información se consideró suficiente y se continuó a las siguientes fases.

5.4. FUENTES DE INFORMACIÓN

Las fuentes de información tomadas para la realización de este proyecto se describen así:

Fuentes de información primaria

Las fuentes primarias se encuentran constituidas por la información original suministrada por el personal de COOPSEGUROS, empleados que hacen parte integral de proceso de afiliaciones y quienes cuentan con la experiencia y conocimiento de sus funciones.

Fuentes de información secundaria

Hace referencia a toda la información documental orientada al análisis y evaluación de la seguridad informática y que se encuentra disponible en documentos como: normas ISO NTC –IEC -27001, ISO NTC –IEC -27002 y metodología MAGERIT, modelos de seguridad informática y otros documentos de la compañía.[38]

[38] Guía fuentes de información http://evirtual.lasalle.edu.co/info_basica/nuevos/guia/fuentesDeInformacion.pdf

5.5. TECNICAS E INSTRUMENTACIÓN DE RECOLECCIÓN DE DATOS

Entrevistas: Utilizadas para obtener información relevante para el desarrollo del proyecto, en este caso se utilizó el modelo de entrevista conversacional, debido a que es un técnica eficaz para obtener datos relevantes y significativos, utilizando una entrevista no estructurada que permitirá tener una opinión personalizadas de los funcionarios que hacen parte del proceso de afiliaciones de COOPSEGUROS.[39]

Observación: La observación es un elemento fundamental dentro de cualquier proceso investigativo, debido a que permite tomar información de primera mano y sobre esta realizar el respectivo análisis. Se realizó la técnica de observación con el fin de registrar patrones de conducta de los usuarios y funcionarios que hacen parte del proceso y sistema informático del área de afiliaciones de COOPSEGUROS.

Revisión documental: De acuerdo con los documentos establecidos en estudios de tipo científico, o normativos y con el fin de realizar este proyecto aplicado, el desarrollo se basó en la documentación disponible como: normas ISO NTC –IEC -27001, ISO NTC –IEC -27002 y metodología MAGERIT, modelos de seguridad informática y otros documentos de la compañía.[40]

A continuación se presentan cada uno de los métodos que serán utilizados para el desarrollo de este proyecto buscando dar cumplimiento al objetivo general del mismo.

Figura 4. Fases metodológicas para el diseño de las PSI

Fuente: el autor

[39] Técnicas e instrumentación de recolección de datos https://es.slideshare.net/nelsycarrillo/tcnica-de-observacin

[40] Revisión documental https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Con el fin de llevar a cabo las fases antes mencionadas para el diseño de políticas de seguridad informática, a continuación se muestran las actividades a realizar:

5.6. DESCRIPCIÓN DEL ESTADO ACTUAL

Esta fase nos permite realizar un esquema y análisis de la situación actual que se está presentado en el área de afiliaciones de COOPSEGUROS, toda vez que se recopila la información, de fuentes de origen primario y/o secundario.

5.7. ANÁLISIS DE INFORMACIÓN E IDENTIFICACIÓN DE RIESGOS

Este proceso consiste en analizar la información recopilada con el fin de identificar los riesgos y vulnerabilidades a los que está expuesta la compañía a nivel de seguridad de la información en el área de afiliaciones, algunos factores a validar:

- Identificar los activos de información del proceso de gestión de tecnología y clasificarlas de acuerdo con su criticidad y nivel de protección
- Valorizar los riesgos identificados de seguridad de la información, de acuerdo con el alcance definido para el diseño de las Políticas en seguridad de la información.
- Establecer controles o acciones que permitan mitigar los riesgos identificados durante el proceso de valorización.

5.8. EL DISEÑO DE POLÍTICAS EN EL ÁREA DE AFILLIACIONES DE COOPSEGUROS

Esta fase será el resultado de los procesos realizados anteriormente, con el fin de diseñar las políticas de seguridad informática en el área de afiliaciones de COOPSEGUROS, para lo cual se establecen los siguientes pasos:

Establecer el alcance de la política de seguridad informática, la aplicabilidad, los responsables y demás factores que intervienen en el proceso.

Definir la aplicabilidad de las políticas de seguridad informática dentro del proceso, teniendo en cuenta que puede llegar a ser extensiva a las demás áreas de la organización.

De acuerdo con la estructura organizacional del proceso, determinar los roles y responsabilidades para proteger los activos de información de la compañía.

Producto del resultado de la evaluación de riesgos y las amenazas identificadas en el área de afiliaciones definir la política de seguridad informática.

A continuación se mencionan algunos de los elementos que deben ser tenidos en cuenta durante el desarrollo del proyecto para realizar el diseño de las políticas de seguridad informática del área de afiliaciones de COOPSEGUROS:

- La recolección de información obtenida mediante entrevistas con el personal que hace parte del proceso de afiliaciones, sobre esta información se podrá hacer un diagnóstico de la situación actual de la compañía a nivel de seguridad informática.

- Identificar y realizar un análisis de los activos de información del proceso de afiliaciones.

- Realizar el análisis de riesgos con su respectiva valoración logrando identificar en dónde se presenta el mayor número de vulnerabilidades que podrían impactar en un nivel alto a la compañía.

- Establecer parámetros que le ayuden a COOPSEGUROS a mejorar la seguridad en los activos del proceso de afiliaciones, basados en la norma ISO/IEC 27001:2013.

6. RESULTADOS

6.1 ESTADO ACTUAL DE LA COMPAÑÍA

COOPSEGUROS cuenta actualmente con 7 empleados los cuales son los encargados de manejar las diferentes líneas de servicio, así mismo se cuenta con una base de datos de más de 500 clientes afiliados a sus diferentes aliados, como son (EPS SURA, NUEVA EPS, SALUD TOTAL, COOMEVA, entre otros). [41]

La compañía actualmente conserva sus bases de datos en hojas de cálculo de Excel, sin protección alguna, estos datos son manipulados por diferentes empleados, no toda la información se encuentra digitalizada y no se cuenta con una base de datos unificada de clientes, asesores, y afiliados.

Los formularios y documentos personales, como cédulas, registros civiles, entre otros, son intercambiados mediante correo electrónico, no se identificó un sistema de protección para la Red interna de compañía, no hay restricciones a página web e internet para los empleados, no hay ningún proceso establecido para el manejo de información y el cuidado que se debe tener con la misma.

Aunque cuentan con un Ingeniero de Sistemas que presta sus servicios esporádicamente, este les presta el servicio de actualización de antivirus y les configura la Red interna para compartir archivos, no se evidencia seguridad en los equipos ni en la Red, hay un equipo de Backup pero no se logró identificar cómo se realiza este proceso. El Gerente no ha dimensionado los riegos a los que se enfrenta la compañía actualmente y los beneficios que tiene el asegurar y proteger

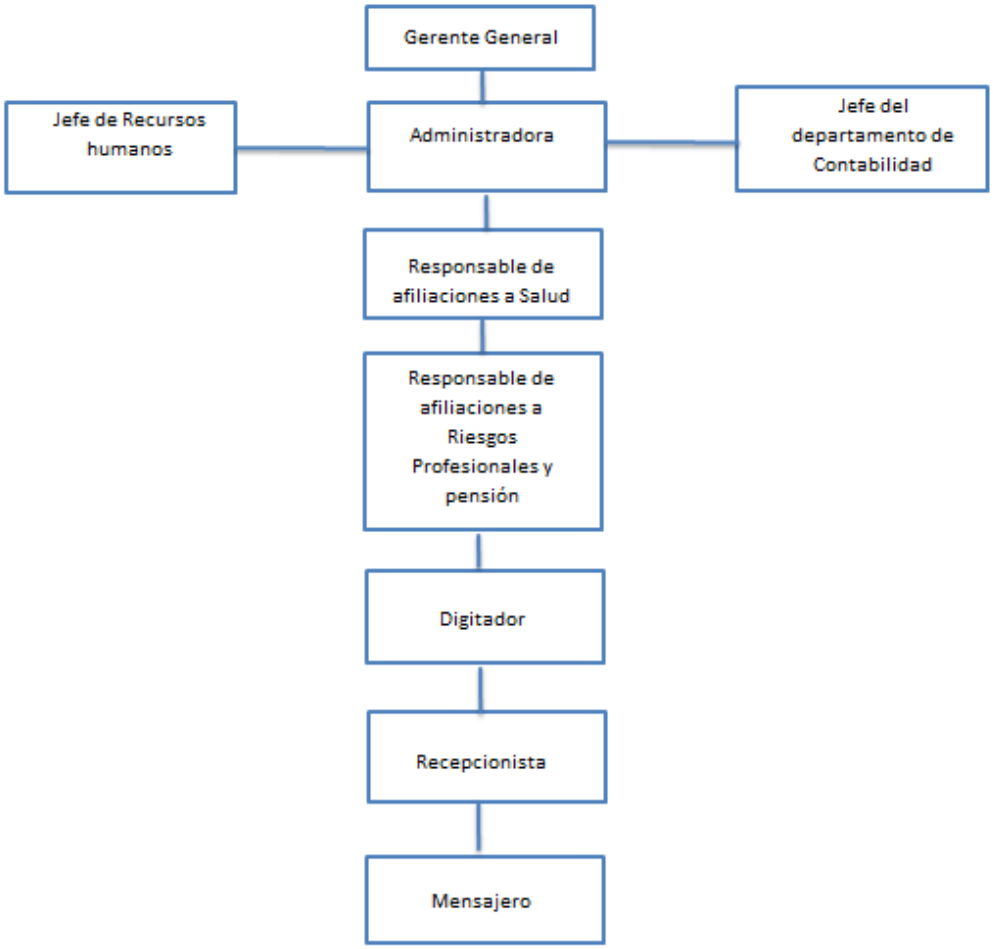
El Gerente de la compañía está interesado en comparar un programa que le permita integrar la información y los servicios que presta, pero para esto, debe identificar actualmente qué tiene y cómo lo están trabajando actualmente. A su vez se muestra comprometido para permitir revisar internamente los procesos que se llevan a cabo en el área de afiliaciones y espera recibir retroalimentación del informe producto de la investigación realizada en su empresa, con el fin de tomar las acciones respectivas que le permitan mejorar el área de afiliaciones.

[41] COOPSEGUROS, [en línea] [citado el 11 de noviembre de 2017] disponible en internet: https://www.coopseguros.com.co/

A continuación se relaciona el resultado de las entrevistas realizadas al personal que interviene en el proceso de afiliaciones de COOPSEGUROS, no se describe toda la información debido a que puede ser sensible y afectar la seguridad de la compañía.

6.2 DIAGRAMA ORGANIZACIONAL

Figura 5. Diagrama Organizacional



Fuente: COOPSEGUROS

6.3 RECOPILACION DE INFORMACIÓN

La compañía COOPSEGUROS cuenta con el área de afiliaciones en donde se efectúa el Core de negocio, el proceso es realizado por 7 funcionarios quienes son los encargados de cumplir con las necesidades de los clientes, de acuerdo con el servicio ofrecido, afiliación de independientes y empresas a salud, pensión y riesgos profesionales en la entidad que el cliente solicite.

Para realizar una evaluación de riesgos en el área de afiliaciones de COOPSEGUROS es necesario que los funcionarios involucrados en este proceso proporcionen información que ayude a identificar las vulnerabilidades a las que se encuentra expuesta la organización, por lo anterior se realizó una entrevista con cada uno de los empleados de esta área.

FORMATO DE ENTREVISTA

Para las entrevistas realizadas a los funcionarios que intervienen en el proceso de afiliaciones de COOPSEGUROS, se realizó el siguiente modelo, en el cual se preguntaron temas asociados a su rol dentro del proceso, las actividades realizadas, los sistemas de información y comunicación que utilizan, entre otras, que como funcionarios del proceso de afiliaciones utilizan: (Ver anexo 1 entrevistas)

A continuación se presenta el resultado consolidado de las respuestas a las entrevistas realizadas:

No.	Situación actual
1	Los procesos de la compañía son manuales
2	La información de los clientes, empleados, proveedores es contenida en bases de datos de Excel
3	No se tienen creadas contraseñas para proteger los archivos de Excel
4	No se realiza Backup de la información
5	No hay un base de datos que contenga los datos históricos de los clientes
6	El volumen de información confidencial que se maneja físicamente es muy alto
7	Las planillas de Excel para hacer el proceso de afiliaciones no contienen soportes

Consolidado de las entrevistas realizadas a los funcionarios (Continuación)

8	Los documentos que soportan la afiliación no siempre se escanean
9	Los computadores no tienen contraseñas por cada uno se comparte la contraseña
10	No siempre se cierra sesión aun cuando se está atendiendo otro asunto
11	No hay permisos o restricciones para recibir correos electrónicos
12	No hay restricciones para acceder a diferentes páginas web
13	La información de los clientes se comparte por la Red interna
14	La clave de internet la comparten con cualquier proveedor o usuario que llegue a la oficina
15	La información que se recibe de los clientes no se custodia de manera adecuada
16	La información personal de los clientes en manipulada por varios funcionarios sin ningún control
17	El personal puede sacar información sensible de la compañía sin problema

Tabla 2 consolidado de las entrevistas realizadas a los funcionarios

Producto del resultado de las entrevistas realizadas al personal que intervienen el proceso de afiliaciones de COOPSEGUROS, se identificó que la organización se encuentra expuesta a diferentes amenazas asociadas a cada activo de la compañía, de acuerdo con el análisis de riesgos realizado a continuación se logrará identificar el nivel de riesgo y la probabilidad de ocurrencia de que estos se materialicen, trayendo implicaciones negativas para la continuidad del negocio.

