DISEÑO DE UN SISTEMA DE GESTIÒN DE SEGURIDAD DE LA INFORMACIÒN (SGSI) BASADO EN LA NORMA ISO/IEC 27001 PARA POSITIVA COMPAÑÍA DE SEGUROS S.A EN LA CIUDAD DE BOGOTÁ

JULIAN ANDRES ARDILA NAVARRETE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2016

DISEÑO DE UN SISTEMA DE GESTIÒN DE SEGURIDAD DE LA INFORMACIÒN (SGSI) BASADO EN LA NORMA ISO/IEC 27001 PARA POSITIVA COMPAÑÍA DE SEGUROS S.A EN LA CIUDAD DE BOGOTÁ

JULIAN ANDRES ARDILA NAVARRETE

PROYECTO DE GRADO

Director

SALOMON GONZALEZ GARCIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS E INGENIERIA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ

2016

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá D.C. 15/05/2016

El proyecto de grado lo dedico a mi amada familia, quienes con su inagotable amor y apoyo, me han acompañado durante toda mi vida. Igualmente brindo mi trabajo a aquellas personas que confiaron en mí y reconocen mi esfuerzo.

AGRADECIMIENTOS

Principalmente a Dios todopoderoso por permitir que llegara hasta este punto, a mi familia, en especial a mis padres por su aliento, amigos por su apoyo incondicional, a todos los profesionales de la vicepresidencia de TIC´S de Positiva Compañía de Seguros por su acompañamiento; también al Ing. Salomón García González por su guía, seguimiento y constante retroalimentación.

TABLA DE CONTENIDO

LISTAS DE TABLAS

Pág

LISTA DE ILUSTRACIONES

Pág

RESUMEN

El Proyecto de grado corresponde al diseño de un Sistema de Gestión de Seguridad de la Información basado en el estándar ISO/IEC 27001 de 2013 para la Casa Matriz de Positiva Compañía de Seguros S.A. Dicho sistema, contempla una serie de elementos, mecanismo, y lineamientos apropiados para el mejoramiento de la seguridad de la información al interior de la entidad en mención.

La estructura del proyecto, está dada por secciones, la primera de ellas concierne al Marco Referencial el cual consta de marco de antecedentes, contextual, teórico, conceptual y legal que soportan la investigación a desarrollar. Seguidamente se encuentra el aparte del Diseño Metodológico en el cual se describe los pasos a seguir a fin de recopilar información relevante, por ejemplo: línea y tipo de investigación, área de investigación, técnicas y herramientas de recolección de información.

La Metodología de desarrollo que por planteamiento relaciona, cuatro fases vitales, a saber:

Fase 1: Diagnostico de la situación actual en materia de seguridad informática en Casa Matriz
Fase 2: Identificar los activos informáticos, definir y aplicar de la metodología de análisis y gestión del riesgo.
Fase 3: Determinar y evaluar la aplicabilidad de los controles de seguridad de la información bajo la norma ISO/IEC 27002:2013
Fase 4: Definición de alcance, objetivos y política del Sistema de Gestión de Seguridad de la Información para la Casa Matriz de Positiva

Finalmente, en la sección de resultados y conclusiones se registra el impacto una vez se dio el desarrollo del proyecto de investigación así como los anexos que documentan la misma.

INTRODUCCIÒN

En la actualidad el sector asegurador es dinámico y está en un permanente proceso de actualización tecnológica; originando con esto significativos cambios en la gestión del negocio, pues es necesaria la adaptabilidad a los versátiles entornos económicos como a los crecientes niveles de seguridad, demandados por los mercados financieros y por supuesto por las personas.

En este afán de adaptarse y ser cada vez más competitivos las organizaciones hacen uso de las herramientas de tratamiento de la información para ofertar sus servicios a cualquier persona o entidad en cualquier lugar del mundo y con esto se abren los caminos para los riesgos informáticos.

Los riesgos a los que se ve enfrentada una entidad están comprendidos desde la pérdida de información de un PC hasta amenazas por Internet, que pueden llegar a generar desconfiguraciones de los sistemas informáticos y por ende interrupciones en la operación, impactos financieros y daños a la reputación de una empresa.

Positiva Compañía de Seguros no es ajena al complejo panorama que representan los ataques informáticos, por tanto se ve en la necesidad de diseñar e implementar un Sistema de Gestión de la Seguridad de la información-SGSI basado en el estándar ISO/IEC 27001 del 2013 que le permita asegurar y controlar sus procesos de negocio y fortalecer la confianza de sus grupos de interés.

1. TITULO

DISEÑO DE UN SISTEMA DE GESTIÒN DE SEGURIDAD DE LA INFORMACIÒN (SGSI) BASADO EN LA NORMA ISO/IEC 27001 PARA POSITIVA COMPAÑÍA DE SEGUROS S.A EN LA CIUDAD DE BOGOTÁ

2. DEFINICIÓN DEL PROBLEMA

Positiva Compañía de Seguros S.A. es una Entidad de economía mixta, adscrita al Ministerio de Hacienda y Crédito Público. Cuenta con cuatro certificaciones otorgadas por ICONTEC en las normas ISO 9001, ISO 14001, OSHAS 18001 con reconocimiento internacional de IQNET. Además de la certificación en NTC GP 1000 para la Gestión en el sector Público en Colombia.

Certificaciones, que han impactado positivamente en la imagen organizacional y han fortalecido la confianza a lo largo de la gestión pero que infortunadamente se han visto afectadas en el último año dada la falta de un SGSI estructurado que le permita a Positiva garantizar la confidencialidad, integridad y disponibilidad de los datos de sus clientes, de su operación, de que los riesgos de la seguridad de la información, sean reconocidos, asumidos, gestionados y minimizados de una forma ordenada, eficiente y adaptable a los cambios que se susciten en los riesgos, el entorno y las mismas tecnologías.

La tercerización de los sistemas de información y la falta de control sobre las bases de datos representan para la entidad factores de riesgo que la han expuesto a las principales amenazas en el manejo de la información, como lo son: Spam, Hoax y Malware (virus, gusanos, troyanos, rootkits, spyware y Keyloggers), además, violación y pérdida de información sensible en algunas áreas como:

- Información de personas jurídicas y naturales afiliadas al ramo de ARL
- Producción (número de primas emitidas) ramo Vida Grupo y ARL
- Información Financiera (Manipulación y pérdida parcial de información financiera)
- Backup en File server (Inexistencia de control sobre la accesibilidad y manipulación de la información contenida).

Por otro lado el administrador de sistemas en la compañía, actúa como un observador sobre la realización periódica de backups de información vital en el file server pero no como el responsable de establecer y mantener el sistema y un control frente al buen uso de las herramientas informáticas con las que cuenta la entidad. Por su parte, los funcionarios no conocen sus responsabilidades frente al proceso de seguridad de la información y tampoco han sido capacitados en el tema.

Dado lo anterior es necesario demostrar ¿Cómo el diseño de un Sistema de Gestión de Seguridad de la Información le proveerá a Positiva Compañía de Seguros S.A los elementos, mecanismo y lineamientos adecuados para mejorar la seguridad de la información al interior de la entidad?

3. JUSTIFICACIÒN

Los avances tecnológicos han generados cambios radicales en la forma de negociar y a su vez han expuesto a nuevos riesgos a las compañías. La facilidad de acceso a las redes y datos, propicia el ingreso no autorizado o mal intencionado y a su vez puede generar la pérdida y violación de la información entre otras graves consecuencias.

Dado que la información es el activo más valioso para las organizaciones debe ser mantenida con integridad y confidencialidad, conservando siempre su disponibilidad. De esto depende gran parte, los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para la consecución de objetivos organizacionales, como lo son la sostenibilidad y fortalecimiento financiero.

En el marco de la competitividad y sostenibilidad, el presente proyecto, describe el diseño e implementación de un Sistema de Gestión de la Seguridad de la información- SGSI basado en la norma ISO/IEC 27001; además, pretende evidenciar la medida en que la implementación de este sistema, mejorará la seguridad de la información disminuyendo el impacto reputacional y operacional, la probabilidad de ocurrencia de las vulnerabilidades, amenazas y riesgos para Positiva Compañía de Seguros S.A. en la ciudad de Bogotá.

4. OBJETIVOS

4.1 GENERAL

Diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) para la Casa Matriz de Positiva Compañía de Seguros S.A. en la ciudad de Bogotá; basado en la Norma NTC-ISO-IEC 27001:2013

4.2 ESPECÍFICOS

4.2.1 Analizar la situación actual de la Casa Matriz, con relación a la Gestión de Seguridad de la Información.

4.2.2 Realizar un análisis y evaluación del riesgo identificando los recursos a proteger con incidencia directa en la operación de la entidad mediante una metodología de evaluación sistemática.

4.2.3 Determinar y evaluar la aplicabilidad de los controles de seguridad de la información bajo la norma ISO/IEC 27002:2013.

.

4.2.4 Establecer la política, alcance y objetivos del Sistema de Gestión de Seguridad de la Información para la Casa Matriz de Positiva.

5. MARCO REFERENCIAL

5.1 ANTECEDENTES

Con el fin de enfocar la investigación sobre la implementación de un Sistema de Gestión de la Seguridad Información, fueron consultados los siguientes proyectos:

Trabajo de investigación nombrado “Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la ofrenda”, elaborado por Aguirre Cardona Juan David y Aristizabal Betancourt Catalina; expone la importancia de diseñar e implementar un SGSI que le garantice a la entidad en mención mejorar los niveles de seguridad de sus activos de información y posteriormente lograr la certificación correspondiente.

Artículo “Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la Comunidad Nuestra Señora de Gracia, alineado tecnológicamente con la norma ISO 27001”. Es el resultado de un proyecto de investigación, que como fin tenía la implementación un SGSI en la Comunidad en mención. Este sistema se basa en las directrices indicadas en la norma ISO/IEC 27001, y en el marco del mismo se generó un análisis de gap, que permitió evidenciar un nivel de brechas significativo en la Comunidad, con base en el cual se establecieron políticas y controles de mejoramiento de los procesos de seguridad de la información y se definieron las declaraciones de aplicabilidad que fortalecieron todo el análisis de riesgos efectuado.

El proyecto de grado: “Diagnóstico y actualización del Sistema de Gestión de Seguridad de la Información (SGSI) para Ventas y Servicios S.A”, creado por Frank González Sánchez; describe la necesidad puntual de mantener actualizado el SGSI y extender la certificación en este estándar a las demás áreas de la compañía. Este proyecto permitió indagar y adentrase en el manejo y la aplicabilidad de la norma ISO 27001 y 27002, a través de las recomendaciones y buenas prácticas.

5.2 CONTEXTO

Positiva Compañía de Seguros S.A. es una entidad de economía mixta adscrita al Ministerio de Hacienda y Crédito Público; su conformación se dio como resultado de la cesión de activos, pasivos y contratos de la Administradora de Riesgos

Profesionales (ARP) del Seguro Social a la Previsora Vida S.A. Compañía de Seguros.

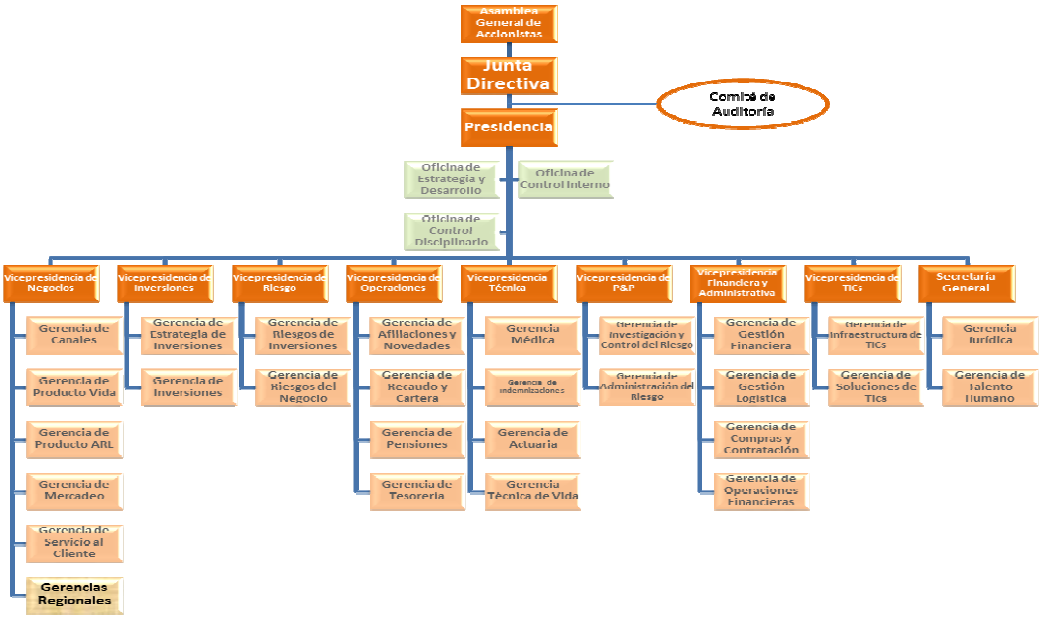
Los servicios ofertados por esta organización, están enmarcados en los ramos de ARL (Administradora de Riesgos Laborales), los ramos de Seguros de vida a saber:

- Accidentes personales
- Vida Grupo y Vida Individual
- Salud
- Exequias

Y los ramos de Seguros pensionales dentro de los cuales se cuenta con:

Rentas vitalicias y conmutación pensional

Ilustración 1 Organigrama



Fuente: Quienes somos-estructura organizacional disponible en: www.positiva.gov.co

5.3 VICEPRESIDENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES TIC´S

La vicepresidencia de TIC´S en Positiva Compañía de Seguros S.A, está conformada por la Gerencia de Infraestructura de TIC´S y la Gerencia de Soluciones TIC´S.