6.4 IDENTIFICACIÓN DE ACTIVOS

La empresa actualmente cuenta con una infraestructura reducida ya que es una empresa pequeña con no más de 100 empleados. Entre sus activos principales relacionados con los Sistemas de Información se pueden encontrar los enumerados en la Tabla 1.

La identificación de activos es una actividad crítica dentro del proceso, debido a que permitirá; establecer las dependencias que tienen los activos uno del otro, valorar los activos con precisión, identificar y valorar el impacto de las amenazas identificadas y establecer salvaguardas que ayuden a proteger los sistemas de información o a reducir el impacto que podría tener la materialidad de un riesgo.

Tipo de activo	Activo
Software	Suite ofimática Microsoft Office 2013
	Antivirus MacAfee gratuito
	Sistema Operativo Windows 7
Hardware	Medios de impresión. Impresoras HP
	Computadores de escritorio Lenovo
Hardware	Router
	Cableado Categoría 5
Comunicaciones	Telefonía ETB
	Red LAN
	Internet ETB
Sistemas de vigilancia	Sistema de vigilancia circuito cerrado
Medios Externos	Memorias USB, CD/DVD, Discos duros Externos Toshiba
Personal	Administradora
	Jefe del departamento de contabilidad
	Responsable de afiliaciones a salud
	Responsable de afiliaciones a riesgos y ARP
	Responsable de seguros
	Recepcionista y digitadora
	Mensajero

Tabla 3. Activos principales para COOPSEGUROS relacionados a los Sistemas de información

De acuerdo con el análisis realizado en el proceso de afiliaciones de COOPSEGUROS y teniendo en cuenta la entrevistas realizadas a los diferentes funcionarios involucrado en el proceso a continuación se describe la utilización actual que tienen los activos de información identificados.

La Tabla 4 describe cuál es el uso de cada uno de estos activos dentro de la organización, exponiendo cómo estos ayudan a los procesos de negocio.

Tipo de activo	Activo
Suite Ofimática Office 2013	Manejo de documentos de soporte en general para la organización, uso de Word 2013
	Uso de correos con clientes -Outlook 2013
	Formularios para la administración de información de los clientes en formatos de Excel 2013
	Operaciones de contabilidad con la disposición de Excel 2013

Activos y sus funciones en la compañía COOPSEGUROS (Continuación)

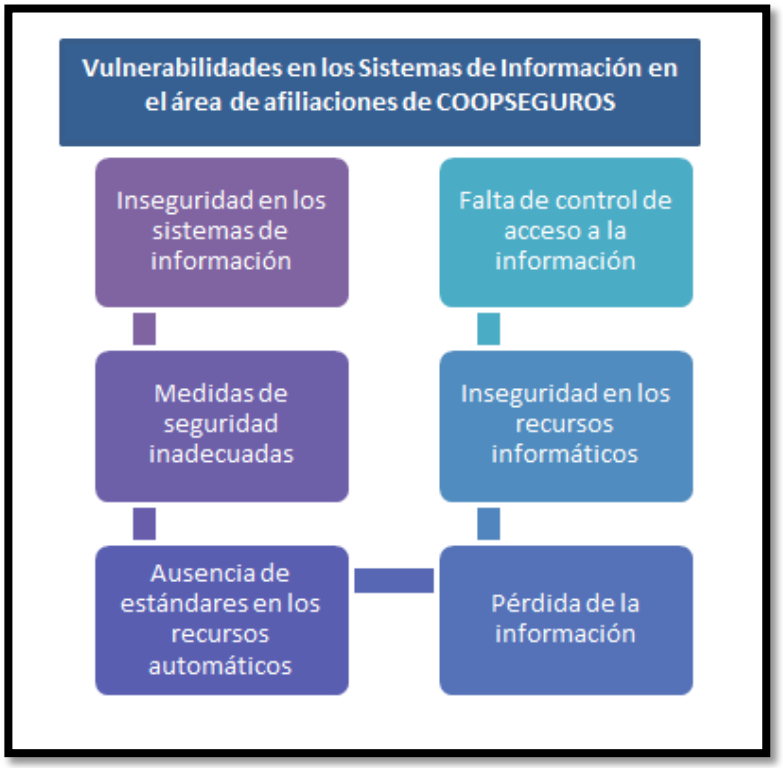
Antivirus MacAfee Gratuito	Protección en tiempo real contra malware de los computadores de los empleados
	Detección de malware en los computadores de los empleados
Sistema Operativo Windows 7	Administración y funcionamiento del hardware para los computadores Lenovo, dispuestos a todos los empleados de la compañía.
Medios de Impresión Impresoras HP	Disposición física de los documentos virtuales
Computadores de escritorio Lenovo	Dispositivos encargados del procesamiento, apoyo y gestión de tareas para los procesos de negocio.
Router	Enrutamiento de tráfico de red entre los segmentos y medios con los que cuenta la compañía.
Cableado categoría 5	Transmisión de datos para la Red Local de la compañía
Telefonía ETB	Comunicación mediante vías telefónicas
	Comunicación interna entre los distintos dispositivos de red
Internet ETB	Acceso y comunicación mediante Internet
Sistemas de vigilancia	Vigilancia de las instalaciones físicas de la compañía
Memorias USB, CD/DVD, Discos duros Externos Toshiba	Almacenamiento de copias de seguridad y software utilizado en la compañía
Administradora	Encargada de la toma de decisiones de la compañía
Jefe del departamento de Contabilidad	Encargada de la supervisión de las tareas de cálculo de ingresos y egresos de la compañía en general
Responsable de las afiliaciones de salud	Personas encargadas del contacto con las entidades prestadoras del servicio de salud al cual se afilian los clientes
Responsable de las afiliaciones de pensión	
Recepcionista	Encargadas del recibir la información de los clientes y grabar la información en Excel, diligencia formularios de afiliación
Digitadora	
Mensajero	Radica la información de los clientes, formularios y soportes en las entidades de saludo, pensión y ARP

Tabla 4 Activos y sus funciones en la compañía COOPSEGUROS

6.5 ANÁLISIS DE LA SITUACIÓN ACTUAL

De acuerdo con la información recopilada mediante entrevistas realizadas al personal de COOPSEGUROS, se evidencia que la situación actual de la empresa es alarmante, debido a que no se identifican la implementación de medidas de seguridad, lo que hace que se presente un alto grado de materialización de las amenazas que pueden traer implicaciones negativas a la compañía.

Figura 6. Análisis critico



Fuente el autor

6.6 ANÁLISIS DE LOS RIESGOS

Es necesario que para cada uno de estos activos se tengan en cuenta las dimensiones enmarcadas en la Tabla 5. Para cada una de estas dimensiones se realiza una valorización, teniendo en cuenta qué tanta afectación puede existir su

un activo presenta problemas en la dimensión evaluada. La Tabla 6 determina los niveles de valorización.

Dimensiones	
[D]	**Disponibilidad.** Los prejuicios que causaría a la compañía el no poder usarlo
[I]	**Integridad**. Los prejuicios causados si el activo se encuentra corrupto
[C]	**Confidencialidad.** Afectación a la compañía si alguien no autorizado conoce o tiene acceso al activo
[A]	**Autenticidad.** Afectación si se desconoce los sujetos que realizan las acciones desarrolladas sobre el activo
[TS]	**Trazabilidad del servicio.** Los prejuicios causados si se desconoce las acciones llevadas a cabo sobre un activo
[TA]	**Trazabilidad de acceso a los Datos.** Los prejuicios provocados a la compañía si se desconoce el acceso que se ha tenido a información importante

Tabla 5 Dimensiones seleccionadas para la priorización de Activos de COOPSEGUROS

Criterios de Valoración de Activos	
10	Daño extremadamente grave
9	Daño muy grave
6-8	Daño grave
3-5	Daño importante
1-2	Daño menor
0	Irrelevante a efectos práctico

Tabla 6 Criterios de valoración para los activos. Fuente MAGERIT v3 Catálogo de los elementos

Una vez definidas las dimensiones y los diferentes grados de valorización se proceden a relacionarlos, para esto se muestra en la Tabla 7 cuál es el valor

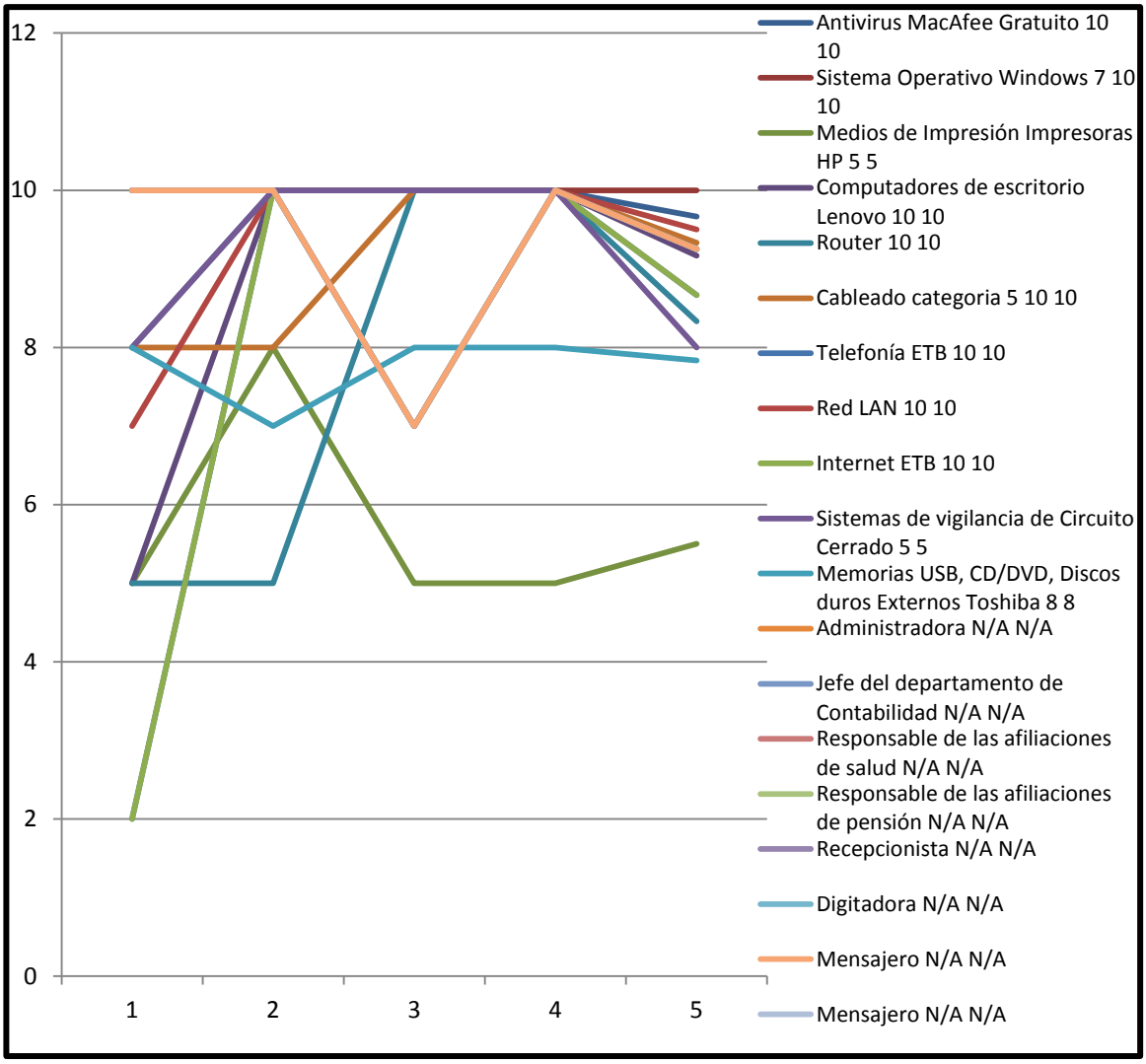
numérico otorgado para cada uno de los activos. La valorización cuantitativa otorga la ventaja de la precisión numérica y además proporciona la posibilidad de trabajar sobre estadísticas de las mismas.

Tipo de activo	Valoración por dimensión						Promedio Valoración
	[I]	[D]	[C]	[A]	[TS]	[TA]	
Suite Ofimática Office 2013	10	10	5	8	8	8	8
Antivirus McAfee Gratuito	10	10	8	10	10	10	10
Sistema Operativo Windows 7	10	10	10	10	10	10	10
Medios de Impresión Impresoras HP	5	5	5	8	5	5	6
Computadores de escritorio Lenovo	10	10	5	10	10	10	9
Router	10	10	5	5	10	10	8
Cableado categoría 5	10	10	8	8	10	10	9
Telefonía ETB	10	10	2	10	10	10	9
Red LAN	10	10	7	10	10	10	10
Internet ETB	10	10	2	10	10	10	9
Sistemas de vigilancia de Circuito Cerrado	5	5	8	10	10	10	8
Memorias USB, CD/DVD, Discos duros Externos Toshiba	8	8	8	7	8	8	8
Administradora	N/A	N/A	10	10	7	10	9
Jefe del departamento de Contabilidad	N/A	N/A	10	10	7	10	9
Responsable de las afiliaciones de salud	N/A	N/A	10	10	7	10	9
Responsable de las afiliaciones de pensión	N/A	N/A	10	10	7	10	9
Recepcionista	N/A	N/A	10	10	7	10	9
Digitadora	N/A	N/A	10	10	7	10	9
Mensajero	N/A	N/A	10	10	7	10	9

Tabla 7 Valoración de los activos de COOPSEGUROS según las dimensiones

Nota: Algunas de las dimensiones no pueden ser aplicadas para los activos humanos; ya que están enfocados a los activos software o hardware.

Figura 7. Valoración de disponibilidad de activos de COOPSEGUROS



Fuente el autor

La Figura 7 muestra el nivel de la dimensión disponibilidad ya que ésta tiende a medirse según el tiempo. Teniendo en cuenta estos valores se puede determinar qué tan valioso es un activo para la organización. Por ejemplo, se puede evidenciar en la Tabla 7 y la Figura 7 que los activos más valiosos para la organización son los Sistemas Operativos Windows 7, los Computadores Lenovo y la Suite Ofimática de Office 2013.

6.7 IDENTIFICACIÓN DE LAS AMENAZAS

Se procede a la identificación de las amenazas que pueden afectar a los activos identificados anteriormente. La Tabla 8 muestra los diferentes tipos de orígenes de amenazas que pueden incurrir.

Orígenes de Amenazas	
[N]	Desastres naturales
[E]	Entorno
[DA]	Defectos de la aplicación
[CA]	Causadas accidentalmente
[CD]	Causadas deliberadamente

Tabla 8 Clasificación de los orígenes de las amenazas

Seguidamente se continúa con la identificación de las posibles amenazas que puedan causar afectaciones a los activos, la Tabla 9 muestra cuáles amenazas pueden incurrir en problemas con los activos.

Tipo de activo	Amenazas
Suite Ofimática Office 2013	[E.1] Incompatibilidad con programas del Sistema Operativo
	[CA.1] Ingreso erróneo de opciones e instalación de software
	[CD.1] Inyección de macros maliciosas para el software
	[DA.1] Actualizaciones defectuosas de la suite
	[DA.2] Vulnerabilidades del software
	[CD.2] Uso de software pirata

Tabla 9 Identificación de las amenazas de los activos de COOPSEGUROS

Identificación de las amenazas de los activos de COOPSEGUROS (Continuación)

Antivirus McAfee Gratuito	[CD.3] Desactivación internacional del Antivirus [E.2] Interrupción del funcionamiento por falta de licenciamiento [DA.3] Vulnerabilidades del software [E.5] Errores de actualización y falta de soporte
Sistema Operativo Windows 7	[E.3] Incompatibilidad con el hardware instalado [E.4] Errores presentados a nivel de hardware [DA.4] Mala configuración por parte de los usuarios finales
	[CD.4] Mala configuración intencional de los usuarios finales [CD.5] Instalación de software malicioso y/o pirata [E.5] Errores de actualización y falta de soporte [DA.6] Configuración por defecto del dispositivo
Medios de Impresión Impresoras HP	[E.6] Falta de recursos necesarios para la impresión [N.1] Corto circuito de la impresora relacionados a picos de energía [N.2] Falla de funcionamiento por vencimiento de ciclo de vida [CD.6] Ataques relacionados a la instalación de malware de impresoras
Computadores de escritorio Lenovo	[N.2] Corto circuito de la impresora relacionados a picos de energía [N.3] Inundación del ambiente físico donde se encuentra el computador [CD.7] Instalación de hardware malicioso o dispositivos destinados a la afectación del funcionamiento normal del computador [DA.5] Desconexión de partes vitales para el funcionamiento del computador
Router	[DA.6] Configuración por defecto del dispositivo [N.4] Corto circuito del dispositivo relacionado a picos de energía [N.5] Inundación del medio físico donde se encuentra el Router [CD.8] Modificación de las tablas de enrutamiento

Identificación de las amenazas de los activos de COOPSEGUROS (Continuación)

Cableado categoría 5	[CD.9] Creación de bucles de red [DA.7] Corte accidental de los cables de comunicación [DA.10] Corte accidental de los cables de comunicación
Telefonía ETB	[N.6] Pérdida de la red telefónica o internet por desastres naturales: inundación, tormentas, terremoto [E.7] Vencimiento de pago para el servicio de telefonía [E.8] Pérdida del servicio por problemas externos a la compañía relacionados a ETB
Red LAN	[CD.11] Uso de técnicas de hacking de alcance para redes locales [CD.12] Distribución local de ataques phising para la estafa de los empleados [CA.7] Mala configuración del acceso a la red local [E.9] Existencia de puntos únicos de fallo [E.10] Existencia de cuellos de botella en el tráfico de la red
Internet ETB	[E.8] Pérdida del servicio por problemas externos a la compañía relacionados a ETB [N.6] Pérdida de la red telefónica o internet por desastres naturales: inundación, tormentas, terremoto
Internet ETB	[DA.8] Acceso a páginas de baja reputación por parte de los empleados de la compañía [CA.9] Ingreso de software malintencionado
Sistema de Vigilancia de Circuito Cerrado	[CD.13] Instalación de dispositivos malintencionados que puedan filtrar los datos de las cámaras [DA.10] Configuración por defecto de las cámaras [CD.14] Instalación intencional de puntos ciegos por parte del proveedor [CD.11] Instalación accidental de puntos ciegos por parte del proveedor
Memorias USB, CD/DVD, Discos	[DA.12] Conexión de medios de almacenamiento de la empresa en computadores de baja reputación [N.7] pérdida de información por cambios en la energía de los medios de almacenamiento [N.8] pérdida de información por degradación de los medios de almacenamiento

Identificación de las amenazas de los activos de COOPSEGUROS (Continuación)

Duros Externos Toshiba	[CD.15] Acceso no autorizado a los medios de almacenamiento
Administradora	[CD.16] Extorsión [CD.17] Ingeniería Social y engaño
Jefe del departamento de Contabilidad	[CD.16] Extorsión [CD.17] Ingeniería Social y engaño
Responsable de las afiliaciones de salud	[CD.16] Extorsión [CD.17] Ingeniería Social y engaño
Responsable de las afiliaciones de pensión	[CD.16] Extorsión [CD.17] Ingeniería Social y engaño
Recepcionista	[CD.16] Extorsión [CD.17] Ingeniería Social y engaño
Digitadora	[CD.16] Extorsión [CD.17] Ingeniería Social y engaño
Mensajero	[CD.16] Extorsión [CD.17] Ingeniería Social y engaño

Tabla 9 Identificación de las amenazas de los activos de COOPSEGUROS

El siguiente paso es valorar cada una de las amenazas teniendo en cuenta la Tabla 6. La Tabla 10 muestra la asignación de la valorización teniendo en cuenta las distintas dimensiones, es decir; qué tanto pueden afectar cada una de las dimensiones, la última columna de la tabla muestra una probabilidad de 1-10 de la materialización de dicha amenaza.

Tipo de activo	**Amenazas**	**Valoración por dimensión**						**P.V**
		I	**D**	**C**	**A**	**TS**	**TA**	
Suite Ofimática	[E.1] Incompatibilidad con programas del Sistema Operativo	2	6	2	5	9	9	4
Office 2013	[CA.1] Ingreso erróneo de opciones de instalación de software	5	6	4	7	9	8	8
	[CD.1] Inyección de macros maliciosas para el software	7	8	8	6	8	7	9

Tabla 10 Valoración de las amenazas identificadas para COOPSEGUROS

Valoración de las amenazas identificadas para COOPSEGUROS (Continuación)

Suite Ofimática Office 2013	[DA.1] Actualizaciones defectuosas de la suite	8	8	9	5	6	5	6
	[DA.2] Vulnerabilidades del software	8	8	9	4	5	4	9
	[CD.2] Uso de software pirata	10	4	9	5	7	7	9
Antivirus MacAfee Gratuito	[CD.3] Desactivación internacional del Antivirus	10	10	10	10	10	10	8
	[E.2] Interrupción del funcionamiento por falta de licenciamiento	10	10	10	10	10	10	9
	[DA.3] Vulnerabilidades del software	9	7	7	7	8	8	9
	[E.5] Errores de actualización y falta de soporte	9	9	9	9	9	9	9
Sistema Operativo Windows 7	[E.3] Incompatibilidad con el hardware instalado	8	9	5	5	6	6	5
	[E.4] Errores presentados a nivel de hardware	8	9	5	5	6	5	5
	[DA.4] Mala configuración por parte de los usuarios finales	8	7	5	5	7	7	8
	[CD.4] Mala configuración intencional de los usuarios finales	8	7	4	4	7	7	9
	[CD.5] Instalación de software malicioso y/o pirata	10	8	9	9	9	9	9
	[E.5] Errores de actualización y falta de soporte	10	10	10	9	9	9	10
	[DA.6] Configuración por defecto del dispositivo	2	5	4	8	8	8	8
Medios de Impresión Impresoras HP	[E.6] Falta de recursos necesarios para la impresión	1	5	5	2	4	4	5
	[N.1] Corto circuito de la impresora relacionados a picos de energía	3	8	5	5	6	6	4

Valoración de las amenazas identificadas para COOPSEGUROS (Continuación)

Medios de Impresión Impresoras HP	[N.2] Falla de funcionamiento por vencimiento de ciclo de vida	3	9	7	7	7	7	6
	[CD.6] Ataques relacionados a la instalación de malware de impresoras	4	7	8	8	8	8	7
Computadores de escritorio Lenovo	[N.2] Corto circuito de la impresora relacionados a picos de energía	9	10	4	6	8	9	4
	[N.3] Inundación del ambiente físico donde se encuentra el computador	9	10	4	6	8	9	5
	[CD.7] Instalación de hardware malicioso o dispositivos destinados a la afectación del funcionamiento normal del computador	9	7	5	6	8	9	7
	[DA.5] Desconexión de partes vitales para el funcionamiento del computador	10	10	7	8	9	9	8
Router	[DA.6] Configuración por defecto del dispositivo	8	6	5	5	7	8	9
	[N.4] Corto circuito del dispositivo relacionado a picos de energía	9	9	4	5	7	8	4
	[N.5] Inundación del medio físico donde se encuentra el Router	9	9	4	5	7	8	5
	[CD.8] Modificación de las tablas de enrutamiento	8	6	5	7	7	8	7
Cableado categoría 5	[CD.9] Creación de bucles de red	5	10	5	6	8	8	4
	[DA.7] Corte accidental de los cables de comunicación	6	10	4	6	8	8	7
	[DA.10] Corte accidental de los cables de comunicación	6	10	4	6	8	8	7
Telefonía ETB	[N.6] Pérdida de la red telefónica o internet por desastres naturales: inundación, tormentas, terremoto	4	9	2	4	6	8	4
	[E.7] Vencimiento de pago para el servicio de telefonía	4	9	2	4	6	8	2
	[E.8] Pérdida del servicio por problemas externos a la compañía relacionados a ETB	3	9	2	4	5	7	4