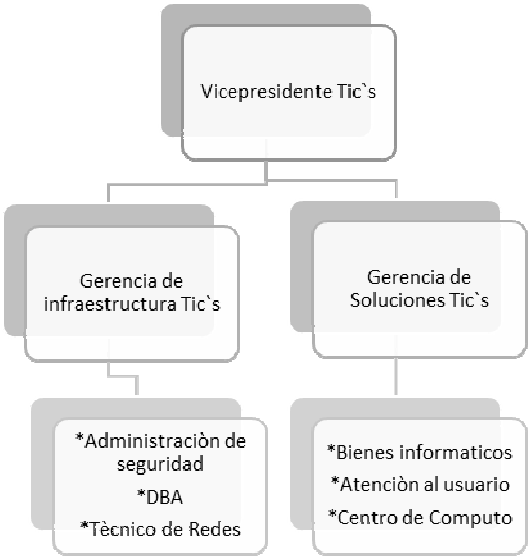
Esta vicepresidencia es responsable de elaborar, desarrollar y proponer la implementación de nuevas tecnologías y sistemas informáticos, planear actividades de mantenimiento preventivo y brindar soporte técnico a toda la compañía.

De acuerdo a la caracterización de cada proceso, la Vicepresidencia de TIC´S, tiene las siguientes funciones[1]:

- Proponer y acompañar los Sistemas de Control Informáticos a ser implementados en las diferentes sucursales y regionales de la compañía.
- Gestionar la capacitación a los responsables operativos con el fin de garantizar la correcta implementación de los Sistemas Informáticos.
- Investigar, desarrollar e implantar tecnologías que soporten la operación de la entidad.
- Coordinar el análisis y desarrollo de los sistemas informáticos en conformidad con el plan estratégico 2015-2018.
- Impulsar el adecuado uso de los recursos informáticos al interior de la organización.
- Participar en los lineamentos generales y específicos para futuras adquisiciones de recursos informáticos.
- Velar y mantener en buen funcionamiento los recursos informáticos de la organización.

[1] POSITIVA COMPAÑÍA DE SEGUROS S.A. Caracterización Proceso Vicepresidencia TIC´S.: La entidad, 2012. 48 p.

Ilustración 2 Organigrama Vicepresidencia de TIC´S



Fuente: El autor

5.3.1 Catálogo de servicios Vicepresidencia TIC´S

El catálogo de servicios TIC´S recopila los servicios que la vicepresidencia presta a cada unidad de negocio de la compañía como soporte al desarrollo de sus actividades[2].

[2] POSITIVA COMPAÑÍA DE SEGUROS S.A. Catálogo de Servicios Informáticos. La entidad, 2012. 5. P.

Ilustración 3 Catálogo de Servicios

Fuente: Catálogo de servicios informáticos-Positiva Compañía de Seguros S.A.

5.3.2 Cargos y Funciones de la Vicepresidencia de TIC`S

Positiva Compañía de Seguros cuenta con dos tipos de funcionarios, aquellos que son trabajadores oficiales (desde el cargo de profesional especializado grado 11 hasta el asistente administrativo grado 2) y aquellos que son servidores públicos (desde el cargo de Vicepresidente hasta el Gerente Regional, sucursal y de área)[3].

El nivel directivo está encabezado por el:

[3] POSITIVA COMPAÑÍA DE SEGUROS. Manual de funciones para Empleados públicos y Trabajadores Oficiales. La entidad. 2011. 1092 p.

- Vicepresidente Grado 8

Tiene como función principal el dirigir la formulación del plan estratégico de tecnologías de la información y comunicaciones de la compañía teniendo en cuenta las necesidades del negocio.

Igualmente debe coordinar el desarrollo de la arquitectura tecnológica de la compañía, de acuerdo a las mejores prácticas de tecnologías de la información y comunicaciones; también, le corresponde dirigir los procesos de investigación, implementación y evaluación de las diferentes tecnologías y servicios de la información, que requiera la compañía y finalmente debe garantizar el cumplimiento de normas, disposiciones, procedimientos y programas propios de la gestión de la vicepresidencia, para garantizar eficiencia y eficacia y oportunidad en las acciones institucionales, de acuerdo con los parámetros definidos.

- Gerente de área Grado 6

Por su parte, debe ser participe en la formulación del plan estratégico de tecnologías de la información y comunicaciones de la Compañía, igualmente es quien define y propone las especificaciones técnicas requeridas para la adquisición y contratación de bienes y servicios tecnológicos; a su vez, debe gestionar el seguimiento a los procesos a cargo de la Gerencia, obedeciendo a las metas e indicadores establecidos y es el encargado de preparar y presentar los informes que sean de su competencia y los requeridos por los entes de control con la oportunidad y periodicidad requerida.

- Profesional Especializado Grado 12 (Líder de proceso):

El líder de proceso es quien propone las estrategias de control y seguimiento para garantizar una adecuada evaluación a la gestión de la vicepresidencia y realiza las recomendaciones pertinentes. También es el encargado de formular proyectos de la Vicepresidencia y gestionar su registro en Casa Matriz, de acuerdo con los lineamientos establecidos, además, debe orientar a todas las dependencias de la compañía sobre los procedimientos y temas relativos a la misma.

- Profesional Universitario grado 5 y 4

Este profesional es quien brinda asistencia profesional a todas las dependencias de la compañía a Nivel Central, Regional y Sucursal sobre los procedimientos y temas relativos de la vicepresidencia de TIC´S.
Apoya la ejecución de planes y programas de acuerdo a las estrategias definidas, realiza estudios e investigaciones requeridas para optimizar los procesos y finalmente evalúa los procesos que se desarrollan en la vicepresidencia para establecer puntos de control, definir estrategias de mejoramiento y garantizar que respondan a los lineamientos establecidos en el SIG de la compañía.

- Técnico Administrativo Grado 3

Este es un cargo que realiza tareas como:

1. Llevar los registros documentales de los procesos de la Vicepresidencia de TIC`S de acuerdo a las políticas institucionales
2. Elaborar, mantener y realizar seguimiento a las bases de datos
3. Recopilar, clasificar y organizar información para la gestión de informes estadísticos
4. Apoyar la ejecución de las actividades para el desarrollo de los proceso de la Vicepresidencia.

- Asistente Administrativo Grado 2

Es el encargado de administrar el archivo y la correspondencia para facilitar la consulta de la documentación requerida, atiende a los usuarios internos y externos de la compañía dando la orientación e información propias de la dependencia; a su vez es quien efectúa las comunicaciones escritas y telefónicas obedeciendo las instrucciones demandas del superior inmediato o profesionales de la vicepresidencia.[4]

[4] POSITIVA COMPAÑÍA DE SEGUROS. Manual de funciones para Empleados públicos y Trabajadores Oficiales. La entidad. 2011. 1093 p

5.4 MARCO TEÓRICO

5.4.1 Seguridad de la información: Comprende todas las medidas preventivas encaminadas a proteger y garantizar la confidencialidad, disponibilidad, integridad y trazabilidad de la información.

Dentro de esta, se tratan los riesgos, las amenazas, el análisis de escenarios, las buenas prácticas de los procesos tecnológicos gestionados en una organización, enfocados a incrementar y mantener el nivel de confianza en lo que compete al tratamiento de la información.[5]

5.4.2 Seguridad Informática: Corresponde a las prácticas ejecutadas para la protección de los sistemas informáticos y los usuarios de estos.

La seguridad informática se logra mediante la implementación de políticas de seguridad, el uso de herramientas para la defensa de la información, como lo son: el antivirus, firewalls, detección de intrusos, detección de anomalías, entre otros, y con la prácticas de gobierno de tecnologías de información, en las que se especifica el cómo actuar y tratar las posibles fallas en el momento en que la información se encuentre en riesgo[6]

5.4.3 Norma ISO/IEC 27001-2013: Es el estándar en el que se registran los requisitos fundamentales y se establece las pautas para el diseño e implementación de un Sistema de Gestión de Seguridad de la Información mediante el uso del ciclo PVHA y las mejores prácticas de seguridad.

La norma contempla 10 dominios de control dentro de los que se cuenta: la Política y organización de la seguridad, clasificación y control de recursos, seguridad del personal, seguridad física y ambiental y control de acceso por mencionar algunos de ellos.

[5] Recuperado de: http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html
[6] Ibid ., p. 5

5.4.4 Norma ISO/IEC 27002: Esta es la guía en cuanto a las buenas prácticas de seguridad de la información. Describe de forma precisa las acciones que han de llevarse a cabo para el establecimiento e implementación de los objetivos de control y controles descritos en el Anexo A de la norma ISO 27001.

5.4.5 Estándar RFC2196: Es uno de los principales estándares para la seguridad de la información que como característica principal propone que la puesta en marcha de este, se logre mediante procedimientos descritos, publicación de guías u otros medios prácticos a consideración de la organización, igualmente propone la inclusión de herramientas de seguridad que garanticen el cumplimiento de las acciones relacionadas, se detecten errores y se asignen responsables para cada posible situación.[7]

Este modelo trata temas como lo son: qué es y porque una la política de Seguridad, arquitectura de red y de servicios, configuración de red y de servicios, firewalls y autenticación dentro de los más relevantes.

5.4.6 Implementación SGSI: De acuerdo a lo planteado en la ISO 27001, la seguridad de la información, reside en la preservación de la confidencialidad, integridad y disponibilidad de los datos así como los sistemas comprometidos en su tratamiento.[8]

5.4.7 Paso para implementar un SGSI: Como se mencionó anteriormente para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información basado en la ISO 27001, se utiliza el ciclo continuo PHVA[9].

Se contemplan las fases descritas a continuación:

- La Fase “Plan” (Planificación). Corresponde al establecimiento de los objetivos de seguridad de la información y selección de los controles adecuados de seguridad.

[7] Díaz, Flor Nancy. Principales Estándares para la Seguridad de la Información IT. Investigación. Madrid-España.: Universidad Pontificia de Salamanca. 2015. 83 p. Recuperado de: http://documents.mx/documents/rfc-2196-principales-estandares-para-la-seguridad-informacion-it.html

[8] INSTITUTO COLOMBIANO DE NORMALIZACIÒN Y CERTIFICACIÒN. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. NTC-ISO-IEC 27001. Bogotá.: El Instituto, 2013. 37 p.

[9] GONZALEZ, Frank. Diagnóstico y Actualización del Sistema de Gestión de Seguridad de la Información (SGSI) para Ventas y Servicios S.A. Trabajo de grado para Ingeniero de Sistemas. Bogotá D.C.: Universidad Católica de Colombia. Programa de Ingeniería de Sistema, 2013. 63 p.

- La Fase “Hacer” (Implementación). Esta etapa es la ejecución de todo lo planificado en la anterior fase. Se indica cómo se debe manejar el sistema en pro de las políticas, controles y procedimientos correspondientes.

- La Fase "Verificar" (Revisión). Es aquí en donde se realiza el monitoreo del SGSI mediante diversos “conductos” y comprobar si los resultados cumplen los objetivos establecidos.

- La Fase "Actuar" mantenimiento y mejora. Corresponde a la realización de todas las acciones de prevención y corrección del SGSI, con el fin de garantizar la mejora continúa del mismo.

Es sustancial resaltar que el PHVA es un ciclo de vida continuo, es decir, que la fase de Actuar nuevamente lleva a la fase de Planificación y así se inicia un nuevo ciclo de cuatro fases.

5.4.8 Desarrollo de las fases de implementación de un SGSI

- Fase de diagnóstico: Aquí se precisa la situación real de la entidad, identificando adecuadamente los activos de información vinculados a los procesos estratégicos, misionales y de apoyo, así como los riesgos asociados a dichos activos.
- Fase de planificación de un SGSI para la organización**:** Para esta etapa se determinan:

Grupos de trabajo

Establecer mesas de trabajo por cada proceso misional y de apoyo involucrando funcionarios que posean conocimiento de la organización, del área y proceso donde trabajan.

Plan de trabajo

Se determina una metodología en la que se identifique claramente las actividades necesarias, el plazo pertinente para efectuar cada actividad, interrelación entre las mismas y finalmente se designa el personal o equipo para que lleve a cabo cada labor.

Asignación de responsabilidades

La especificación de los límites y compromisos permiten un adecuado monitoreo, por tanto es importante precisar que se espera de las personas que se asignen al proyecto.