Valoración de las amenazas identificadas para COOPSEGUROS (Continuación)

Red LAN	[CD.11] Uso de técnicas de hacking de alcance para redes locales	9	7	9	8	8	7	6
	[CD.12] Distribución local de ataques phising para la estafa de los empleados	4	3	9	7	7	7	6
	[CA.7] Mala configuración del acceso a la red local	5	7	2	5	5	6	7
	[E.9] Existencia de puntos únicos de fallo	7	9	2	5	5	6	4
Red LAN	[E.10] Existencia de cuellos de botella en el tráfico de la red	7	9	2	5	5	6	6
Internet ETB	[E.8] Pérdida del servicio por problemas externos a la compañía relacionados a ETB	4	9	2	4	4	5	4
	[N.6] Pérdida de la red telefónica o internet por desastres naturales: inundación, tormentas, terremoto	4	9	2	4	4	5	4
	[DA.8] Acceso a páginas de baja reputación por parte de los empleados de la compañía	7	4	9	4	4	6	8
	[CA.9] Ingreso de software malintencionado	9	7	9	8	8	8	9
Sistema de Vigilancia de Circuito Cerrado	[CD.13] Instalación de dispositivos malintencionados que puedan filtrar los datos de las cámaras	9	7	9	9	9	9	4
	[DA.10] Configuración por defecto de las cámaras	7	4	4	6	7	7	8
	[CD.14] Instalación intencional de puntos ciegos por parte del proveedor	4	4	4	6	8	8	7
	[CD.11] Instalación accidental de puntos ciegos por parte del proveedor	4	4	5	6		9	8
Memorias USB, CD/DVD, Discos Duros Externos Toshiba	[DA.12] Conexión de medios de almacenamiento de la empresa en computadores de baja reputación	5	4	9	5	7	7	9
	[N.7] pérdida de información por cambios en la energía de los medios de almacenamiento	4	4	4	5	7	7	4

Valoración de las amenazas identificadas para COOPSEGUROS (Continuación)

Memorias USB, CD/DVD, Discos Duros Externos Toshiba	[N.8] pérdida de información por degradación de los medios de almacenamiento	5	4	2	4	4	5	9
	[CD.15] Acceso no autorizado a los medios de almacenamiento	7	4	9	8	8	8	8
Administradora	[CD.16] Extorsión	N/A	7	10	10	7	10	7
	[CD.17] Ingeniería Social y engaño	N/A	7	10	10	7	10	8
Jefe del departamento de Contabilidad	[CD.16] Extorsión	N/A	7	10	10	7	10	7
	[CD.17] Ingeniería Social y engaño	N/A	7	10	10	7	10	7
Responsable de las afiliaciones de salud	[CD.16] Extorsión	N/A	7	10	10	7	10	7
	[CD.17] Ingeniería Social y engaño	N/A	7	10	10	7	10	7
Responsable de las afiliaciones de pensión	[CD.16] Extorsión	N/A	7	10	10	7	10	7
	[CD.17] Ingeniería Social y engaño	N/A	7	10	10	7	10	7
Recepcionista	[CD.16] Extorsión	N/A	7	10	10	7	10	7
	[CD.17] Ingeniería Social y engaño	N/A	7	10	10	7	10	7
Digitadora	[CD.16] Extorsión	N/A	7	10	10	7	10	8
	[CD.17] Ingeniería Social y engaño	N/A	7	10	10	7	10	7
Mensajero	[CD.16] Extorsión	N/A	7	10	10	7	10	7
	[CD.17] Ingeniería Social y engaño	N/A	7	10	10	7	10	7

Tabla 10 Valoración de las amenazas identificadas para COOPSEGUROS

6.8. IDENTIFICACIÓN DE LAS VULNERABILIDADES

Es importante identificar cuáles son las falencias de los activos de la organización, las cuales podrían ser aprovechadas por las diferentes amenazas

enmarcadas. La Tabla 11 muestra una lista de vulnerabilidades para cada uno de los activos.

Tipo de activo	Amenazas
Suite Ofimática Office 2013	[VUL.1] Software desactualizado, actualmente se encuentra en la versión 2016 [VUL.2] Inyección de fórmulas de Excel 2013 [VUL.3] Inyección de código malicioso mediante textos enriquecidos [VUL.4] Inyección de código mediante macros [VUL.5] Corrupción de los procesos de la Suite [VUL.6] No existe uso de algoritmos para la firma de documentos ofimáticos
Antivirus MacAfee Gratuito	[VUL.7] Pérdida de información [VUL.8] Software gratuito que no cuenta con un soporte adecuado sobre las firmas de virus [VUL.9] Desactivación del servicio por software malicioso [VUL.10] Falsificación del antivirus, troyano AV.
Sistema Operativo Windows 7	[VUL.11] Falsificación de las firmas de virus [VUL.12] Software ya no cuenta con soporte por parte de Windows. Por lo tanto, no tiene parches de seguridad [VUL.13] Exposición a explotación remota mediante Eternal Blue y algunos virus actuales [VUL.14] Fácilmente explotable de manera local [VUL.15] Blanco de la mayoría de ataques dispuestos en la actualidad para los sistemas Operativos de Windows
Medios de Impresión Impresoras HP	[VUL.16] Poca tolerancia a los fallos de hardware [VUL.17] Drivers de HP son blancos fáciles para el hardware [VUL.18] Blanco actual de botnets [VUL.19] No cuentan con UPS, ni métodos de alimentación interrumpida
Computadores de escritorio Lenovo	[VUL.20] Personal de cualquier tipo tiene acceso a las computadoras

Tabla 11 Identificación de vulnerabilidades de COOPSEGUROS

Identificación de vulnerabilidades de COOPSEGUROS (Continuación)

Router	[VUL.21] Dispositivos físicos carecen de rótulos
	[VUL.22] El router se encuentra configurado por defecto
	[VUL.23] Tablas de enrutamiento dinámicas
Cableado categoría 5	[VUL.24] No cuenta con UPS, ni métodos de alimentación interrumpida
	[VUL.25] El cableado se encuentra visible y no está basado en los estándares internacionales
Telefonía ETB	[VUL.26] Las instalaciones de telefonía son fácilmente accesibles por cualquier tipo de personal
	[VUL.27] Diseño de red cuenta con bajos niveles de segmentación
Red LAN	[VUL.28] Ausencia de swiches, por ende; no existen Vlans.
Internet ETB	[VUL.29] Puntos de acceso se encuentran visibles a todo el mundo
	[VUL.30] Inexistencia de implementaciones DMZ
Sistema de Vigilancia de Circuito Cerrado	[VUL.31] Inexistencia de implementaciones de Firewall
	[VUL.32] Las cámaras se encuentran visibles y sus mecanismos son fácilmente accesibles por cualquier persona
Memorias USB, CD/DVD, Discos Duros Externos Toshiba	[VUL.33] No existen suman de comprobación sobre los dispositivos extraíbles.
	[VUL.34] Dispositivos físicos carecen de rótulos
Administradora	[VUL.35] Se encuentra información disponible y fácilmente en la Red
	[VUL.36] No cuenta con capacitaciones sobre la peligrosidad de la Ingeniería Social
Jefe del departamento de Contabilidad	[VUL.37] Se encuentra información disponible y fácilmente en la Red
	[VUL.38] No cuenta con capacitaciones sobre la peligrosidad de la Ingeniería Social

Identificación de vulnerabilidades de COOPSEGUROS (Continuación)

Responsable de las afiliaciones de salud	[VUL.35] Se encuentra información disponible y fácilmente en la Red [VUL.39] No cuenta con capacitaciones sobre la peligrosidad de la Ingeniería Social
Responsable de las afiliaciones de pensión	[VUL.40 Se encuentra información disponible y fácilmente en la Red [VUL.41] No cuenta con capacitaciones sobre la peligrosidad de la Ingeniería Social
Recepcionista	[VUL.35] Se encuentra información disponible y fácilmente en la Red [VUL.42] No cuenta con capacitaciones sobre la peligrosidad de la Ingeniería Social
Digitadora	[VUL.43] Se encuentra información disponible y fácilmente en la Red [VUL.44] No cuenta con capacitaciones sobre la peligrosidad de la Ingeniería Social
Mensajero	[VUL.45] Se encuentra información disponible y fácilmente en la Red [VUL.46] No cuenta con capacitaciones sobre la peligrosidad de la Ingeniería Social

Tabla 11 Identificación de vulnerabilidades de COOPSEGUROS

6.9 ESTIMACIÓN DE LOS RIESGOS

Según las vulnerabilidades expuestas en la tabla 9 y las amenazas encontradas y valorizadas en la tabla 8 se procede a entregar una estimación del riesgo por cada uno de los activos dentro de las dimensiones establecidas inicialmente. La tabla 10 muestra la estimación cuantitativa de la estimación de riesgos.

Tipo de activo	Valorización Estimación de Riesgos						Promedio Riesgos
	[I]	[D]	[C]	[A]	[TS]	[TA]	
Suite Ofimática Office 2013	9	7	10	7	7	7	8
Antivirus MacAfee Gratuito	9	8	5	7	7	7	7
Sistema Operativo Windows 7	9	10	10	10	10	10	10
Medios de Impresión Impresoras HP	5	5	5	7	7	7	6

Muestra de estimación cuantitativa de la estimación de riesgos de COOPSEGUROS (Continuación)

Computadores de escritorio Lenovo	9	9	5	10	10	10	9
Router	5	5	4	7	8	8	6
Cableado categoría 5	5	5	5	9	9	9	7
Telefonía ETB	5	5	5	4	7	7	6
Red LAN	5	7	7	8	8	8	7
Internet ETB	5	5	5	4	7	7	6
Sistemas de vigilancia de Circuito Cerrado	5	6	8	7	8	8	7
Memorias USB, CD/DVD, Discos duros Externos Toshiba	5	5	9	8	7	7	7
Administradora	N/A	8	8	8	8	8	7
Jefe del departamento de Contabilidad	N/A	8	8	8	8	8	7
Responsable de las afiliaciones de salud	N/A	8	8	8	8	8	7
Responsable de las afiliaciones de pensión	N/A	8	8	8	8	8	7
Recepcionista	N/A	8	8	8	8	8	7
Digitadora	N/A	8	8	8	8	8	7
Mensajero	N/A	8	8	8	8	8	7

Tabla 12 Muestra de estimación cuantitativa de la estimación de riesgos de COOPSEGUROS

6.10 ESTIMACIÓN DEL IMPACTO

El riesgo es el incidente que impide el cumplimiento de un objetivo. En informática el riesgo se describe como el producto de materialización de un daño sobre un activo por la probabilidad de ocurrencia de una amenaza, aprovechando las vulnerabilidades presentadas en el sistema.[42]

A continuación se presenta el análisis realizado anteriormente de forma gráfica, teniendo en cuenta la siguiente escala para calificar el valor de los activos, la magnitud del impacto y la magnitud del riesgo:

[42] Análisis de riesgos http://pegasus.javeriana.edu.co/~CIS1130SD03/Documentos_files/Analisis_de_Riesgos.pdf

Criterios de Valorización		
MA	10	Daño extremadamente grave
A	9	Daño muy grave
M	6-8	Daño grave
B	3-5	Daño importante
MB	1-2	Daño menor

Tabla 13 Criterios de Valoración Fuente el autor

DEGRADACIÓN						
IMPACTO		**1%**	**10%**	**50%**	**80%**	**100%**
VALOR	**MA**	M	A	A	MA	MA
	A	B	M	M	A	A
	M	MB	B	B	M	M
	B	MB	MB	MB	B	B
	MB	MB	MB	MB	MB	MB

Tabla 14 Nivel de Degradación Fuente el autor

Se evalúa el grado de repercusión que pueda tener cada activo, dentro de las dimensiones de valoración analizadas en los puntos anteriores, como son: Disponibilidad, integridad, Confidencialidad, Autenticidad y Trazabilidad. De acuerdo con lo establecido en la metodología MAGERIT V.3.

Los activos con calificación Media deberán ser re-evaluados por la organización para mejorar, cambiar o implementar nuevos controles, los de calificación muy Alta y Alta deberán ser objeto de atención prioritaria, pues el riesgo esta descubierto y la empresa está expuesta.

Para el diseño del mapa de riesgos informáticos se tuvo en cuenta cada uno de los factores de riesgos informáticos identificado en la tabla de amenazas, a los cuales se les asignó un valor de probabilidad de ocurrencia por un valor de la magnitud del daño causado a los activos identificados en el desarrollo de este trabajo, teniendo en cuenta las entrevistas realizadas al personal del área de afiliaciones de COOPSEGUROS (Ver anexo b).

A continuación se muestra la Matriz del análisis de riesgos realizada en el área de afiliaciones de COOPSEGUROS:

Tipo de activo	Valorización Estimación de Riesgos						Afectación
	[I]	[D]	[C]	[A]	[TS]	[TA]	
Sistema Operativo Windows 7	9	10	10	10	10	10	10
Computadores de escritorio Lenovo	9	9	5	10	10	10	9
Suite Ofimática Office 2013	9	7	10	7	7	7	8
Antivirus MacAfee Gratuito	9	8	5	7	7	7	7
Cableado categoría 5	5	5	5	9	9	9	7
Red LAN	5	7	7	8	8	8	7
Sistemas de vigilancia de Circuito Cerrado	5	6	8	7	8	8	7
Memorias USB, CD/DVD, Discos duros Externos Toshiba	5	5	9	8	7	7	7
Administradora	N/A	8	8	8	8	8	7
Jefe del departamento de Contabilidad	N/A	8	8	8	8	8	7
Responsable de las afiliaciones de salud	N/A	8	8	8	8	8	7
Responsable de las afiliaciones de pensión	N/A	8	8	8	8	8	7
Recepcionista	N/A	8	8	8	8	8	7
Digitadora	N/A	8	8	8	8	8	7
Mensajero	N/A	8	8	8	8	8	7
Medios de Impresión Impresoras HP	5	5	5	7	7	7	6
Router	5	5	4	7	8	8	6
Telefonía ETB	5	5	5	4	7	7	6
Internet ETB	5	5	5	4	7	7	6

Tabla 15 Matriz de análisis de riesgos de COOPSEGUROS

6.11 ANÁLISIS DE RIESGOS PROMEDIO.

De acuerdo con el resultado de la Tabla 15 Matriz de riesgos de COOPSEGUROS, en donde se evidencia una valoración de cada activo de acuerdo con la magnitud del daño causado por la probabilidad de ocurrencia de una amenaza, como se observa a continuación existen riesgos de muy alto impacto (rojos) los cuales pueden implicar un daño importante de los activos de información ocasionados por daños a nivel de infraestructura y sistemas,

los riesgos de impacto alto (azul) pueden ser causados por negligencia por parte del personal y los riesgos de impacto medio (amarillo) causados por debilidades en los datos y la información.

Tipo de activo	Valorización Estimación de Riesgos						Degradación
	[I]	[D]	[C]	[A]	[TS]	[TA]	
Suite Ofimática Office 2013	9	7	10	7	7	7	80%
Antivirus McAfee Gratuito	9	8	5	7	7	7	70%
Sistema Operativo Windows 7	9	10	10	10	10	10	10%
Medios de Impresión Impresoras HP	5	5	5	7	7	7	60%
Computadores de escritorio Lenovo	9	9	5	10	10	10	90%
Router	5	5	4	7	8	8	60%
Cableado categoría 5	5	5	5	9	9	9	70%
Telefonía ETB	5	5	5	4	7	7	60%
Red LAN	5	7	7	8	8	8	70%
Internet ETB	5	5	5	4	7	7	60%
Sistemas de vigilancia de Circuito Cerrado	5	6	8	7	8	8	70%
Memorias USB, CD/DVD, Discos duros Externos Toshiba	5	5	9	8	7	7	70%
Administradora	N/A	8	8	8	8	8	70%
Jefe del departamento de Contabilidad	N/A	8	8	8	8	8	70%
Responsable de las afiliaciones de salud	N/A	8	8	8	8	8	70%
Responsable de las afiliaciones de pensión	N/A	8	8	8	8	8	70%
Recepcionista	N/A	8	8	8	8	8	70%
Digitadora	N/A	8	8	8	8	8	70%
Mensajero	N/A	8	8	8	8	8	70%

Tabla 16 Análisis de riesgos promedio

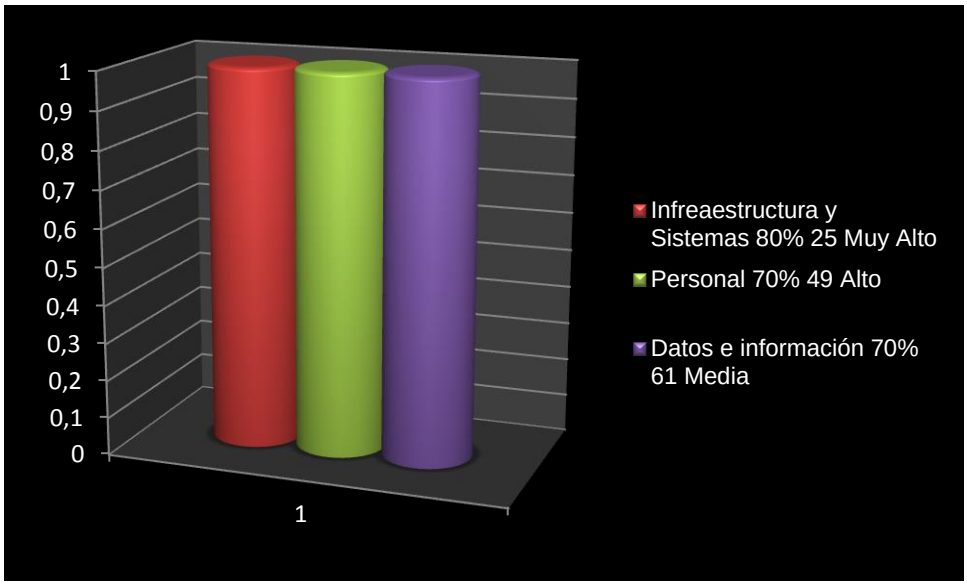
A continuación se computa porcentualmente cada probabilidad de ocurrencia de acuerdo con la valoración de los activos y la probabilidad de ocurrencias de las Amenazas Tablas 7 y 10.

Análisis de Riesgo Promedio		Probabilidad de Amenaza		
Magnitud de Daño	Infraestructura y Sistemas	80%	25	Muy Alto
	Personal	70%	49	Alto
	Datos e información	70%	61	Media

Tabla 17 probabilidad de Amenaza

Para dar una mayor visibilidad del análisis realizado y el impacto que probabilidad de cada amenaza, a continuación se presenta de forma gráfica los riegos identificados.

Figura 8. Exposición de los riesgos de acuerdo con la clasificación



Fuente: El autor

Como se puede observar en la gráfica No. 8 los activos del área de afiliaciones de COOPSEGUROS se encuentran en un nivel de ocurrencia alto, de acuerdo con la clasificación dada (Infraestructura y sistemas, Personal, Datos e información), se evidencia que la empresa no cuenta con un inventario que le permita clasificar sus activos, identificar las amenazas a las

que están expuestos cada uno de ellos y tomar acciones para minimizar el impacto que esto pueda causar a la organización.

Una vez realizado el inventario de activos, la identificación de amenazas y la valoración de cada una de forma detallada, el Gerente de la organización cuenta información de la situación actual en la que se encuentra el proceso de afiliaciones y por lo tanto podrá identificar en dónde debe empezar a tomar planes de acción.

7. ANÁLISIS DE LA INFORMACIÓN

7.1 GESTIÓN DE RIESGOS

Una vez realizado el análisis de riesgos en el área de afiliaciones de COOPSEGUROS se evidencia la exposición al riesgo y el impacto que estos pueden tener en la organización, lo que ha permitido determinar la siguiente calificación de los riesgos:

- Es muy alto por lo anterior requiere un nivel de atención urgente
- Es alto por lo que se debe prestar atención
- Es medio por lo que se debe analizar para realizar el debido tratamiento de los mismos

Producto del análisis, la compañía cuenta con información para tomar decisiones conociendo qué es lo que se debe proteger (activos valorados = de lo que se quiere proteger (amenazas valoradas)) y que se ha protegido (salvaguardas valoradas). Todo esto resumido en los valores de impacto y riesgo. [43]

7.2 IDENTIFICACIÓN DE RIESGOS CRÍTICOS

Todas las organizaciones tienen un nivel de exposición al riesgo en sus activos, sin embargo es importante identificar cuáles son los activos que poseen un mayor nivel de riesgo con el fin de implementar salvaguardas para evitar una materialización de las amenazas. A continuación se presenta la

[43] Magerit versión 3.0 Metodología de Análisis de Riesgos de los Sistemas de Información. https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar.html

situación observada en el área de afiliaciones de COOPSEGUROS una vez evaluados los activos y conociendo el nivel de riesgo a los que se encuentran expuestos:

7.2.1. INFRAESTRUCTURA Y SISTEMAS

A nivel de infraestructura y sistemas, los activos de información en el área de afiliaciones de COOPSEGUROS se encuentran expuestos a un nivel de riesgo del 80% de probabilidad de ocurrencia, lo que le implica a la compañía tomar de manera urgente medidas correctivas para proteger sus activos.

Tipo de activo	Valorización Estimación de Riesgos						Degradación
	[I]	[D]	[C]	[A]	[TS]	[TA]	
Suite Ofimática Office 2013	9	7	10	7	7	7	80%
Antivirus McAfee Gratuito	9	8	5	7	7	7	70%
Sistema Operativo Windows 7	9	10	10	10	10	10	10%
Medios de Impresión Impresoras HP	5	5	5	7	7	7	60%
Computadores de escritorio Lenovo	9	9	5	10	10	10	90%
Router	5	5	4	7	8	8	60%
Red LAN	5	7	7	8	8	8	70%
Cableado categoría 5	5	5	5	9	9	9	70%

Tabla 18 Magnitud de daño Infraestructura y sistemas

7.2.2. PERSONAL (RECURSO HUMANO)

Los activos relacionados con el recurso humano de la organización son los más vulnerables, como se pudo observar en el análisis de riesgos realizado en el área de afiliaciones de COOPSEGUROS se evidenció un nivel de riesgo del 70% asociado a la probabilidad de ocurrencia de una amenaza asociada con el personal de esta área, por lo que implica que la organización implemente medidas correctivas y cree políticas de Seguridad de la Información.

Tipo de activo	Valorización Estimación de Riesgos						Degradación
	[I]	[D]	[C]	[A]	[TS]	[TA]	
Administradora		8	8	8	8	8	70%
Jefe del departamento de Contabilidad		8	8	8	8	8	70%
Responsable de las afiliaciones de salud		8	8	8	8	8	70%
Responsable de las afiliaciones de pensión		8	8	8	8	8	70%
Recepcionista		8	8	8	8	8	70%
Digitadora		8	8	8	8	8	70%
Mensajero		8	8	8	8	8	70%

Tabla 19 Magnitud de daño Personal (Recurso humano)

7.2.3. DATOS E INFORMACIÓN

La información de la compañía es el activo más importante en las organizaciones, de acuerdo con el análisis de riesgos realizado en el área de afiliaciones de COOPSEGUROS se observó un nivel de riesgo de 70% asociado a la materialidad de vulnerabilidades en la información y los datos de la compañía, estos resultados deben llamara la atención del gerente de la compañía por lo que se deben implementar medidas correctivas de manera urgente así como la creación de Políticas de Seguridad de la Información.

Tipo de activo	Valorización Estimación de Riesgos						Degradación
	[I]	[D]	[C]	[A]	[TS]	[TA]	
Comunicaciones Telefonía ETB	5	5	5	4	7	7	60%
Herramientas de Internet ETB	5	5	5	4	7	7	60%
Sistemas de vigilancia de Circuito Cerrado	5	6	8	7	8	8	70%
Memorias USB, CD/DVD, Discos duros Externos Toshiba	5	5	9	8	7	7	70%

Tabla 20 Magnitud de daño Datos e Información

De acuerdo con el análisis de riesgos realizado a los activos de información asociados al proceso de afiliaciones de COOPSEGUROS se evidencia una exposición al riesgo alto con un promedio del 80% asociado a deficiencias a nivel de seguridad en infraestructura, sistemas de información, la información de la compañía y el personal. Por lo anterior es de vital importancia que la Gerencia de COOPSEGUROS tome acciones correctivas e implemente salvaguardas que minimicen la materialización de los riesgos a los cuales se encuentran expuestos los activos informáticos de la compañía.

8. DISEÑO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

El propósito de las políticas de seguridad informática, es proteger los activos de información de las amenazas a las que se encuentra expuesta, con el fin de establecer mecanismos para mitigar o minimizar el impacto de los riesgos identificados la compañía. Teniendo en cuenta la exposición al riesgo en el que se encuentran los activos de información del área de afiliaciones de COOPSGUROS se identifica la necesidad de implementar políticas de seguridad informática, las cuales deben ser dirigidas a los funcionarios y personal involucrado en el proceso con el objetivo de proteger el objetivo más importante de la compañía, la información.