Para el caso en particular se establece:

Tabla 1 Responsables del proyecto

Nombre Responsable	**Papel y Función**
Ing. Julián Andrés Ardila Navarrete	Ingeniero de Sistemas-Investigador del proyecto
Ing. Laura Victoria González	Vicepresidenta de TIC´S-Monitoreo y evaluación del proyecto
Ing. Salomón García González	Director del proyecto

Fuente: El Autor

- Fase de implementación: Acá debe reflejarse el cumplimiento de los objetivos previamente establecidos. Generalmente en esta fase se realiza un comparativo entre lo obtenido Vs lo planificado y así se establece las brechas existentes.

- Fase de evaluación y Monitoreo: El objetivo es evaluar los resultados obtenidos una vez fue implementado el SGSI. Esta fase contempla tres tareas a saber:

Evaluación de los resultados del SGSI, diseño del programa de seguimiento, transmitir a los funcionarios el resultado de la evaluación y el mejoramiento continuo del SGSI.

5.4.9 Metodología de análisis y evaluación de riesgos: El análisis de riesgos especifica la utilización metodológica de la información disponible, con el fin de identificar peligros y estimar los riesgos[10.]

[10] POVEDA, José. Análisis y valoración de los riesgos-Metodologías. Artículo. Bogotá D.C.: Universidad Católica de Colombia. Programa de Ingeniería de Sistema, 2013. 63 p. Recuperado de: https://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-8.pdf

En el momento en que se considera el diseño de un SGSI, es fundamental ajustarse a las necesidades y los recursos de la organización, es decir, logar un nivel de seguridad aceptable con los medios disponibles. Es aquí, en donde el análisis de riesgos es vital; pues hacerlo permite indagar sobre los peligros a los que se enfrenta la organización y la importancia de cada uno de ellos. Con esta información, se tomarán decisiones fundamentadas acerca de qué medidas de seguridad deben implantarse.

Por lo anterior, un aspecto de gran relevancia a la hora de realizar la implantación de un SGSI es tener en cuenta que la inversión en seguridad tiene que ser proporcional al riesgo.

A continuación, las opciones de acuerdo al enfoque y grado de profundidad para el análisis de riesgos.

- Enfoque de Mínimos:

Como su nombre lo indica se determinan un mínimo de activos y se hace un análisis conjunto, de manera que se emplean una cantidad mínima de recursos, consumiendo poco tiempo y por lo tanto su costo de implementación es bajo.

- Enfoque informal:

Aquí no se requiere de formación especial, ni mucho tiempo y personal como el análisis detallado. Las desventajas de este informe son que al no estar basado en métodos estructurados, se dejen de lado áreas de riesgos o amenazas importantes y el análisis puede ser subjetivo.

- Enfoque detallado:

Es el ideal, pues permite obtener una idea exacta y objetiva de los riesgos a los que se enfrenta la organización. Dentro de este aspecto es posible decidir apropiadamente un nivel de seguridad por cada activo y escoger los controles con precisión, sin embargo, requiere más recursos financieros, personal y tiempo para llevarlo a cabo.

Enfoque combinado:

Este enfoque está centrado en el ahorro de recursos al tratar antes y de manera más exhaustiva los riesgos. De esta forma se consigue un nivel de seguridad razonable en la organización con recursos ajustados.

Metodologías más reconocidas:

5.4.9.1 Octave: Es una metodología desarrollada en EEUU por el SEI, la cual permite considerar los temas organizacionales y técnicos, su interrelación y el uso de la infraestructura tecnológica por parte de las personas

Esta metodología se basa en los aspectos de: riesgo operativo, prácticas de seguridad y tecnología. [11]

5.4.9.2 Magerit 3.0: Esta es una técnica de análisis de riesgos creada por el Ministerio de Administraciones Públicas español, en la que se especifica las tareas apropiadas para un análisis y gestión del riesgo efectivo.[12]

Magerit, cuenta con catálogos detallados de amenazas, vulnerabilidades y salvaguardas; igualmente con una herramienta, denominada PILAR, mediante la cual se gestiona el análisis y la gestión de los riesgos de los sistemas de información.

5.4.9.2.1 Análisis y evaluación del riesgo: El primer paso a seguir en la metodología Magerit, es la realización del inventario de activos de información e identificación y selección de los dominios a evaluar.[13]

- Inventario de activos de información: En este aspecto, es primordial establecer los procesos principales del negocio, pues cada proceso involucra activos de información específicos.[14].

[11] DUQUE, Blanca. Metodologías de Gestión del Riesgo. Auditoria. Universidad de Caldas, facultad de ingeniería. Disponible en: https://auditoriauc20102mivi.wikispaces.com/file/view/Metodolog%C3%ACas+deGesti%C3%B2n+de+Riesgos.pdf
[12] MARTOS, Fernando. Centros Hospitalarios de Alta Resolución de Andalucía-Auxiliares Administrativos. Primer Edición. España.2006. 195 p. Recuperado de: https://books.google.com.co/books?id=SmwP1cZdI4cC&pg=PA195&dq=LA+METODOLOG%C3%8DA+MAGERIT+3.0&hl=es&sa=X&ved=0ahUKEwiK5d7u_KTJAhUJWCYKHadoB14Q6AEIJTAC#v=onepage&q=LA%20METODOLOG%C3%8DA%20MAGERIT%203.0&f=false
[13] Ibid., p. 2

- Identificar y determinar los dominios y procesos para el análisis de vulnerabilidades, amenazas y riesgos existentes.

5.4.9.2.2 Identificación de vulnerabilidades: Esta labor contempla el uso de listas de verificación y herramientas de software que permitan determinar que amenazas pueden materializarse para que representen una vulnerabilidad del sistema informático.

Las posibles vulnerabilidades están asociadas a:

*Seguridad Física: tales como lo son los de*sastres naturales, inundaciones, incendios y control de acceso.

En tanto a la s*eguridad en las conexiones a Internet* se relaciona las políticas en el Firewall, VPN y detección de intrusos.

La *Seguridad en la infraestructura de comunicaciones* contempla los routers, switches, firewall, hubs y RAS.

Por su parte la *Seguridad en Sistema Operacionales (Unix, Windows)* se enfoca en el correo electrónico por ser un medio de alta difusión de código malicioso.

La *Seguridad en las aplicaciones Críticas:* dado que las aplicaciones cuentan con un soporte de sistemas operativos, hardware servidor, redes LAN y el CDP, es la entidad la que determina cuales son críticas para sí misma y por cada una de ellas construye una matriz de riesgo.

5.4.9.2.3 Determinación de las amenazas: mediante la aplicación de la metodología de análisis y gestión de riesgos informáticos se establece cuáles son las probabilidades de ocurrencia de un evento que pueda causar daño sobre los componentes de un sistema.

[14] POSITIVA COMPAÑÍA DE SEGUROS S.A. Informe de Gestión 2014.: La entidad, 2014. 31 p. Recuperado de: https://www.positiva.gov.co/positiva/PlaneacionGestion/Documents/INFORME%20DE%20GESTION%202014.pdf

Tabla 2 Amenazas

De origen natural
Desastres naturales

De origen industrial
Contaminación electromagnética
Avería de origen físico o lógico
Corte del suministro eléctrico
Condiciones inadecuadas de temperatura o humedad
Fallo de servicios de comunicaciones
Interrupción de otros servicios y suministros esenciales
Degradación de los soportes de almacenamiento de la información
Emanaciones electromagnéticas

Errores y fallos no intencionados
Errores de los usuarios
Errores del administrador
Errores de monitorización (log)
Errores de configuración
Deficiencias en la organización
Difusión de software dañino
Errores de [re-]encaminamiento
Errores de secuencia
Escapes de información
Alteración accidental de la información
Destrucción de información
Fugas de información
Vulnerabilidades de los programas (software)
Errores de mantenimiento / actualización de programas (software)
Errores de mantenimiento / actualización de equipos (hardware)
Caída del sistema por agotamiento de recursos
Pérdida de equipos
Indisponibilidad del personal

Ataques intencionados
Manipulación de los registros de actividad (log)
Manipulación de la configuración
Suplantación de la identidad del usuario
Abuso de privilegios de acceso
Uso no previsto
Difusión de software dañino
[Re-]encaminamiento de mensajes
Alteración de secuencia
Acceso no autorizado
Análisis de tráfico
Interceptación de información (escucha)
Modificación deliberada de la información
Destrucción de información
Divulgación de información
Manipulación de programas
Manipulación de los equipos
Denegación de servicio
Robo
Ataque destructivo
Indisponibilidad del personal
Extorsión
Ingeniería social (picaresca)

Fuente: MAGERIT versión 3.0. Metodología de Análisis y Gestión de Riesgos

5.4.9.2.4 Valoración de las amenazas: Esta valoración se basa en dos parámetros, uno es la degradación, que hace referencia a que tan afectado puede resultar un activo y la probabilidad, a la posibilidad de que se materialice la amenaza.

Tabla 3 Medición de la degradación

MA	100%	Muy Alta	Daño muy grave
A	75%	Alta	Daño grave
M	50%	Media	Daño importante
B	25%	Baja	Daño menor
MB	0,1%	Muy Baja	Daño despreciable

Fuente: MAGERIT versión 3.0. Metodología de Análisis y Gestión de Riesgos

Tabla 4 Medición de la probabilidad

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

Fuente: MAGERIT versión 3.0. Metodología de Análisis y Gestión de Riesgos

- Determinación del impacto potencial: una vez materializada la amenaza se calcula el impacto del daño sobre el activo, así:

  Impacto = Valor x Degradación

- Determinación del riesgo potencial: Se evalúa el riesgo en función del impacto y su probabilidad, como lo indica la siguiente formula:

  Riesgo = Impacto x Probabilidad

5.4.9.2.5 Caracterización de las Salvaguardas: Las salvaguardas son elementos de defensa que menguan la probabilidad de materialización de una amenaza y restringen el daño.

5.4.9.2.6 Identificación de las salvaguardas: esto se lleva acabo teniendo en cuenta criterios como: tipo de activo a proteger, dimensiones de seguridad, amenazas de las que se necesita protección y salvaguardas alternas.

Tabla 5 Tipo de salvaguardas

Protecciones generales u horizontales
Protección de los datos / información
Protección de las claves criptográficas
Protección de los servicios
Protección de las aplicaciones (software)
Protección de los equipos (hardware)
Protección de las comunicaciones
Protecciones generales u horizontales

Protección en los puntos de interconexión con otros sistemas
Protección de los soportes de información
Protección de los elementos auxiliares
Seguridad física – Protección de las instalaciones
Salvaguardas relativas al personal
Salvaguardas de tipo organizativo
Continuidad de operaciones
Externalización
Adquisición y desarrollo

Fuente: MAGERIT versión 3.0. Metodología de Análisis y Gestión de Riesgos

Tabla 6 Valoración de salvaguardas

Factor	nivel	significado
0%	L0	inexistente
10%	L1	inicial / ad hoc
50%	L2	reproducible, pero intuitivo
90%	L3	proceso definido
95%	L4	gestionado y medible
100%	L5	optimizado

Fuente: MAGERIT versión 3.0. Metodología de Análisis y Gestión de Riesgos

5.4.9.2.7 Evaluación del riesgo: Mediante un comparativo entre los riesgos estimados Vs los riesgos establecidos se establece el grado de importancia del mismo[15].

La evaluación del riesgo tiene en cuenta, estimado, valoración del riesgo sobre los activos y la probabilidad de ocurrencia.

Estimación del estado de riesgo: acá se toma como referencia los riesgos descubiertos anteriormente, y para ello se tiene:

La *Estimación del impacto,* se calcula el **impacto potencial**, correspondiente a exposición del sistema, es decir, activos Vs amenazas; el **impacto residual**, al igual que el anterior más la eficacia de las salvaguardas desplegadas.

[15] DE FREITAS, Vidalina. Análisis y Evaluación del Riesgo de la información: Caso de Estudio Universidad Simón Bolívar. Articulo como opción de grado de Magister en Ingeniería de Sistemas. Venezuela.: Revista Venezolana de Información, Tecnología y Conocimiento, 2009. 55 p.

Estimación del riesgo: evaluación del riesgo al que están expuestos los activos del sistema: es necesario relacionar el **riesgo potencial**, que refiere el sometimiento del sistema de acuerdo al valor de los activos y las amenazas por su parte el **riesgo residual**, se toman los dos aspectos anteriores más la efectividad de las salvaguardas desarrolladas.

5.4.9.3 Gobierno TI: Procedimiento enfocado a encaminar y controlar el uso actual y próximo de las tecnologías de la información. Dentro de esta táctica, se admite la articulación de la planeación estratégica de una organización con los procesos de TI, recursos de TI e información. Representa las buenas prácticas orientadas al soporte de los objetivos del negocio mediante la información y las tecnologías[16].

El Gobierno de las TI considera tres aspectos importantes en las organizaciones, como lo son:

- Qué decisiones deben tomarse en materia de gestión y el uso de las TI.
- Quienes deben tomar decisiones.
- Y como estas serán realizadas y verificadas.

5.5 MARCO CONCEPTUAL

En este aparte se presentan algunas definiciones importantes relacionadas al SGSI que se busca implementar.

- ***Amenaza:*** Posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño sobre cualquier elemento de un sistema de seguridad.[17].

- ***Autenticidad:*** Corresponde a la originalidad de la información Es la acción que permite certificar la fuente de donde proceden los datos a manipular.