Es importante que las políticas de seguridad informática sean parte de la cultura empresarial y por tal motivo se vea el compromiso por parte de la Alta Gerencia para el diseño, difusión, consolidación y cumplimiento de las mismas. A continuación se plantean Políticas de Seguridad Informática para el área de afiliaciones de COOPSEGUROS con el propósito de salvaguardar los activos de información.

8.1. OBJETIVOS

- Proteger los sistemas de información del área de afiliaciones de COOPSEGUROS frente a amenazas de seguridad informática internas o externas asegurando el cumplimiento de la confiabilidad, integridad, disponibilidad y confidencialidad de la información.

- Implementar medidas de seguridad informática comprendidas en la Política apoyados en la alta Dirección alineadas con la estrategia y los objetivos de la compañía.

8.2. RESPONSABILIDAD

La Dirección y todo el personal de COOPSEGUROS independiente de su nivel jerárquico dentro de la organización serán los responsables de aplicar y cumplir con las Políticas de Seguridad Informática, este cumplimiento es de carácter obligatorio una vez sean aprobadas y divulgadas al interior de la organización.

8.3. CUMPLIMIENTO

Para la implementación de la estrategia de Seguridad Informática, COOPSEGUROS debe regirse por lo establecido en la normatividad vigente aplicable propiamente al negocio desarrollado por la compañía, con el fin de evitar incumplimientos y violaciones de las leyes del derecho civil, penal y los requisitos establecidos de seguridad informática.

8.4 SANCIONES PREVISTAS POR INCUMPLIMIENTO

El incumplimiento de lo dispuesto en las políticas de seguridad informática, tendrá como resultado sanciones o llamados de atención de acuerdo al nivel de incumplimiento. Las políticas diseñadas serán una guía procedimental y medio de comunicación basada en los lineamientos establecidos en la norma ISO 27001 la cual indica los estándares adecuados a nivel de Seguridad Informática.

8.5 POLITICAS DE SEGURIDAD INFORMÁTICA DIRIGIDAS AL PERSONAL

Como se evidenció en el análisis de riesgos realizado en el área de afiliaciones de COOPSEGUROS la exposición al riesgo presentado por negligencias del personal es alto, por lo que es necesario implementar políticas de seguridad dirigidas al personal del área de afiliaciones y a las demás que intervienen en este proceso, estas políticas deben ser difundidas con el fin de hacer un buen uso y mantenimiento de las mismas. De acuerdo a la confidencialidad de la información, el personal de la compañía deberá trabajar acorde a los códigos de ética profesional, las normas y procedimientos establecidos en los contratos y el reglamento interno de la organización.

- Todos los funcionarios de la compañía y los usuarios internos y externos que intervienen en los Sistemas de información, recibirán una adecuada capacitación y actualización periódica de las normas, procedimientos y políticas de seguridad informática

- Se prohíbe todo tipo de publicación de información como: ubicación, nombre de dispositivos, marcas, entre otras; mediante etiquetas o en la configuración de los equipos de red, como: routers, servidores, clientes, etc.

- Las contraseñas utilizadas para la configuración de redes y telecomunicación deben estar basadas en un estándar que incluya aspectos como: estructura, tiempo de validez, reutilización, etc. Cada funcionario deberá tener una identificación única en cada sistema al que tenga acceso (usuario) y esta debe estar acompañada de un elemento de autenticación (contraseña) la cual será de carácter personal y confidencial para la utilización de los recursos tecnológicos necesarios para realizar sus labores.

- Los recursos informáticos de la compañía dispuestos para la operación del negocio, deben ser usados únicamente para fines laborales. El producto del uso de estos recursos tecnológicos será de propiedad de COOPSEGUROS, cualquier otro uso está sujeto a previa autorización de la Gerencia.

- Todo funcionario y/o usuario interno o externo deberá firmar un acuerdo de confidencialidad y un acuerdo de seguridad de los sistemas de información para hacer uso de los recursos tecnológicos de

COOPSEGUROS, este acuerdo debe ser firmado antes de que sea otorgado el login de acceso a los equipos y al sistema.

- El funcionario es el responsable de todas las actividades relacionadas con su identificación. Esta identificación no puede ser utilizada por otra persona diferente a la que se le otorga, por lo anterior el usuario no debe permitir que otro individuo realice labores bajo su identidad, de la misma forma que los usuarios no deben realizar actividades bajo la identidad de otra persona. La utilización de los activos informáticos por parte de terceras personas con consentimiento del usuario o por descuido o negligencia, lo hace responsable de los posibles daños que esto pueda ocasionar.

- El personal del área de afiliaciones de COOPSEGUROS que envié información privada a terceros deberá mantener un registro de toda la divulgación (correo) y este debe contener qué información fue revelada, a quién fue entregada y la fecha de envió.

- Si se transporta información sensible de la compañía en medio legibles por el computador como: CD´s memorias USB, entre otras, esta información deberá ser encriptada, siempre y cuando el receptor acepte el intercambios de información cifrada mediante una herramienta de cifrado. Así mismo si se va a trasmitir datos sensibles a través de cualquier canal de comunicación, estos datos deben ser enviados de forma encriptada.

- El internet está limitado exclusivamente para fines laborales, los usuarios de Internet deben ser advertidos de la existencia de recursos tecnológicos que generan reportes sobre las actividades realizadas. Toda comunicación mediante correo electrónico interno se considera una comunicación de tipo laboral por lo que podrá ser supervisada por la administración.

- Todos los funcionarios que dispongan de correo electrónico institucional están obligados a revisarlo al menos tres veces al día y será su responsabilidad mantener espacio libre en el buzón.

- Está prohibido el uso del correo electrónico con fines religiosos, políticos, lúdicos o de carácter personal en beneficios de terceros o que involucre derechos fundamentales de las personas. Por lo anterior se

prohíbe él envió, reenvió o la transmisión de mensajes humorísticos, pornográficos, tipo cadena, publicitarios o cualquier otro mensaje ajeno a temas laborales.

- En caso que el usuario reciba un correo no deseado o SPAM debe abstenerse de abrirlo y avisar inmediatamente a la administración.

- Todos los dispositivos de red deberán estar correctamente salvaguardados, teniendo en cuenta aspectos como la ubicación, protección física y el suministro eléctrico.

- El personal bien sea interno o externo que realice trabajos de configuración de los equipos de red deberá contar con una certificación o título que respalde sus capacidades y conocimientos.

- Si el usuario está conectado a un sistema que contiene información sensible de la compañía, esté no debe dejar el computador desatendido sin cerrar primero la sesión del mismo.

- Las contraseñas no deben ser guardadas de forma legible en archivos de Excel, Word, teclas de función terminal, archivos de texto, en los computadores o en cualquier otra ubicación que pueden ser tomadas por personas no autorizadas, del mismo modo se prohíbe tener las contraseñas en cualquier medio impreso.

8.6 POLITICAS DE SEGURIDAD INFORMÁTICA DIRIGIDAS A LA INFRAESTRUCTURA Y SISTEMAS.

- Es obligación de la Gerencia de la compañía establecer un área o departamento el cual será el encargado de realizar mantenimiento periódico preventivo y correctivo a los equipos, la conservación de su instalación, la verificación de la seguridad física en informática y respectivo acondicionamiento. Por lo que se debe crear un procedimiento formal en el que se especifique a los responsables, las fechas, la elaboración de informes, entre otros, que indique la forma en la que se realizará el mantenimiento.

- Periódicamente se deberá actualizar y llevar un inventario de los equipos y dispositivos tecnológicos que formen parte del sistema

informático de la compañía, independiente que estén o no en uso, el inventario debe contener parámetros como: proveedor, fecha de adquisición, modelo, manual técnico y de usuario, garantías, usuario responsable entre otros aspectos que se consideren.

- Se deberá implementar controles para las áreas en donde se ubican los dispositivos de alta importancia como: cuartos de servidores o comunicaciones y de igual manera se debe registrar las actividades realizadas por el personal que accede a estas áreas.

- Cualquier cambio y/o actualización de los sistemas de información deben ser realizado por personal autorizado y deberá contar con la documentación respectiva que soporte dichos cambios.

- El sistema debe limitar el número de intentos consecutivos al ingresar la contraseña. Una vez superado los tres intentos el usuario debe pasar a un estado de suspendido, bloqueado o deberá ser desconectado dependiendo la intencionalidad con la que se quiera ingresar.

- Está prohibido realizar mantenimiento a equipo de cómputo que no sean propiedad de COOPSEGUROS.

- Ningún equipo electrónico de la compañía podrá salir de la misma sin una autorización firmada que soporte la salida del equipo por personal autorizado.

- Todo cliente, proveedor o tercero deberá contar con autorización para ingresar a la compañía cualquier equipo electrónico donde pueda obtener información como: equipos de video, cámaras, celulares, portátiles, entre otros.

- Los equipos de cómputo deben quedar apagados cada vez que no haya presencia de funcionarios en la oficina (durante la noche) con el fin de proteger la seguridad de la compañía.

8.7 POLITICAS DE SEGURIDAD INFORMÁTICA PARA EL MANEJO DE INFORMACIÓN Y DATOS

- Todos los computadores del área de afiliaciones de COOPSEGUROS deben tener establecida la configuración de cierre de sesión automática después de un lapso de inactividad del equipo.

- Se debe contar con todas las licencias de software, estas deben estar custodiadas por el personal autorizado, así mismo se deberá hacer una revisión de las mismas mínimo una vez al año, con el fin de garantizar que los equipos cuenten con software legal y autorizado por la compañía.

- COOPSEGUROS deberá implementar mecanismos para que todos os archivos que son descargados de Internet sean validados por un software de detección de virus informático, antes de ser transmitidos a los computadores del área de afiliaciones.

- La compañía debe contar con un área de sistemas la cual deberá revisar periódicamente los registros de cada uno de los sistemas de información para tomar acciones oportunas sobre posibles amenazas a nivel de seguridad de la información.

- El área de sistemas de COOPSEGUROS deberá correo un software de identificación de vulnerabilidades como mínimo una vez al año, adicionalmente el área de afiliaciones deberá contar con un software de cortafuegos y antivirus que adicionalmente cuente con una consola de administrador la cual permita visualizar los reportes de eventos relacionados con vulnerabilidades, a nivel general COOPSEGUROS deberá contar con un firewall que proporcione un software de IDS (Instrusion Detection System), detección de virus y bloqueo de correos no deseado.

- Se deberá contar con la opción de gestión de log (archivos de transacción) para los sistemas y las aplicaciones del área de afiliaciones de COOPSEGUROS; también se deberá contar con una aplicación de monitoreo que alerte sobre el mal funcionamiento de un sistema de información.

- A toda la información sensible de la compañía que se encuentre en los sistemas informáticos, se les debe realizar un backup con una periodicidad definida, y a esta información se le deben hacer pruebas

para confirmar el buen estado de la misma, así como una backup de cada copia minimizando el riesgo por daño o deterioro de los equipos.

- El único elemento conectado directamente a Internet será el firewall, garantizando que toda conexión a internet pase primero por el firewall.

- Es necesario que todos los equipos cuenten con Proxy que filtre todo contenido activo como java, adobe, flash player, ActiveX debido a que estos datos pueden implicar la seguridad de los sistemas de información de la compañía.

- Se deben establecer acuerdos relacionados al manejo de la información de COOPSEGUROS por parte de los terceros, los cuales debe contener cláusulas de confidencialidad y reserva de la información.

8.8. ACTUALIZACIÓN Y DIVULGACIÓN DE LAS POLITICAS DE SEGURIDAD INFORMÁTICA.

Las políticas de seguridad informática se deben aprobar por la Gerencia de la compañía a su vez debe ser monitoreadas y divulgadas en la organización, asegurando que todos los empleados, proveedores, clientes y demás partes involucradas conozcan los lineamientos establecidos en COOPSEGUROS nivel de seguridad informática.

Es importante que la Gerencia de COOPSEGUROS incorpore personal que cuente con conocimiento certificado en evaluación y análisis de riesgos que le permitan evaluar y monitorear las políticas definidas para minimizar los daños a los que está expuesta a nivel de seguridad informática, velando por el cumplimiento y actualización de las políticas.

9. PLAN DE DIVULGACIÓN, SENSIBILIZACIÓN Y CAPACITACIÓN EN POLÍTICAS DE SEGURIDAD INFORMÁTICA

Una vez COOPSEGUROS establezca las políticas de Seguridad Informática en el área de afiliaciones, es necesario diseñar una estrategia para la divulgación y sensibilización de las mismas, dirigida a los funcionarios y personas que intervienen en el proceso.