[16] INSTITUTO COLOMBIANO DE NORMALIZACIÒN Y CERTIFICACIÒN. Gobierno Corporativo de la Tecnología de la Información. Norma Técnica NTC-ISO-IEC 38500. Bogotá.: El Instituto, 2009. 10 p. Recuperado de: http://tienda.icontec.org/brief/NTC-ISO-IEC38500.pdf

[17] Recuperado de: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

- ***Confidencialidad:*** Indica que la información que se considera secreta no será divulgada, solo se permitirá el acceso a esta a quienes estén autorizados.[18]

- ***Disponibilidad:*** Asequibilidad de una cosa o persona en el momento en que estos sean requeridos. [19].

- ***Estándares de Seguridad:*** son delineamientos técnicos detallados que garantizan la interrelación de los elementos de un sistema.

- ***Gestión de riesgos:*** Implica todas las acciones fundamentadas y orientadas a garantizar el funcionamiento de un sistema informático; abarcando la seguridad de la información, minimizando el impacto de los riesgos y de las amenazas existentes.

- ***Integridad:*** Estado de un objeto o individuo al poseer todas sus características sin alteración alguna.[20].

- ***Ingeniería social:*** Labor enfocada a logar información de las personas mediante prácticas relacionadas con la comunicación y la aplicación de engaños.

- ***Modelo de Seguridad:*** Es un modelo que abarca pautas procedimentales tenientes a mantener el control dado el uso de los sistemas informáticos.

- ***Políticas de Seguridad:*** Lineamientos que rigen la seguridad de la información.

- ***Riesgo:*** Es la probabilidad de sufrir un daño o pérdida. Se mide en términos de impacto y probabilidad de ocurrencia[21].

[18] ORGANIZACIÓN INTERNACIONAL PARA LA ESTANDARIZACIÓN. Sistema de Gestión de la Seguridad de la Información. ISO/IEC 27001. España.: El instituto, 2013. 14 p.
[19] Ibid., p. 3.
[20] Ibid., p. 3.
[21] AGUIRRE CARDONA, Juan David y ARISTIZABAL BETANCOURT, Catalina: Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la ofrenda. Pereira, 2013, 23 P. Trabajo de grado (Ingenieros de Sistemas). Universidad Tecnológica de Pereira. Facultad de Ingenierías. Programa de Ingeniería de Sistemas y Computación.

- ***Seguridad de la información***: Recopilación de técnicas y medidas preventivas enfocadas en la protección de la información al interior de una organización.

- ***Sistema de Gestión de Seguridad de la Información (SGSI):*** *Sistema que se basa en la administración del riesgo,* realiza, aplica, verifica, valida y mejora la seguridad de la información[22].

- ***Tolerancia a fallos:*** Capacidad de responder a un suceso inesperado.

- **Trazabilidad:** Habilidad del sistema para establecer quién, cómo y cuándo se hizo a fin de detectar posibles incidentes de seguridad de la información

- **Vulnerabilidad:** Debilidad de un bien informático o de un control, que puede ser aprovechada por una amenaza..[23]

5.6 MARCO LEGAL

En el momento en que se contempla la implementación de un SGSI, es importante tener en cuenta la legislación que regula todo lo concerniente a seguridad de la información. En Colombia se tiene:

- Decreto 1360 de 1989, donde se reglamenta el soporte lógico (software) en el registro nacional de derecho de autor, considerando al software como una creación del dominio literario en conformidad a la ley 23 de 1982 sobre derechos de autor[24].

- Ley 527 de 1999, que establece y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y las firmas digitales, además de establecer las entidades de certificación y otras disposiciones[25].

[22] Ibid., p. 2.
[23] PRANDINI, Patricia y PALLERO, Marcela. Vulnerabilidades, amenazas y riesgo en "texto claro". (En línea). http://www.magazcitum.com.mx/?p=2193. (citado en 25 de mayo de 2013).
[24] JARAMILLO, A. Manual de derecho de autor. (en línea). (2 de Septiembre de 2015). Disponible en: http://www.derechodeautor.gov.co/documents/10181/331998/Cartilla+derecho+de+autor+
[25] CUERVO, J. Aspectos Jurídicos de Internet y el comercio electrónico. (en línea). (2 de Septiembre de 2015)Recuperado de :http://www.informatica-juridica.com/trabajos/Aspectos_juridicos_de_Internet_y_el_comercio_electronico.asp

- Decreto 1747 de 2000, que reglamenta parcialmente la ley 527 de 1999, con lo relacionado a las entidades de certificación, los certificados y las firmas digitales[26].

- Resolución 26930 de 2000, la cual fija los estándares para la autorización y el funcionamiento de las entidades de certificación y sus auditores"[27].

- Ley estatutaria 1266 de 2008, que establece las disposiciones generales del habeas data y regula el manejo de la información que se contiene en las bases de datos personales, especialmente la financiera, crediticia, comercial, de servicios y la proveniente de terceros países[28].

- Ley 1273 de 2009, con la que se modifica el código penal, se crea un nuevo bien jurídico denominado "de la protección de la información y los datos", y se preservan integralmente los sistemas que utilicen las tecnologías de información y de comunicación[29].

- Decreto 1377 de 2013, Por el cual se reglamenta la ley 1581 de 2012. El propósito de este decreto es facilitar la ejecución y el acatamiento de la ley 1581, contemplando factores como la autorización y el derecho del titular de la información para el procesamiento de los datos personales[30].

- Ley estatutaria 1581 de 2012, por la cual se fijan disposiciones en materia de protección de datos personales. El objetivo de esta ley es el salvaguardar el derecho constitucional de todo individuo al conocimiento, actualización y corrección de la información registrada en cualquier base de datos[31].

[26] Decreto. Artículo 160 del Decreto ley 19 de 2012. (en línea). (2 de Septiembre de 2015). Disponible en: http://www.sic.gov.co/drupal/

[27] Resolución. Por la cual se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores. (en línea). (2 de Septiembre de 2015). Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=5793

[28] Concepto. Oficina Jurídica Nacional. (en línea). (2 de Septiembre de 2015). Disponible en: http://www.legal.unal.edu.co/sisjurun/normas/Norma1.jsp?i=42011

[29] DELTA. (2014). Ley de delitos informáticos en Colombia. (en línea). (2 de Septiembre de 2015). Disponible en: http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia

[30] Decreto por el cual se reglamenta la ley 1581 de 2012. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646

[31] Ley estatutaria 1581 de 2012. Por la cual se fijan disposiciones en materia de protección de datos personales. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

6. DISEÑO METODOLÓGICO

6.1 LÍNEA Y TIPO DE INVESTIGACIÓN

La metodología de desarrollo del presente proyecto de grado, se basa en los planteamientos definidos en materia de Seguridad de la Información y Diseño e implementación de Sistemas de Gestión de Seguridad de la Información.

Principalmente se busca; realizar un SGSI que brinde seguridad y protección a la información sensible de los grupos de interés de la aseguradora y prevenir la ocurrencia e impacto de amenazas y riesgos.

6.2 TIPO DE INVESTIGACIÓN

6.2.1 Investigación Exploratoria: A través de la entrevista y observación se pretende levantar datos que permitan el diagnóstico inicial sobre el tratamiento de la información manejada por la aseguradora y los mecanismos de control y seguridad al interior de la misma. Relacionado con lo anterior, es importante conocer los procedimientos actuales y el plan estratégico establecido por la compañía para el periodo 2015-2018.

6.2.2 Investigación Descriptiva: Este tipo de investigación permite la delimitación de los hechos que conforman el problema de investigación, como lo son:

- Establecer características propias de Casa Matriz como unidad de investigación (número de equipos de cómputo, aplicaciones utilizadas, número de usuarios, etc.).

- Identificar conductas, actitudes de las personas que se encuentran en el universo de investigación (comportamientos sociales, preferencias, etc.)

- Descubrir y comprobar la posible asociación de las variables de investigación.

6.3 AREA DE INVESTIGACIÓN

La presente propuesta se enmarca dentro del área de conocimiento: Gestión de la Seguridad Informática, específicamente en, Sistema de Gestión de Seguridad de la Información "SGSI" basado en el estándar ISO/IEC 27001:2013 y gestión del riesgo informático.
La gestión del riesgo: contempla el análisis, valoración y clasificación del riesgo con el fin de hallar los controles apropiados para contrarrestarlos[32].

Este método sigue cuatro pasos, como lo son:

- Análisis: Mediante esta acción es posible establecer que partes del sistema necesitan protección, además, identificar cuáles son las vulnerabilidades y amenazas y reconocer el grado de riesgo al que se enfrentan.
- Clasificación: Se categoriza el riesgo y el nivel de aceptación.
- Reducción y control: corresponde a labores de sensibilización del usuario y al análisis de la efectividad de las medidas seleccionadas[33]

6.4 TECNICAS E INSTRUMENTOS DE RECOLECCION DE INFORMACIÓN

Para este proyecto puntualmente, se hará uso de todas las fuentes bibliográficas posibles relacionadas con el Diseño e Implementación de un SGSI basado en el estándar NTC 27001:2013, esto con el fin de establecer antecedentes que sustenten la investigación.

Las técnicas de recolección de datos elegidas para el desarrollo de esta investigación son: La observación, encuesta y entrevista.

6.4.1 Observación: Esta técnica permite entrar en contacto directo con los profesionales de informática y una investigación continúa de los procedimientos reales sucedidos en el sistema.

6.4.2 Entrevista Estructurada: Mediante preguntas precisas es posible socializar la temática de investigación y conocer el punto de vista de las diferentes partes involucradas, además, permite registrar de forma estandarizada

[32] AGUILERA, Purificación. Seguridad Informática: Ciclos Formativos. México: Editex, 2010, p.9.
[33] SEGUNDA COHORTE DEL DOCTORADO EN SEGURIDAD ESTRATÉGICA. Seguridad de la Información. En: Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica, 2014, No. 1, p 15-16

datos sobre seguridad informática y procedimientos ejecutados por la organización.

6.4.3 Encuesta: Debido a su estructura con preguntas de múltiples opciones referentes a la seguridad informática es posible conocer la posición de las personas involucradas frente a la problemática y también saber el grado de conocimiento de las mismas respecto a la temática tratada en esta investigación.

Los instrumentos seleccionados para este proyecto son: Lista de cotejo, cuestionario y guía de entrevista.

6.5 POBLACIÓN Y MUESTRA

6.5.1 Población: El presente proyecto implicara la Casa Matriz ubicada en la ciudad de Bogotá de Positiva Compañía de Seguros, pues es aquí en donde se toman las decisiones y se realizan todas las actividades administrativas para el funcionamiento de la entidad.

6.5.2 Muestra: Se estima que para el estudio en referencia, se involucrara cerca de 345 personas dentro de las cuales 35 son profesionales del área de informática e infraestructura y 310 son funcionarios que actúan como usuarios de los sistemas informáticos (bases de datos, equipos de cómputo, red local). Además de estos, los procedimientos y procesos operativos y administrativos de la organización se tendrán en cuenta.

6.6 METODOLOGÍA DE DESARROLLO

Con el fin de desarrollar satisfactoriamente la presente propuesta se ha contemplado cuatro fases vitales las cuales a su vez, permitirán el diseño de un SGSI basado en la norma ISO/IEC 27001-2013 para Positiva Compañía de Seguros S.A, a saber.

6.6.1 Fase 1: Diagnostico de la situación actual en materia de seguridad informática en Casa Matriz

Se considera necesario realizar un reconocimiento sobre las disposiciones establecidas al interior de la compañía en materia de Seguridad de la información, para ello se propone:

- Realizar una consulta de documentación existente (misión, visión, objetivos organizacionales, planeación estratégica, políticas, procesos, procedimientos, instructivos, manuales, normatividad entre otros).
- Entrevistas a los líderes de proceso misionales y de apoyo para establecer la existencia de una política y procedimientos de seguridad.
- Observación del manejo de la información sensible de la compañía.

6.6.2 Fase 2: Identificar los activos informáticos, definir y aplicar de la metodología de análisis y gestión del riesgo.

De acuerdo a lo enunciado, lo primordial es realizar un inventario de activos de información para la organización bajo estudio, esto permitirá, seleccionar los dominios descritos en la norma ISO/IEC 27001-2013 y así aplicarlos en la evaluación de riesgos, con el propósito de minimizarlos. , por tanto se proponen las siguientes actividades:

- Visita de reconocimiento a Casa Matriz con el fin de identificar y determinar el tipo de activos informáticos, estos serán listados en la plantilla “Relación de activos de seguridad de la información”
- Definición y aplicación de la metodología para el análisis y gestión de riesgos informáticos

6.6.3 Fase 3: Determinar y evaluar la aplicabilidad de los controles de seguridad de la información bajo la norma ISO/IEC 27002:2013

Una vez realizado el análisis de las amenazas, vulnerabilidades y riesgos a los que están expuestos los activos se procede a:

- Verificar mediante un análisis comparativo el nivel de cumplimiento de los requerimientos del estándar ISO/IEC 27002:2013 con el objetivo de

reconocer las deficiencias presentadas por la Casa Matriz de Positiva y determinar los controles aplicables.

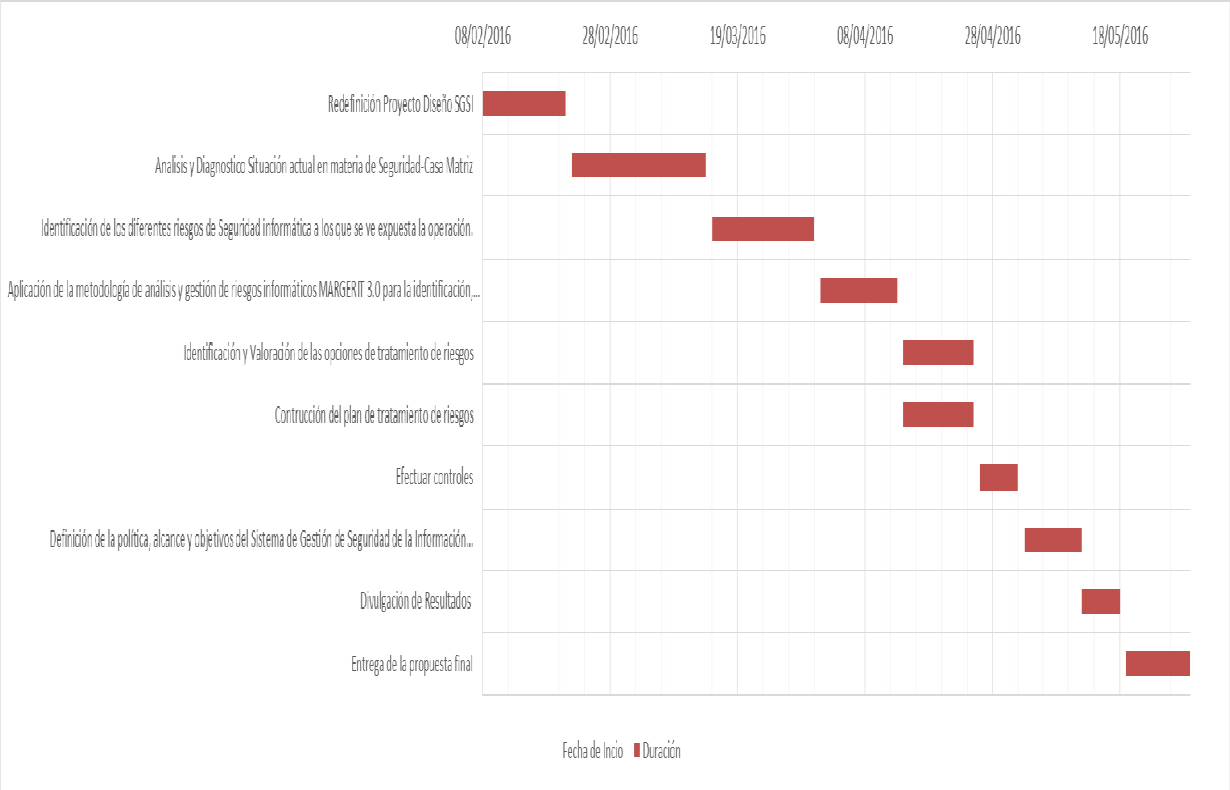
6.6.4 Fase 4: Definición de la política, alcance y objetivos del Sistema de Gestión de Seguridad de la Información para la Casa Matriz de Positiva.

Conforme a los resultados obtenidos en el análisis de riesgos mediante la aplicación de la metodología MAGERIT 3.0 y las necesidades de seguridad dilucidadas del mismo para la organización se procede a:

- Realizar una reunión informativa con los directivos de la entidad para comunicar del proceso de ejecución del proyecto y emitir un presupuesto a medida.
- Definición del equipo de trabajo para la ejecución formal del proyecto, asignación de las responsabilidades a tal efecto y los objetivos de cada etapa.
- Ejecutar un profundo análisis diferencial de seguridad, comparando la situación actual de la empresa con los requisitos de ISO/IEC 27001-2013
- Documentar y gestionar los formatos soporte a la organización. Se trabaja en la elaboración de la documentación para el sistema de Gestión de Seguridad de la Información, así como los formatos en los que se dejaran registro de las prácticas en él incluidas.
- Implementación de las metodologías creadas, preservando el cumplimiento de la misma.

7. CRONOGRAMA DE ACTIVIDADES

Ilustración 4 Cronograma de actividades para el desarrollo del proyecto



Fuente: El autor

8. ANALISIS SITUACIÓN ACTUAL DE LA CASA MATRIZ CON RELACIÓN A LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

8.1 Fase 1. Diagnóstico y análisis situación actual en relación a la seguridad informática en Casa Matriz-Positiva Compañía de Seguros

Por su naturaleza las aseguradoras pertenecen a un sector que maneja una compleja cantidad de información técnica, financiera y de gestión de negocios, muy codiciada y que la hace atractiva para los "ladrones" de identidad e información.

La situación actual en la organización en materia de seguridad informática está asociada básicamente a que:

- No hay una cultura en la protección y uso de la información y los riesgos que esto pueda desencadenar.
- La información no cuenta con una clasificación de acuerdo a su valor, periodicidad o utilidad; razón por la cual no hay definida una responsabilidad en las personas que la generan, puesto que participa más de un individuo en el proceso.
- Positiva Compañía de Seguros, específicamente su Casa Matriz no cuenta con un inventario de los activos de información que detalle de manera precisa el tipo de datos y el uso que se le da.
- El acceso y tratamiento de la información no está delimitada de acuerdo al cargo o función del colaborador.
- Se percibe que no hay un monitoreo de acceso a los equipos e información.
- No hay establecidos procedimientos para prevenir o actuar ante la materialización de alguna amenaza o vulnerabilidad.

8.1.1 Consulta de documentación existente (misión, visión, objetivos organizacionales, planeación estratégica, políticas, procesos, procedimientos, instructivos, manuales, normatividad entre otros).

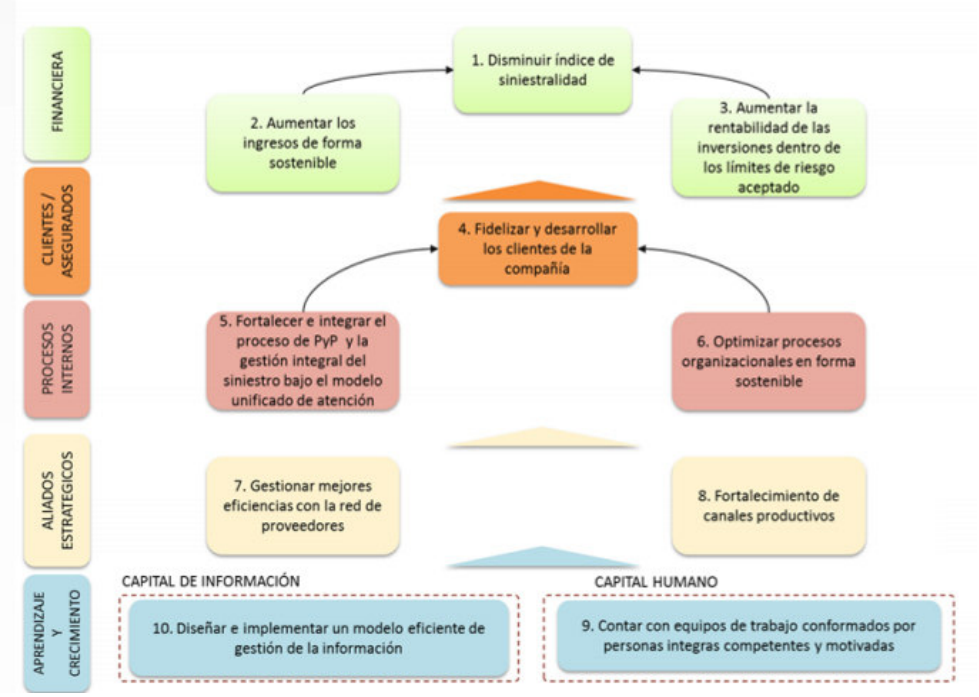
Se realiza la consulta de documentación existente mediante el acceso a la intranet de la organización se encontraron algunos ajustes sobre la misión, visión y la planeación estratégica a seguir durante el año 2015-2018, esto debido a las necesidades mismas del negocio.

Misión: "Protegemos integralmente a las personas y sus familias con un equipo humano competente y comprometido, ofreciendo soluciones de aseguramiento y prevención para general valor a la sociedad"[34]

Visión: "Ser la compañía líder en seguros de personas, reconocida por la calidad de sus servicios"[35]

Objetivos estratégicos: Para hacer posible la visión establecida por la compañía, se definieron objetivos enmarcados en cinco perspectivas medibles a través de indicadores que permiten el seguimiento[36].

Ilustración 5 Objetivos Estratégicos 2015-2018



Fuente: Positiva Compañía de Seguros S.A.-Oficina de Estrategia y Desarrollo

La compañía cuenta con un Sistema Integrado de Gestión muy bien estructurado, documentado y avalado por el ICONTEC en el año 2015. Dicho sistema está conformado por los siguientes sistemas a saber:

[34] Positiva Compañía de Seguros S.A. Quienes Somos. Disponible en: https://www.positiva.gov.co/positiva/Compania/Paginas/default.aspx
[35] Ibid.
[36] Ibid.

- Sistema Gestión de calidad-Modelo Estándar de Control Interno
- Sistema de Gestión Ambiental
- Sistema de Gestión de Seguridad, Salud Ocupacional y Ambiental-RUC
- Sistema de Gestión de Continuidad del Negocio
- Sistema de Gestión de Seguridad y Salud Ocupacional
- Sistema de Gestión y Seguridad de la información

Ilustración 6 Sistema integral de Gestión de Calidad

Fuente: Positiva Compañía de seguros. Sistema integrado de Gestión

El Manual “Sistemas Integrales de Gestión” describe las directrices en materia del SIG de Positiva Compañía de Seguros S.A. y hace referencia a los documentos, que permiten gestionar la calidad de los servicios ofrecidos, la seguridad y salud ocupacional del talento humano, la continuidad del negocio y la preservación del medio ambiente, proporcionando la estructura básica para evaluar la estrategia, la gestión y los propios mecanismos de evaluación.

Este manual se encuentra a disposición de todos los funcionarios, como guía fundamental para la descripción de los Sistemas Integrales de Gestión SIG de Positiva.

Por su parte, el Sistema de Gestión de Seguridad de la información, esta contemplado como parte del SIG de la entidada, sin embargo, tan solo se observa un compromiso muy general de garantizar la confidencialidad, integridad y disponibilidad de la información de los grupos de interes de la misma, pero no hay claridad en como lograra dicho compromiso. Dicho lo anteior se precisa que Positiva y en especifico su Casa Matriz no cuenta con un SGSI estruturado, documentado y mucho menos se han definido politicas en materia de seguridad informática.

Ilustración 7 Compromiso de Seguridad Informática

Fuente: Sistema de Gestión de seguridad de la Información: Disponible en: www.positiva.gov.co/

8.1.1.1 Análisis-Seguridad de instalaciones físicas

El edificio cuenta con sistema de vigilancia de circuito cerrado de televisión, compuesto por un puesto de mando unificado en el que se monitorean las cámaras de vigilancia instaladas así:

- ✓ Cámaras de vigilancia para seguridad de parqueaderos.
- ✓ Cámaras de vigilancia para áreas restringidas (Presidencia, Vicepresidencia de Inversiones, Oficina de control interno y Gerencia de operaciones financieras)
- ✓ Cámaras de vigilancia del perímetro.

El acceso a Casa Matriz está controlado por:

- ✓ Personal de Vigilancia: La entidad cuenta con 6 personas distribuidas así: dos en la recepción, dos vigilantes en las entradas de los parqueaderos y dos vigilantes que realizan recorrido por las instalaciones cada hora.
- ✓ Recepción con atención 24 horas del día. El ingreso los fines de semana debe ser autorizado por la administración del edificio, los colaboradores deben portar su carnet que los acredita como funcionarios de la entidad.
- ✓ Sistema Biométrico para la identificación del personal
- ✓ Tarjeta de proximidad para el ingreso a las áreas restringidas
- ✓ Software de control y registro de visitantes

Ilustración 8 Cámaras de Seguridad

Fuente: El autor

8.1.1.2 Análisis-Seguridad de los activos informáticos

- Seguridad institucional

A pesar de que en Positiva Compañía de Seguros S.A.-Casa Matriz no se cuenta con un SGSI estructurado que establezca políticas de seguridad y evidencie documentación requerida para formalizar el mismo; si se considera y exige en la actualidad a todos los funcionarios nuevos la siguiente directriz:

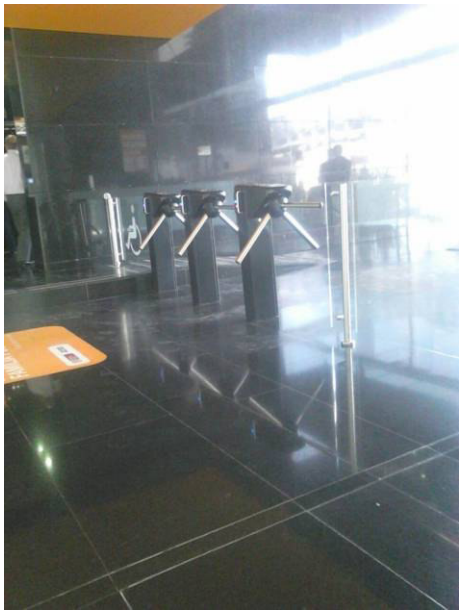
Política: "Toda aquella persona que ingresa como usuario nuevo, (funcionario) a Positiva Compañía de Seguros a manejar equipos de cómputo y hacer uso de los servicios informáticos para el desarrollo de su función, debe acogerse a las condiciones de confidencialidad, uso adecuado de los bienes informáticos y de la información así como leer y acatar lo dispuesto en la CARTA DE COMPROMISO DE LICENCIAMIENTO, USO DE SOFTWARE Y CUMPLIMIENTO DE POLÍTICAS INFORMÁTICAS".