A continuación se presenta un Plan diseñado como propuesta para capacitar y divulgar las políticas al interior de la organización:

- Realizar una planificación o cronograma de capacitación sobre políticas de seguridad informática, este debe ser publicado para que todos los funcionarios lo conozcan a demás debe ser de carácter obligatorio la asistencia de todos.
  Responsables: La Dirección de COOPSEGUROS y las personas calificadas que diseñaron las Políticas de Seguridad Informática

- Mediante la intranet realizar campañas de divulgación y tips para tener en cuenta diariamente con el fin de asegurar los activos de la compañía, cumpliendo con las políticas de seguridad informática.

- La compañía cuenta con cartelera física, esta se puede aprovechar para realizar campañas de divulgación y concientización de la aplicación y cumplimiento de las Políticas de Seguridad Informática.

- Realizar capacitaciones de acuerdo con el cronograma establecido de una manera dinámica, a través de videos que permitan educar a cada uno de los empleados en seguridad informática.

- Desarrollar talleres y actividades lúdicas que permitan a cada funcionario de la compañía generar cultura de seguridad conociendo y cumpliendo con las Políticas de Seguridad Informática diseñadas.

10. CONCLUSIONES

Mediante la elaboración del presente proyecto se puede concluir que el objeto de estudio se cumplió debido a que se logró evidenciar que el área de afiliaciones de COOPSEGUROS no cuenta con procesos normativos o directriz alguna orientada a brindar seguridad a los sistemas de información. Tampoco cuenta con mecanismos de evaluación, lo que no le permite identificar las amenazas, vulnerabilidades y riesgos a los que se encuentran expuestos sus activos de información.

Con el análisis realizado a la información recopilada del proceso de afiliaciones se evidencio la necesidad de implementar políticas de seguridad informática que contribuyan a la mejora continua de los procesos, con el fin de asegurar los activos de la compañía y el funcionamiento del negocio. Es importante el avance que está teniendo la compañía a nivel operativo pero debe velar por el aseguramiento de la información y estar consciente de la responsabilidad que tiene al mantener un volumen importante de información confidencial de usuarios, clientes y proveedores.

Con la identificación de vulnerabilidades junto con el análisis realizado a los riesgos se pudo observar el nivel de ocurrencia y el impacto que podría causar a la compañía la materialización de alguno de estos. Se agruparon los activos y se les dio una clasificación (infraestructura, sistemas, personal y datos e información) dando como resultado un nivel de probabilidad de ocurrencia mayor al 70% (Alto) para cada uno; con esta información la empresa puede tomar acciones de manera urgente y oportuna, con el fin de proteger sus sistemas de información.

Se evidencia falta de controles para proteger la información que se intercambia con las diferentes entidades o terceros, lo que puede generar impactos negativos y de alto riego para la compañía, trayendo como consecuencia, incumplimiento con los clientes, imagen negativa y posibles implicaciones de carácter jurídico y normativo, por lo que se hace necesario

que COOPSEGUROS implemente mecanismos de seguridad que permitan garantizar la autenticidad, integridad y confidencialidad de los datos.

Producto de las entrevistas realizadas al personal del área de afiliaciones de COOPSEGUROS se identificaron vulnerabilidades de alto impacto, entre las que se encuentran: ausencia de capacitación a nivel de seguridad informática, deficiencia en las contraseñas utilizadas o no existen, manipulación de la información por varios funcionarios sin tener controles, los equipos electrónicos no cuentan con permisos de acceso a nivel de perfiles o privilegios teniendo en cuenta la labor que realiza y su cargo. Así mismo se identificaron riesgos a nivel físico como sobrecargas eléctricas, falta de ventilación, posibles incendios por acumulación de papel.

COOPSEGUROS no cuenta con planes de continuidad en caso de ocurrir una eventualidad, lo que lo dificultaría el normal funcionamiento en el proceso de afiliaciones de la compañía, en caso de materializarse una vulnerabilidad; esto a su vez traería impactos negativos a nivel económico, reputacional, jurídico, debido a incumplimientos de las condiciones ofrecidas a sus clientes.

Una vez realizado el proyecto sobre el área de afiliaciones de COOPSEGUROS, una pyme que no cuenta con personal calificado ni mecanismos que le permitieran evaluar la realidad de cómo se encuentra el proceso actualmente a nivel de seguridad informática, el Gerente de la compañía tendrá una visión más clara de cómo lo puede afectar la falta de políticas y controles en sus procesos, así como una solución a la problemática evidenciada.

11. RECOMENDACIONES

Conforme a la recopilación de información y el análisis de riesgos realizado en el área de afiliaciones de COOPSEGUROS, se realizan las siguientes recomendaciones, las cuales serán presentadas al Gerente de la compañía, como retribución a la disposición y colaboración ofrecida durante la elaboración de este proyecto:

Implementar controles de manera urgente en toda la cadena del proceso de afiliaciones, manteniendo un nivel de seguridad alto sobre la información y los datos sensibles que maneja la compañía, es necesario que la empresa conozca y se asesore de la normatividad Colombiana vigente en cuanto a seguridad de la información se refiere.

Establecer un grupo de personal calificado que se identifique plenamente dentro de la organización como la autoridad, los cuales deben establecer controles, normas y/o las políticas de seguridad informática, velar por su cumplimiento y actualización así como de la comunicación y divulgación de las mismas dentro de la organización.

Crear un área de informática o un grupo de especialistas en esta área que permita apalancar la aplicación de políticas y controles, que monitoreen permanentemente las vulnerabilidades y amenazas a las que están expuestas los activos de información de la compañía, proponiendo soluciones para mejorar los procesos de seguridad del área.

Realizar capacitaciones periódicas dirigidas al personal de la compañía en temas asociados a la normatividad vigente y la que implemente la empresa para la mitigación de riesgos, estas capacitaciones deben ser didácticas y realizadas en un leguaje entendible para todos los funcionarios, adicionalmente su participación debe ser de carácter obligatorio.

REFERENCIAS BIBLIOGRÁFICAS

GAONA VASQUEZ Karina, aplicación de la metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información en la empresa Pesquera e Industria Bravito S.A., Tesis Universidad Politécnica Salesiana sede Cuenca, Octubre 2013

PAE, Magerit Metodología de Análisis y gestión de riesgos de los Sistemas de Información. [En línea] [Citado el 21 de septiembre, 2017]. Disponible en internet:https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WRXXmpiGOpo

METODOLOGÍA. Mejores prácticas recomendadas en Seguridad Informática para la implementación y seguimiento de los Sistemas de Gestión de la Seguridad Informática (SGSI). [En línea] [Citado el 20 de septiembre, 2017] Disponible en Internet: http://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf

DIAZ Fabián, Implementación de un SGSI en la comunidad Nuestra Señora de Gracia alineado tecnológicamente con la norma ISO 27001. [En línea] [Citado el 21 de septiembre, 2017]. Disponible en: http://www.konradlorenz.edu.co/images/stories/articulos/SGSI.pdf

SEGURIDAD Informática, Pilares básicos. [En línea] [Citado el 26 de septiembre, 2017]. Disponible en Internet: http://ecaths1.s3.amazonaws.com/schsistemas22011/1438588133.segrinfo_pilares.pdf

MANUAL de Políticas de Seguridad de la información, Instituto Colombiano de Crédito y Estudios Técnicos en el Exterior. [En línea] [Citado el 27 de septiembre, 2017]. Disponible en internet: https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manualseguridadinformacion.pdf

NORMA Técnica. Normatividad y certificaciones aplicadas a SGSI. (ISO 2700 –ISO 27001 –ISO27002-ISO 27003 –ISO 27004-ISO 27005- ISO 27035:2011, COBIT, ITIL, entre otras. [En línea] [Citado el 29 de septiembre, 2017]

Disponible en internet: http://www.iso27000.es/download/doc_iso27000_all.pdf

LEY Colombiana 1273 de 2009 delitos informáticos. [En línea] Citado el 21 de septiembre, 2017]. Disponible en internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

MINTIC. Ley 1273 de 2009. [En línea] [Citado el 22 de septiembre de 2017] Disponible en internet: http://www.mintic.gov.co/portal/604/w3-article-3705.html

EL PROYECTO DE INVESTIGACIÓN. Metodología para realizar trabajos aplicados. [En línea] [Citado el 21 de septiembre, 2017]. Disponible en internet: http://www.smo.edu.mx/colegiados/apoyos/proyecto-investigacion.pdf

PULIDO Andrea, RINCON Paulo, Diseño de Políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector de transporte de Bogotá. Trabajo de grado para obtener el título de Ingeniería de Sistemas de la Universidad San Buenaventura, Bogotá 2010

NTC –ISO/IEC 27001 Tecnología de la Información. Técnicas de Seguridad en Sistemas de Seguridad de la Información (SGSI) requisitos. Norma Técnica Colombiana. Icontec Internacional.

CIRCULAR EXTERNA 052 DE 2007, Superfinanciera De Colombia, capitulo décimo segundo: requerimientos mínimos de seguridad y calidad en el manejo de información a través de canales y medios de distribución de productos y servicios. Entra en vigencia mediante tres etapas: la primera inicia el 01° de julio de 2008, la segunda el 1° de enero de 2009 y la última el 1° de enero de 2010.

CERTICAMARA. ABC para proteger los datos personales Ley 1581 2012 decreto 1377 de 2013. [En línea] [Citado el 02 de octubre, 2017]. Disponible en internet: http://www.ceticamara.com.

METOGOLOGIA para la gestión de la Seguridad Informática, [En línea] [Citado el 20 de octubre, 2017]. Disponible en internet:

http://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf

TECNOLOGIA del futuro, [en línea] [citado el 22 de octubre, 2017]. Disponible en internet: http://nizquierdo3.botot.com.co/2012/12/la-facilidad-de-la-nueva-era.html

TECNOLOGIA de la información, Técnicas de Seguridad. Sistemas de la Gestión de la Seguridad de la Información (SGSI) Requisitos. Norma Técnica Colombiana. ICONTEC Internacional. Norma NTC –ISO/IEC 27001

POLITICAS de seguridad a nivel de TI, [en línea] [citado el 18 de octubre, 2017]. Disponible en internet: http://capacityacademy.com/2014/03/17/son-las-politicas-de-seguridad-de-la-tecnologia-de-la-informacion/

POLITICAS de seguridad de la información, [en línea] [citado el 01 de noviembre, 2017]. Disponible en internet: http://www.segu-info.com.ar/politicas/polseginf.htm

UBIRBE Otálora Carlos Javier, Estudiante de Ingeniería de Sistema de la Universidad Nacional Abierta y a Distancia UNAD, presenta proyecto de Seguridad Informática para las Bases de Datos del Campus Virtual de la UNAD.

DAZA Sandra Milena Y Giraldo Murillo Andrés, estudiantes de Ingeniería de Sistemas de la EAN realizan investigación de Aplicación de un sistema de Gestión de Vulnerabilidades para la Infraestructura Informática de ABC Ltda.

SISTEMA de gestión- vulnerabilidades, {en línea] [citado el 31 de octubre, 2017], Disponible en internet: Minerva.ttp://biblioteca.universia.net/html_bura/ficha/params/title/aplicacion-sistemagestion-vulnerabilidades-infraestructura-informatica-abc-ltda/id/55867643.html
http://tesis.ipn.mx/jspui/bitstream/123456789/8428/1/IF2.52.pdf.

JARAMILLO Lara José Luis, presenta Propuesta de trabajo de grado para obtener el título de Ingeniero Informático de la Universidad Autónoma de Occidente en la ciudad de Santiago de Cali, tema: Estandarización de

Políticas y controles de seguridad de la información para el proceso “Gestionar la Seguridad Informática y la Continuidad de las Soluciones de TIC” (MP11P4).

MONCAYO Diana, estudiante de Ingeniería de Sistemas de la Escuela Politécnica Nacional de la ciudad de Quito- Ecuador el Modelo de Evaluación de Riesgos en activos Tic´s para pequeñas y medianas empresas del sector automotriz.