Es de aclarar que esta directriz también está siendo socializada a los antiguos colaboradores y se les solicita firmar la carta de compromiso.

Igualmente, los nuevos ingresos, retiros o cambios de personal (traslados y ascensos), son notificados a la Gerencia de Infraestructura para que esta a su vez asigne los equipos de cómputo, de alta en la base de datos de empleados, cree la cuenta de correo electrónico, determine el perfil para las aplicaciones, brinde el

acceso al file server e intranet de la entidad y por supuesto capacitación sobre el buen manejo de los activos informáticos. En caso de retiro o cambio de personal este realiza las modificaciones pertinentes y retira todos los permisos de acceso.

Ilustración 9 Sistema biométrico de autenticación



Fuente: El autor

- Seguridad en áreas de trabajo

En este aspecto, Casa Matriz cuenta con unos lineamientos básicos de seguridad, una guía de seguridad para usuarios locales y el modelo de seguridad para estaciones de trabajo Microsoft Windows definidos por la Gerencia de Infraestructura TIC´S. (Anexo)

El estándar o plantilla de seguridad recomendada por dicha Gerencia, es aplicada de forma automática a partir de la conexión del equipo al dominio, adquiriendo los atributos y/o permisos configurados previamente.

Además de lo anterior, se contemplan algunas políticas para las áreas de trabajo y usuarios del dominio, así:

- ✓ Límites de seguridad del Dominio.
- ✓ Sincronización de hora; NTP.
- ✓ Parametrización de uso de contraseñas.
- ✓ Bloqueo de cuentas de usuario.

- ✓ Configuración de tiempo de sesión.
- ✓ Políticas de Logs de Auditoria.
- ✓ Opciones de registro de eventos.
- ✓ Servicios de red.
- ✓ Prohibición de conexiones anónimas.
- ✓ Autorización para instalaciones.
- ✓ Estructuración de derechos de usuario.
- ✓ Inicio de sesión.
- ✓ Comunicación segura entre cliente – servidor.
- ✓ No se permite enumeración de cuentas de usuario.
- ✓ Acceso a dispositivos como USB.

Ilustración 10 Control de acceso al CPD

Fuente: El autor

Por su parte, el Centro de datos en Casa Matriz cuenta con controles de tipo preventivo, de monitoreo, reactivos y proactivos.

De acuerdo al documento *ESTÁNDAR DE SEGURIDAD EN EL CENTRO DE DATOS VA-OD-ESCD-01.*

La organización tiene definidas pautas de:

Seguridad preventiva

Gestión de activos**:** Aquellos activos de tecnología de la información existentes en el centro de datos tienen asignado un responsable e incluidos en el inventariado general de activos de la organización.

Gestión de incidencias: registrar todos los eventos relacionados con incidentes que se presenten teniendo en cuenta los siguientes datos:

- ✓ Fecha y hora del incidente
- ✓ Tipo de incidente: Ambiental, humo, fuego, agua y eléctrico
- ✓ Infraestructura: fallo eléctrico, líneas caídas, ,accesos y salidas, intrusos, robos, fallo de requisitos para salida de activos
- ✓ Persona que detecta y comunica el incidente.
- ✓ Identificación de posibles activos afectados
- ✓ Tipo de tratamiento
- ✓ Resolución o escalamiento

Seguridad ante intrusos, sabotaje y accidentes

Previa categorización de espacios informáticos, están determinadas las siguientes medidas:

- ✓ Las puertas y ventanas de salas de categoría A, B o C permanecerán cerradas cuando no estén en uso.
- ✓ El cableado de comunicaciones esta realizado con fibra óptica para evitar daños o accesos no autorizados.
- ✓ Los armarios de equipamiento y paneles racks de cableado y servidores disponen de puerta con cerradura

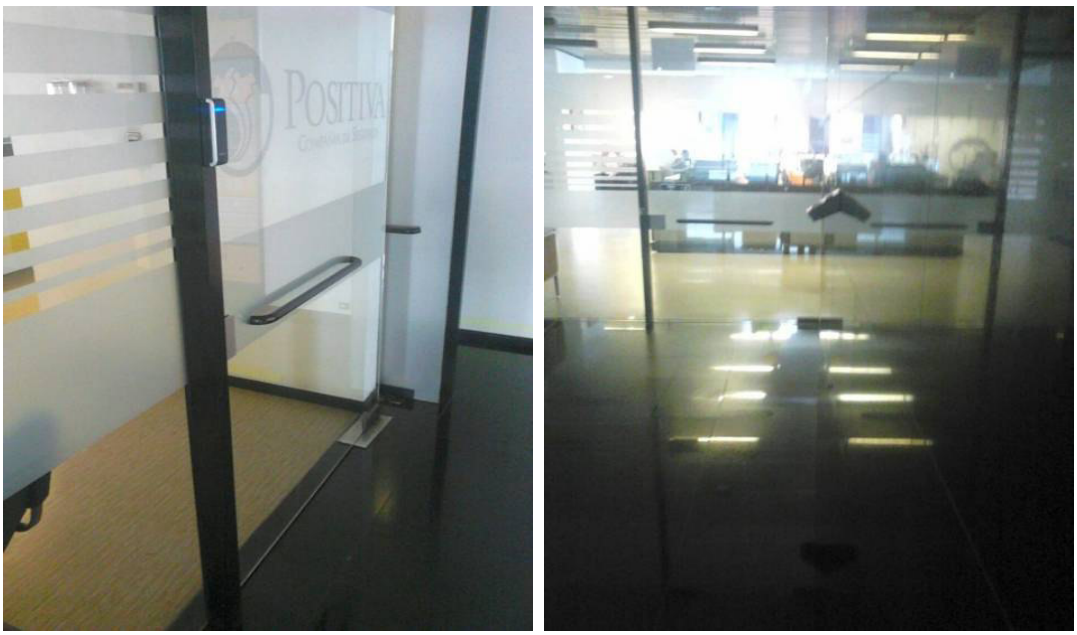
Acceso a personas

El centro de datos tiene acceso restringido, por tanto solo el personal identificado y autorizado puede tener acceso, siendo la Gerencia de infraestructura la única facultada para autorizar el acceso al mismo, dado previo requerimiento o solicitud de acceso por parte de otras áreas interesadas ó terceros.

Las vías de entrada al centro de datos están controladas por cámaras de vigilancia, lectores de tarjeta y detectores biométricos.

Tanto los ingresos como las salidas son registrados con fecha, hora, persona que accede o sale, autorización y motivo.

Ilustración 11 Sistema de tarjeta de proximidad



Fuente: El autor

Entrada o salidas de equipos

Aquellos equipos que entren o salgan del centro de datos deben estar autorizados por la Gerencia de Soporte TIC´S y se registrará la salida del equipo en el formato para retiro o traslado de equipos informando (clase, marca, modelo, número de serie, placa de inventario), datos del remitente y destinatario, y motivo (ingreso o retiro del equipo, reparación, equipos de demostración o prueba, equipos de diagnóstico, etc.).

Seguridad activa

Esta contempla medidas con el objetivo de detectar la ocurrencia de incidentes, como lo son:

- ✓ Detectores de presencia
- ✓ Sistemas de video vigilancia
- ✓ Acompañamiento de visitas

Seguridad reactiva

Considera controles que minimicen el impacto una vez producido un incidente.

- ✓ Una vez se detecte una alarma se generan automáticamente copias de seguridad de los registros de acceso a las zonas afectadas para su análisis.
- ✓ Materializado algún incidente dentro del centro de datos que afecte las operaciones normales de Casa Matriz inmediatamente se ponen en marcha los planes de continuidad de negocio y planes ante recuperación de desastres pertinentes.

Seguridad proactiva

Incluye medidas que permitan anticiparse a los incidentes.

- ✓ Revisión y mantenimiento

Esta determinado que es necesario comprobar periódicamente el funcionamiento de todos los detectores de acceso y alarmas.

Revisar, actualizar y revocar periódicamente el listado de tarjetas de acceso y permisos.

Inspeccionar el sistema de cableado para divisar la presencia de equipos no autorizados conectados a los mismos.

- Protección y ubicación de los equipos de computo

En este aspecto, ningún funcionario puede mover o reubicar un computador o equipo de comunicación, instalar o desinstalar dispositivos. De requerirse, el colaborador debe hacer la solicitud mediante Aranda a través del módulo gestión de infraestructura o soluciones tecnológicas según sea el caso.

- ✓ Los computadores son situados en áreas de trabajo donde el acceso es mínimo.
- ✓ Monitoreo continuo de las condiciones ambientales
- ✓ Se supervisa las instalaciones de procesamiento y almacenamiento de información para evitar acceso no autorizado.

- ✓ Está prohibido comer, beber y fumar en áreas de equipos de procesamiento de información, así como de las estaciones de trabajo.
- ✓ Los portátiles deben usar guayas o candados de seguridad anclados a escritorios o guardados bajo llave cuando no se estén usando.

Seguridad de los equipos de soporte energético

- ✓ Se hace uso de suministro de energía sin interrupción (UPS) para garantizar el funcionamiento continuo de los equipos que soportan operaciones críticas para Casa Matriz.
- ✓ Revisiones periódicas a los equipos UPS
- ✓ Uso de generadores o plantas eléctricas en caso de una falla de energía prolongada.
- ✓ Inspección al sistema de instalación eléctrica, cajas de conexión y paneles de distribución de electricidad.

Seguridad del cableado

La compañía considero las siguientes protecciones para los sistemas críticos o sensibles:

- ✓ Instalación de conductos blindados, habitaciones o cajas bloqueadas en los puntos de inspección y terminación.
- ✓ Uso de cubiertas (blindaje) electromagnéticas para proteger los cables.
- ✓ Acceso controlado a los módulos de cableado (patch panel) y a cuartos de cableado

- Mantenimiento de equipos

Positiva a través de su Vicepresidencia de TIC´S cuenta con una firma externa llamada COMSISTELCO autorizada únicamente para gestionar el mantenimiento, servicio y reparación de equipos informáticos.

Es responsabilidad del colaborador registrar, evidenciar el mantenimiento y soporte realizado a los equipos y respaldar la información contenida en el mismo a través de la copia de seguridad garantizando que los datos vitales no serán tratados por el técnico de COMSISTELCO.

- Uso de dispositivos extraíbles.

Los funcionarios solo están autorizados para realizar copias de seguridad-Backups a través del file server, es decir, cada área tiene una carpeta asignada para depositar en ella la información vital; dicha carpeta cuenta con un monitoreo a fin de evitar que la información contenida allí sea eliminada, dañada, manipulada o sustraída.

Sin embargo, se ha encontrado que debido a las fallas del servicio de file server, los usuarios han decidido hacer uso de USB, discos portátiles, cd o dvd externos para realizar las copias de seguridad. Dichos dispositivos extraíbles no están restringidos o regulados por una política de seguridad, lo que expone a la compañía a una fuga de información intencional o no intencional.

- Seguridad en los sistemas de información

Los sistemas de información de Positiva Compañía de Seguros- Casa Matriz, son aquellos sistemas operativos, de infraestructura, aplicaciones de negocio y servicios de aplicación protegidos mediante la introducción de seguridad en todo el ciclo de vida del desarrollo, es decir que son definidos los controles en cada uno de los entornos y tecnologías empleadas. Antes del paso a producción, se desarrollan pruebas de seguridad de aplicación.

Se contemplan los siguientes controles

Validación de los datos de entrada

Existen controles establecidos durante la etapa de diseño y desarrollo de sistemas o aplicaciones con el propósito de garantizar la validez de los datos ingresados, tanto en la capa de presentación (usuario) como en la capa de negocio, estos controles son:

- ✓ Control de secuencia de ejecución
- ✓ Control del rango de valores posibles y de validez, de acuerdo a criterios predeterminados.
- ✓ Control de paridad
- ✓ Control contra valores cargados en las tablas de datos.
- ✓ Controles por oposición, de forma tal que quien ingrese un dato no pueda autorizarlo y viceversa.

Validación datos de salida

Se encuentran implantados controles como lo son:

- ✓ Confirmación de coherencia para comprobar si los datos de salida son válidos.
- ✓ Control de conformidad de cuentas para asegurar el procesamiento de todos los datos.

- ✓ Prohibición del suministro de información no necesaria.

Los cuales permiten verificar la salida de los datos de las aplicaciones o sistemas de Positiva Compañía de Seguros S.A.

- Protección de los datos de producción

La Vicepresidencia de TIC´S en Casa Matriz ha establecido que el uso de la base de datos operativa (de producción) está prohibido para la realización de pruebas de los sistemas o aplicaciones.

Las pruebas de los sistemas se efectuarán en el ambiente de preproducción el cual es alimentado con la información contenida en las bases de datos de la entidad, esto con una fecha específica de corte, es decir, que la información utilizada en este ambiente corresponde a dos meses atrás de la información real que es manejada en producción. Estos datos serán cambiados conservando la estructura para proteger la confidencialidad de la información (enmascaramiento de datos).

Con el fin de proteger los datos de prueba se estableció en la compañía el siguiente procedimiento:

- ✓ Despersonalización de los datos antes de ser utilizados.
- ✓ Aplicación de procedimientos de control de acceso similares al ambiente de producción.
- ✓ Autorización formal para realizar copias de la base de datos operativa como base de datos de prueba, relacionando dicha autorización en el formato control de bases de datos.
- ✓ Depuración inmediata de la información operativa usada una vez se hayan completado las pruebas.

- Control de Cambios a datos de producción

Toda modificación, actualización o eliminación de los datos operativos que se originen serán realizadas mediante los sistemas que procesan dichos datos y previa autorización del dueño de la información.

- Seguridad en las comunicaciones y red

De acuerdo a la interacción entre ambientes virtuales o físicos de las aplicaciones/componentes, estos son cifrados según la sensibilidad de la información transmitida.

En tanto a la red, está configurada de acuerdo a los requerimientos y necesidades de la entidad, esta es monitoreada para garantizar su disponibilidad, rendimiento y la gestión de incidentes oportunamente.

A continuación se describen los requisitos de seguridad:

- ✓ Las sesiones inactivas se cierran después de un periodo determinado de inactividad en los servidores.
- ✓ La red de Positiva Compañía de Seguros S.A. esta segmentada y protegida con dispositivos adicionales.
- ✓ Disposición de un entorno de Desarrollo, Pruebas y Producción en la Arquitectura de red.
- ✓ Los sistemas de información que provean servicios a los usuarios están ubicados en redes específicas de servidores, separadas de las redes de usuarios.
- ✓ Los sistemas y dispositivos de comunicaciones conectados a la red están correctamente bastionados.

8.1.1.3 Resultados de las entrevistas a los líderes de proceso misionales y de apoyo para establecer la existencia de una política y procedimientos de seguridad.

Una vez socializado el fin de esta entrevista a los líderes de proceso, se procedió a su aplicación y tabulación de los resultados obteniendo lo siguiente:

Tabulación-Seguridad en General

- ✓ ¿De cuántos ordenadores dispone su área?

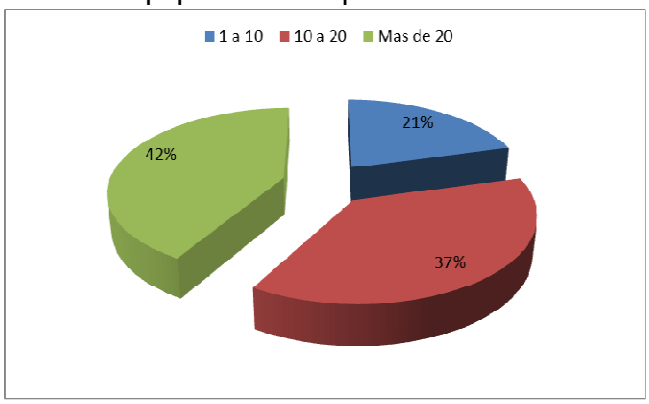
1-10 10-20 +20

Tabla 7 Tabulación respuestas pregunta No.1

Valor ponderado	Frecuencia	Porcentaje %
1 a 10	5	20,83%
10 a 20	9	37,50%
Mas de 20	10	41,67%
Total	24	100,00%

Fuente: El autor

Ilustración 12 Cantidad de equipos de computo



Fuente: El autor

Dado que las áreas no tienen el mismo número de colaboradores se aprecia que la mayor parte de los procesos cuenta con más de 20 computadores representando el 41.67% y la dependencia que posee menos equipos entre 1 a 10 corresponde al 20.83%.

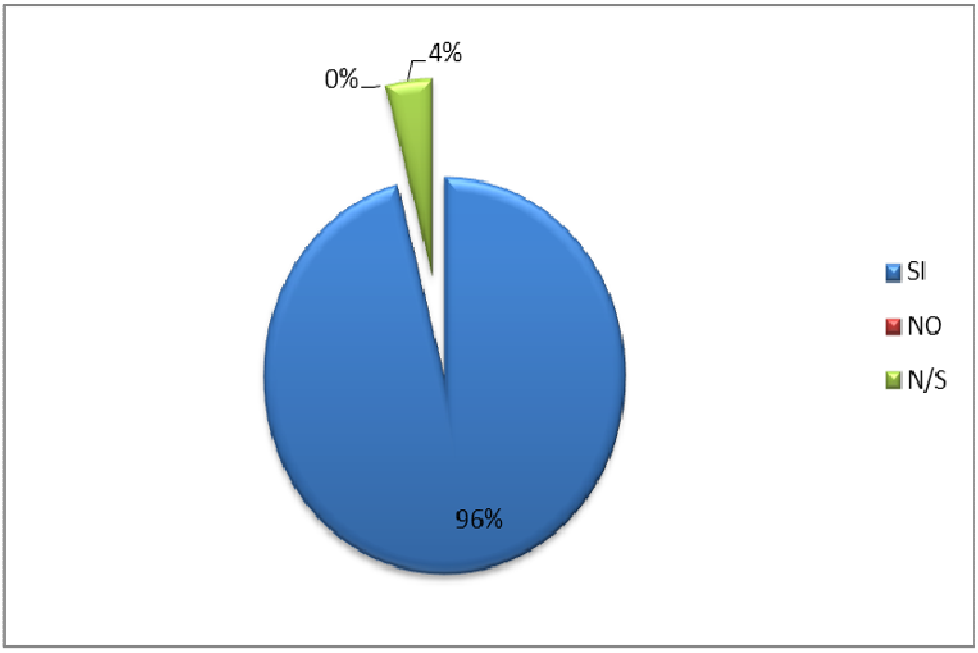
- ✓ Los equipos de cómputo de su área, ¿tienen instalado antivirus?
- ✓ El antivirus que tienen instalado (si es el caso), ¿está actualizado con las últimas definiciones?

Tabla 8 Tabulación respuestas pregunta No. 2

Valor ponderado	Frecuencia	Porcentaje %
SI	23	96%
NO	0	0
N/S	1	4%
Total	24	100%

Fuente: El autor

Ilustración 13 Existencia de Antivirus



Fuente: El autor

Una vez formulada las dos preguntas enunciadas anteriormente a los entrevistados, se evidencia que el 96% respondieron afirmativamente y conocen que todos los equipos del área a la cual pertenecen tiene instalado un antivirus como medida de protección contra algún virus que pueda afectar el normal funcionamiento del equipo y que este a su vez es actualizado de acuerdo a los ultimas definiciones.

Tan solo una persona correspondiente al 4% indico no saber si todos los equipos del proceso al cual pertenece tenían instalado un antivirus y si este era actualizado de acuerdo a los requerimientos establecidos.

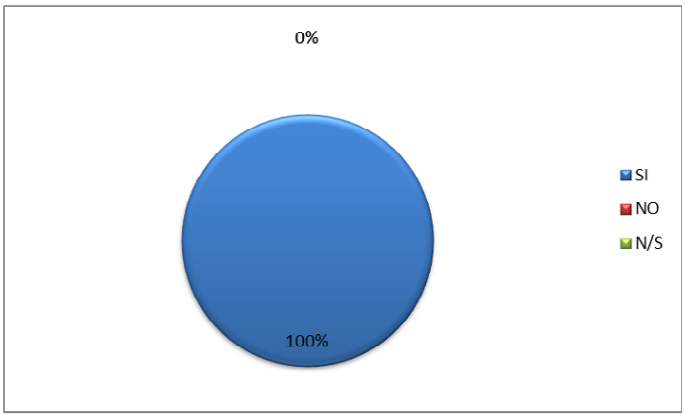
- ✓ ¿Se realiza un mantenimiento informático periódico sobre los ordenadores de la empresa?

Tabla 9 Tabulación respuestas pregunta No. 3

Valor ponderado	Frecuencia	Porcentaje %
SI	24	100%
NO	0	0
N/S	0	0%
Total	24	100%

Fuente: El autor

Ilustración 14 Mantenimiento preventivo



Fuente: El autor

El 100% de la población entrevistada afirmo que en Casa Matriz se realiza cada 6 meses el mantenimiento preventivo a los equipos de cómputo, esto de acuerdo a un cronograma previamente definido y aceptado por los directivos. Dicho mantenimiento toma aproximadamente 2 horas por equipo.

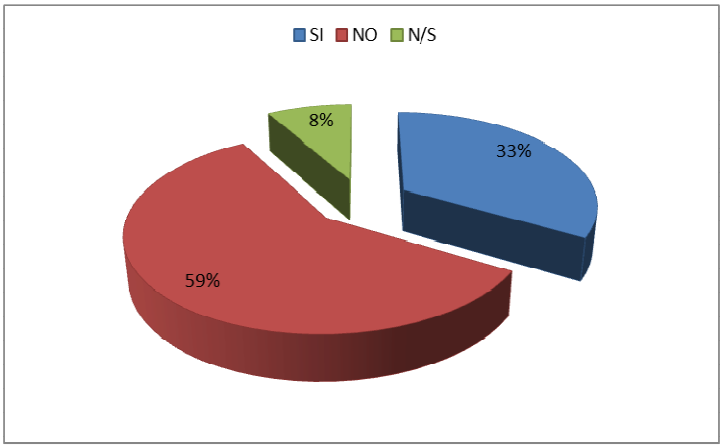
- ✓ ¿Se utilizan programas de descarga de archivos de usuario (música, películas, programas...)?

Tabla 10 Tabulación respuestas pregunta No. 4

Valor ponderado	Frecuencia	Porcentaje %
SI	8	33,33%
NO	14	58,33%
N/S	2	8,33%
Total	24	99,99%

Fuente: El autor

Ilustración 15 Programas de descarga libre



Fuente: El autor

En este caso el 58.33% indico que no era posible instalar programas que no fueran autorizados por la Vicepresidencia de TIC´S, mucho menos si estos eran de uso gratuito. Por su parte el 33.33% afirmo que si se hacía uso de aplicaciones de uso gratuito para descargar no solo música sino otro tipo de archivos multimedia a pesar de que se esté incurriendo en el incumplimiento de la "CARTA DE COMPROMISO DE LICENCIAMIENTO, USO DE SOFTWARE Y CUMPLIMIENTO DE POLÍTICAS INFORMÁTICAS", en tanto a las personas que indicaron no saber si este tipo de descargas se estaban efectuando al interior del área coincidieron en que no era posible hacerlo dado que estaba prohibido en Casa Matriz.

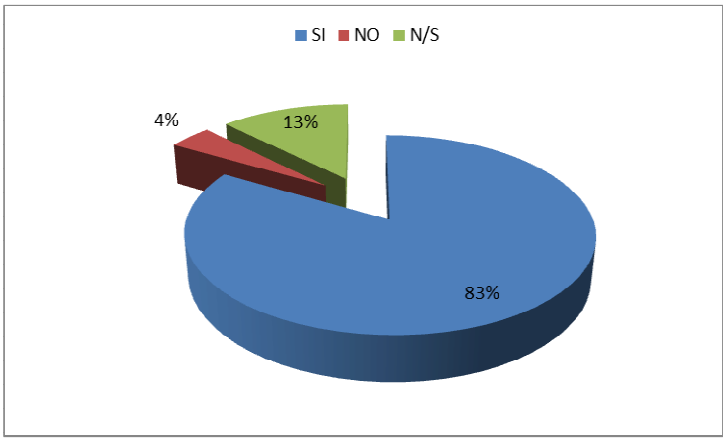
- ✓ ¿Conoce si Casa Matriz cuenta con un servidor central de datos?
- ✓ Sobre dicho servidor, ¿sabe si se le realiza un mantenimiento informático periódico?

Tabla 11 Tabulación respuestas pregunta No.5

Valor ponderado	Frecuencia	Porcentaje %
SI	20	83,33%
NO	1	4,17%
N/S	3	12,50%
Total	24	100,00%

Fuente: El autor

Ilustración 16 Centro de Procesamiento de datos



Fuente: El autor

Para este cuestionamiento se puedo observar que 3 personas correspondiente al 12.50% no sabe si en Casa Matriz existe un servidor central, aunque más que no saber confunden el data center alterno. Para el caso de las respuestas afirmativas representando el 83.33% sabe que si hay un servidor central y un data center alterno. En cuanto al mantenimiento del mismo, las respuestas coincidieron en cuanto a saber si existía o no un servidor central de datos y de acuerdo a sus respuestas asumieron que este tenía que tener un mantenimiento informático periódico. Es de notar que hay desconocimiento en cuanto a los activos informáticos y su manejo.