COOPSEGUROS, [en línea] [citado el 11 de noviembre de 2017] disponible en internet: https://www.coopseguros.com.co/

PLAN de continuidad de negocio [en línea] [citado el 22 de octubre, 2017] Disponible en internet: http://www.iso27000.es/iso27000.html

SEGURIDAD en bases de datos, [en línea] [citado el 24 de octubre, 2017]. Disponible en internet: https://msdn.microsoft.com/esco/library/cc434708%28v=vs.71%29.aspx?f=255&MSPPError=-2147217396

CICLO PHVA del SG-SST, Plan de contingencia, [en línea] [citado el 25 de septiembre. 2017] Disponible en internet: http://www.bdigital.unal.edu.co/57426/42/43092659.2017.ANEXO%202.pdf

GUIA de Administración del Riesgo, [en línea] [citado el 24 de septiembre, 2017]. Disponible en internet: http://www.dafp.gov.co/

PADILLA PACHA Cristina, Análisis de riesgos Informáticos para la protección de los Sistemas de Información en el área de Tecnologías de Información del Gobierno Tunguragua.2012 p.79

ACTIVOS de Seguridad de la Información, [en línea] [citado el 26 de septiembre, 2017] Disponible en http://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-7.pdf

ANÁLISIS de riesgos, base de la Gestión Empresarial. [En línea] [Citado el 24 de septiembre, 2017] Disponible en internet:

http://www.criptored.upm.es/intypedia/video.php?id=introduccion-gestion-riesgos&lang=es

GUÍA de estudios ETS seguridad informática, [en línea] [citado el 26 de septiembre. 2017] Disponible en: http://www.buenastareas.com/ensayos/Horario-Voca-8-Segundo-Semestre/1513007.html

CONCEPTOS de seguridad informática, [en línea] [citado el 12 de octubre, 2017] Disponible en: http://www.fcca.umich.mx/descargas/apuntes/Academia%20de%20Informatica/Adm%C3%B3n%20de%20Centros%20de%20Computo%20%20%20R.C.M/UNIDAD%20IV.pdf

CALIDAD Ernst &Young Calidad en todo lo que hacemos, [en línea] [citado el 31 de octubre, 2017] Disponible en: http://www.ey.com/mx

ANÁLISIS y gestión de riesgos Tecnológicos, [en línea] [citado el 1 de noviembre, 2017] Disponible en internet: http://www.mnet.com.mx/analisis.html

NARANJO Bertha, Diseño de un plan estratégico de seguridad de información en una empresa del sector comercial, Universidad Superior Politécnica de Litoral, Guayaquil.

IMPLEMENTACIÓN de políticas de Seguridad de la Información, [en línea] [citado el 05 de noviembre de 2017] Disponible en internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

CRIPTOGRAFÍA, [en línea] [citado el 10 de noviembre de 2017] Disponible en internet: https: //www.genbetadev.com/seguridad-informatica/tipos-de-criptografia-simetrica-asimetrica-e-hibrida,

SISTEMA de Gestión de Seguridad de la Información (SGSI), [en línea] [citado el 15 de noviembre de 2017] Disponible en internet: http://repositorio.utp.edu.co/dspace/bitstream/11059/4117/1/0058A284.pdf

ANEXOS

ANEXO A

ENTREVISTA REALIZADA A LA ADMINISTRADORA

Nombre: Ana Rocío Guerra.

Perfil: Es la persona que centraliza las decisiones y la información, en general mantiene los procesos alineados con el fin de cumplir siempre al cliente en los servicios de afiliación a seguridad social, pensión y riesgos para independientes y empresas.

De acuerdo con la entrevista realizada se concluye:

a. La compañía ha venido creciendo su portafolio de servicios y así mismo su información, bases de datos, sistemas, soportes físicos de los clientes, pagos, entre otros.
b. Los procesos de la compañía son manuales y su información es contenida en bases de datos de Excel sin protección alguna, se tiene acceso a diferentes claves para ingresar a varias páginas para extraer o cargar datos personales de los clientes, pero únicamente se tiene instalado el antivirus, y no se guarda backup de la información contenida en las bases de datos.
c. No se tiene una base histórica de los clientes y no es fácil realizar seguimiento a un cliente y el estado en el que se encuentra su solicitud, diariamente se debe concluir la actividad que tiene cada empleado, pero en el caso que se presente un reclamo, no es fácil rastrear nuestra gestión.
d. Manejamos mucha información confidencial en físico y no tenemos establecido un protocolo para el manejo de esta información.
e. Estamos muy atentos a recibir sugerencias y recomendaciones para mejorar el proceso de afiliaciones.

ENTREVISTA REALIZADA A LA JEFE DEL DEPARTAMENTO DE CONTABILIDAD

Nombre: Marta Lucia Gámez

Perfil: Es la persona administra la parte contable de la compañía.

De acuerdo con la entrevista realizada se concluye:

a. Para el área contable si tenemos programa que le permite tener su contabilidad y datos financieros al día.
b. Se dificulta el proceso cuando se realiza un reclamo por parte de un cliente que presenta un pago pero no tiene el servicio.
c. Las planillas que se realizan para hacer los cargues contables que pasan primero por el área de afiliaciones presentan algunas inconsistencias, se adjunta la planilla y a veces faltan los soportes (cedulas, registros civiles, datos de la empresa)
d. Manejamos mucha información confidencial en físico y no tenemos establecido un protocolo para el manejo de esta información.
e. La información de los clientes la tenemos en Excel y compartimos los archivos por la Red interna.

ENTREVISTA REALIZADA A LOS RESPONSABLE DE LAS AFILIACIONES A SALUD, RIESGOS Y ARP.

Nombre: Jennifer Montañez Pinto – Responsable afiliaciones a salud

Nombre: Tatiana Ramírez Gómez – Responsable afiliaciones a Riegos y ARP.

Perfil: Son las personas encargadas de atender a los asesores y a los clientes, reciben las afiliaciones, los documentos personales de cada uno y diligencian los formatos para la afiliación. Esta información la almacenan en una base de datos por cada servicio y la reportan a cada entidad según corresponda.

De acuerdo con la entrevista realizada se concluye:

a. La información la recibimos físicamente y por correo electrónico escaneada, (cedulas, registros civiles) y se imprime. Se realiza la afiliación en el formato, se adjuntan los soportes y por cada paquete de cliente se diligencia en la base de datos para luego transmitir a cada entidad.
b. No se tiene establecido un control documental para el manejo adecuado de la información física
c. Los datos sensibles de cada cliente son incluidos en la base de datos de Excel y se transmiten a cada entidad, se comparten por la red interna, no cuentan con clave de bloqueo o alguna protección.

d. No se tiene una base de datos consolidada de los clientes que tiene actualmente la compañía. Son varios archivos que se crean diariamente.

ENTREVISTA REALIZADA A LA RECEPCIONISTA Y DIGITADORA

Nombre: Andrea Catalina Roa – Responsable del área de recepción

Nombre: Blanca Barreto Ramírez– Responsable de digitadora.

Perfil: Son las personas encargadas de recibir a los clientes y sus documentos la recepcionista recibe los documentos y los radica con un número y los ingresa a una planilla manual, este paquete lo entrega junto con una copia de la planilla a la digitadora para que ingrese la información a una base de datos y en ella lleva un control de que documentos entrego y cuando los radico y se lo entrega a las personas de afiliaciones.

De acuerdo con la entrevista realizada se concluye:

a. La información sensible de los clientes es manipulada por dos personas diferentes en el momento de recibirla.
b. La transcripción y envió de datos construidos en Excel diariamente y enviados al área de afiliaciones no cuenta con protección
c. No se tiene creado un backup de la información

ENTREVISTA REALIZADA AL MENSAJERO

Nombre: Carlos Andrés Tinaco – Responsable de la mensajería.

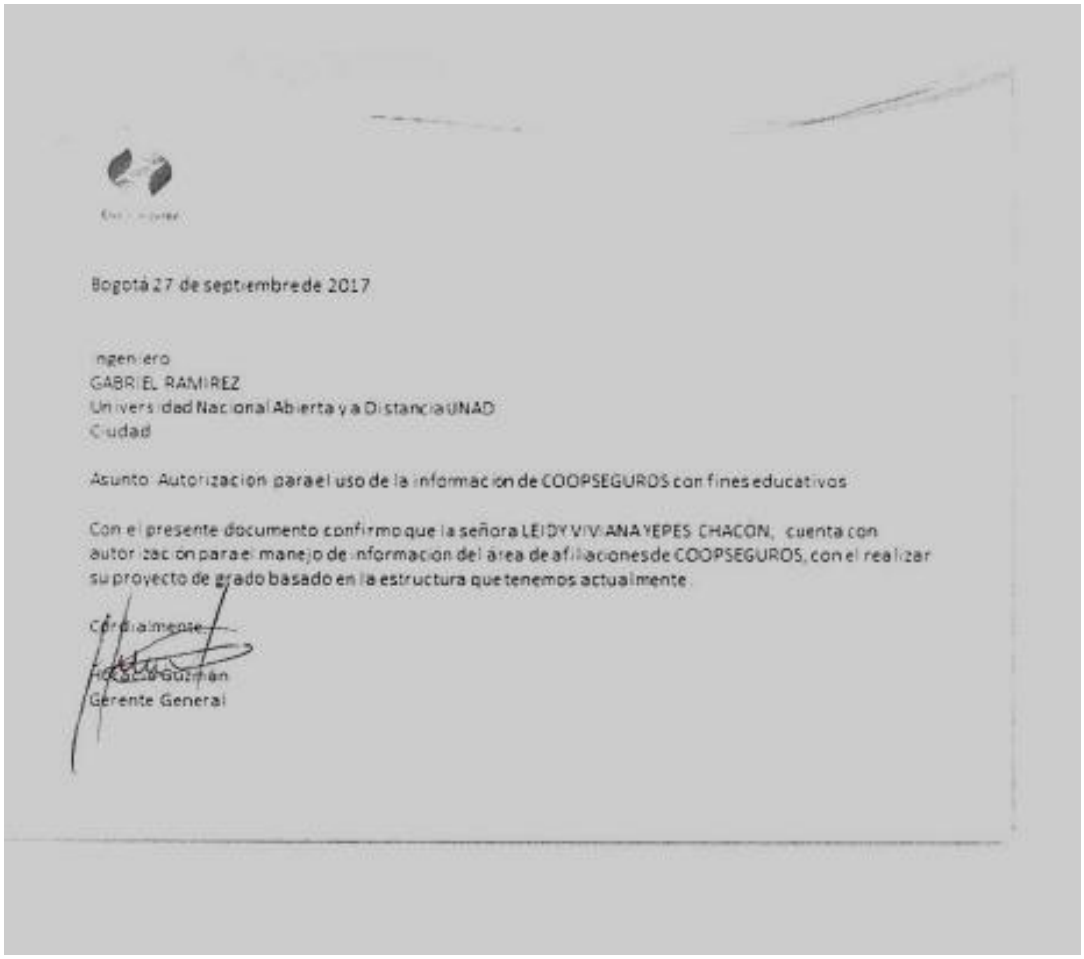
Perfil: Es la persona encarga de radicar directamente los formularios y los soportes de los afiliados en cada entidad de riesgos, salud y ARP.

De acuerdo con la entrevista realizada se concluye:

a. La información es entregada con unas indicaciones específicas, pero no se entregan en sobres sellados y se corre el riesgo de perder formularios o datos sensibles de los clientes.
b. Cuando se presentan devoluciones por diferentes motivos, el mensajero no siempre alcanza a llegar nuevamente y esta información es entregada en la oficina de Coopseguros al día siguiente.

ANEXO B

AUTORIZACIÓN DE COOPSEGUROS PARA EL MANEJO DE INFORMACIÓN



Bogotá 27 de septiembre de 2017

Ingeniero
GABRIEL RAMIREZ
Universidad Nacional Abierta y a Distancia UNAD
Ciudad

Asunto: Autorizacion para el uso de la informacion de COOPSEGUROS con fines educativos

Con el presente documento confirmo que la señora LEIDY VIVIANA YEPES CHACON, cuenta con autorizacion para el manejo de informacion del área de afiliaciones de COOPSEGUROS, con el realizar su proyecto de grado basado en la estructura que tenemos actualmente.

Cordialmente,

Hector Guzman
Gerente General

ANEXO C.

CRONOGRAMA DE ACTIVIDADES

CRONOGRAMA DE ACTIVIDADES																
MESES	AGOSTO				SEPTIEMBR				OCTUBRE				NOVIEMBRE			
SEMANAS	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Actividades																
Descripción del estado actual de la empresa	X	X	X	X	X											
Descripción de los activos de COOPSEGUROS						X	X	X								
Análisis de la información- identificación de vulnerabilidades, riesgos									X	X						
Valoración de los riesgos y su impacto de acuerdo con la norma ISO/IEC 27001:2013										X	X	X				
Diseño de Políticas												X	X			
Conclusiones													X			
Recomendaciones													X	X		
Entrega del proyecto															X	

Fuente: el autor