Comunicaciones

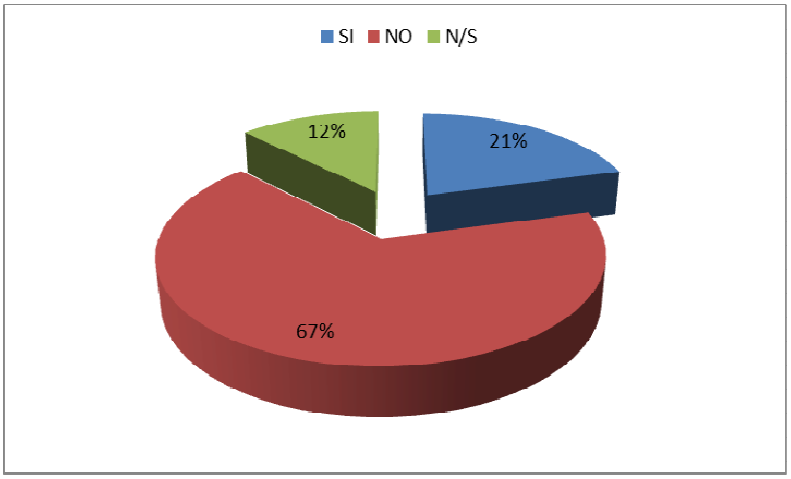
- ✓ ¿En la entidad se trabaja desde algún ordenador externo, por conexión vía Internet?

Tabla 12 Tabulación respuestas pregunta No. 6

Valor ponderado	Frecuencia	Porcentaje %
SI	5	20,83%
NO	16	66,67%
N/S	3	12,50%
Total	24	100,00%

Fuente: El autor

Ilustración 17 Ordenadores externos



Fuente: El autor

Con un 67% la respuesta NO tiene la mayor representación; es por esto que nuevamente se evidencia que hay desconocimiento por parte de los líderes de proceso, en Casa Matriz existe el proyecto de Teletrabajo por tanto si hay personas que trabajan desde un ordenador externo, tan solo el 21% de los entrevistados afirmo que se gestionan procesos desde fuera de las instalaciones.

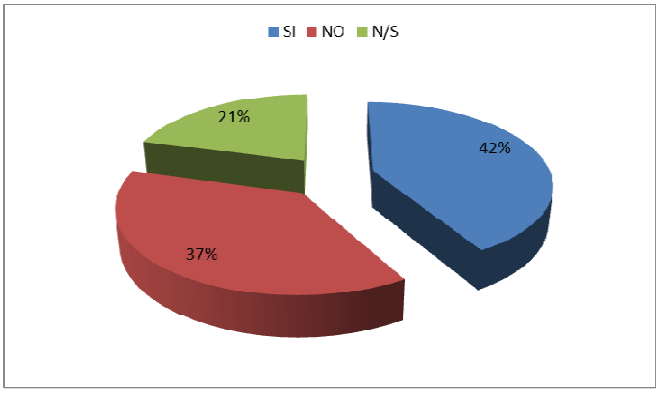
- ✓ Si la conexión en Casa Matriz es mediante la red (WIFI), ¿conoce si se utilizan las medidas de seguridad pertinentes para proteger dicha conexión?

Tabla 13 Tabulación respuestas pregunta No. 7

Valor ponderado	Frecuencia	Porcentaje %
SI	10	41,67%
NO	9	37,50%
N/S	5	20,83%
Total	24	100,00%

Fuente: El autor

Ilustración 18 Red Wifi



Fuente: El autor

En este aspecto, se puede observar que el 42% afirma que hay conexión vía WIFI y que cuenta con las medidas pertinentes, sin embargo, el 37% informa que la conexión de la mayoría de equipos es mediante la red LAN y por su parte el 21% indica no saber si los ordenadores de Casa Matriz se conectan de esta forma.

Datos de la empresa

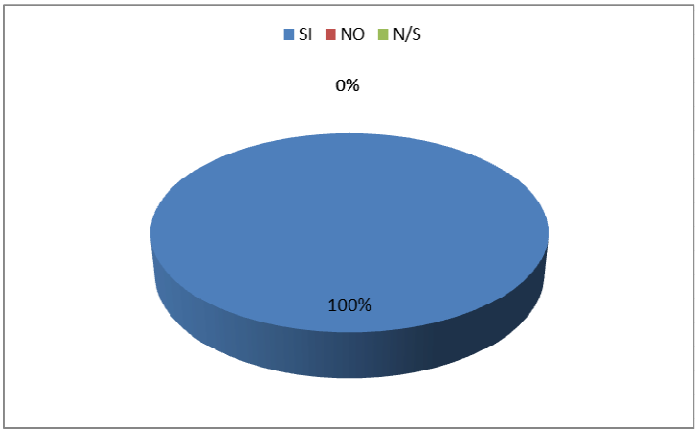
- ✓ ¿Los computadores de su área tienen datos de la empresa almacenados en el disco duro?

Tabla 14 Tabulación respuestas pregunta No. 8

Valor ponderado	Frecuencia	Porcentaje %
SI	24	100,00%
NO	0	0,00%
N/S	0	0,00%
Total	24	100,00%

Fuente: El autor

Ilustración 19 Estaciones de trabajo



Fuente: El autor

Las 24 personas entrevistadas coincidieron en que era una pregunta muy obvia pero afirmaron que efectivamente la mayor parte de la información de la compañía reposa en cada una de las estaciones de trabajo y que esta solo se reubica cuando se realizan los backups del área.

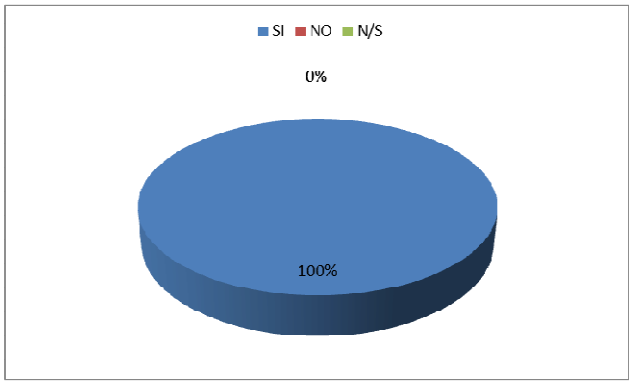
✓ ¿Se realiza copia de seguridad de la información que maneja su área?

Tabla 15 Tabulación respuestas pregunta No. 9

Valor ponderado	Frecuencia	Porcentaje %
SI	24	100,00%
NO	0	0,00%
N/S	0	0,00%
Total	0	100,00%

Fuente: El autor

Ilustración 20 Copias de seguridad



Fuente: El autor

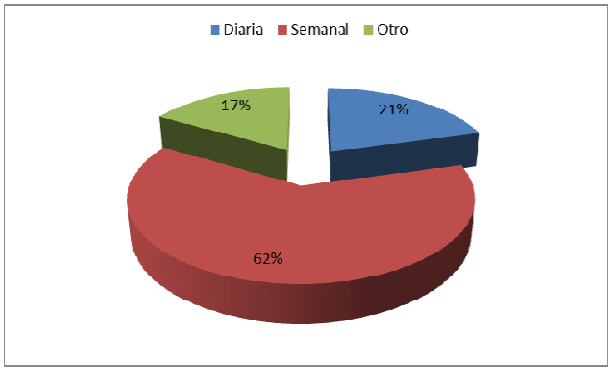
Con qué frecuencia

Tabla 16 Tabulación respuestas pregunta No. 10

Valor ponderado	Frecuencia	Porcentaje %
Diaria	5	20,83%
Semanal	15	62,50%
Otro	4	16,67%
Total	24	100,00%

Fuente: El autor

Ilustración 21 Frecuencia de copias de seguridad



Fuente: El autor

El 100% de los entrevistados coincidieron en que se realizan copias de seguridad con el fin de respalda la disponibilidad de la información, esta práctica esta

apropiada por los colaboradores más por ser una exigencia que por el sentido mismo de su importancia a la hora de mantener la información dispuesta cuando esta se requiera. En tanto a la frecuencia con la que se realizan las copias de seguridad el 62% indica que esta se realiza semanalmente debido a la importancia de la información, el 21% indica que lo hace diario debido a la sensibilidad de los datos manejados por estas áreas y por su parte solo el 17% responde que estas se llevan a cabo cada 20 o 30 días según sea la necesidad.

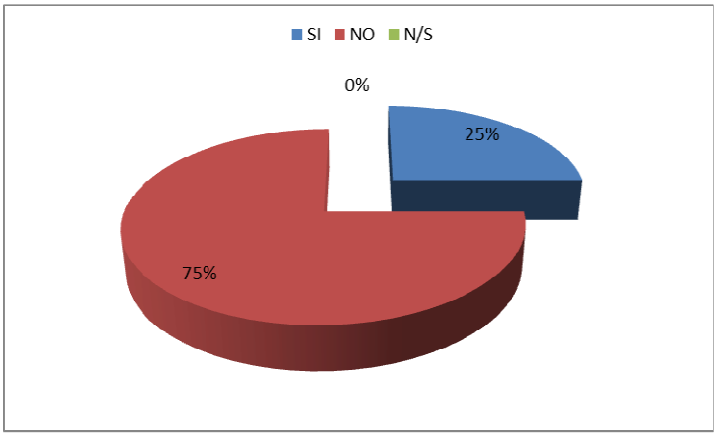
- ✓ ¿Usted o sus colaboradores a cargo poseen alguna copia de seguridad (USB / DVD /Otro) fuera de la empresa?

Tabla 17 Tabulación respuestas pregunta No. 11

Valor ponderado	Frecuencia	Porcentaje %
SI	6	25,00%
NO	18	75,00%
N/S	0	0,00%
Total	0	100,00%

Fuente: El autor

Ilustración 22 Uso de USB



Fuente: El autor

El 75% revela que no es posible guardar copias de seguridad en dispositivos extraíbles, esto debido a que no es correcto, sin embargo, algunos

extraoficialmente indicaron que en algún momento tuvieron que llevar a cabo esta práctica debido a que la Gerencia de Infraestructura no garantizaba que la información guardada en el File server no fuera manipulada, sustraída, dañada o eliminada; dado que no se contaba con un adecuado monitoreo.

El restante 25% aclaro que debido a algunas fallas del File Server se vieron obligados a guardar la información en alguno medio extraíble pero que estos mismos fueron conservados dentro de las instalaciones de la entidad.

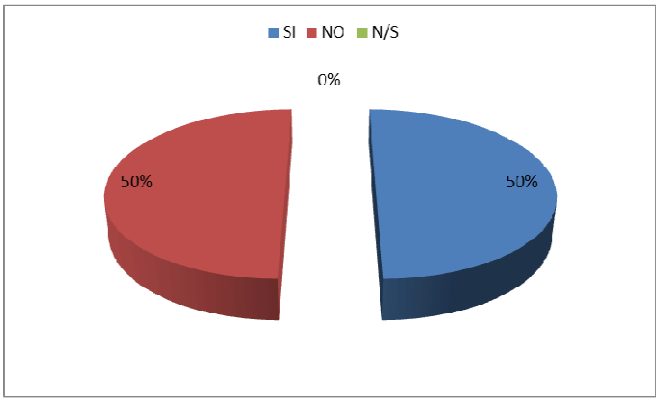
✓ ¿Se realiza un mantenimiento de las copias de seguridad de Casa Matriz?

Tabla 18 Tabulación respuestas pregunta No. 12

Valor ponderado	Frecuencia	Porcentaje %
SI	12	50,00%
NO	12	50,00%
N/S	0	0,00%
Total	0	100,00%

Fuente: El autor

Ilustración 23 Mantenimiento de equipos



Fuente: El autor

Se aprecia que en este sentido las opiniones están divididas esto debido a los incidentes presentados en el File Server, aunque ya fueron superadas aún persiste el temor de guardar allí la información importante de los procesos.

Programas y Aplicaciones Informáticas

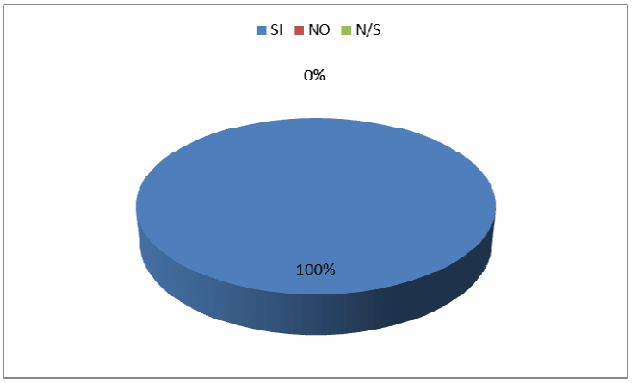
- ✓ ¿Los programas y aplicaciones usadas en Casa Matriz, cumplen con las características de seguridad informática propuestas por Positiva?

Tabla 19 Tabulación respuestas preguntas No. 13

Valor ponderado	Frecuencia	Porcentaje %
SI	24	100,00%
NO	0	0,00%
N/S	0	0,00%
Total	0	100,00%

Fuente: El autor

Ilustración 24 Aplicaciones informáticas



Fuente: El autor

Todos coinciden en que los sistemas de información cuentan con parámetros de seguridad que garantizan la confiabilidad, integridad y disponibilidad de la información, aunque en si Positiva no tenga unas políticas claramente definidas en materia de software.

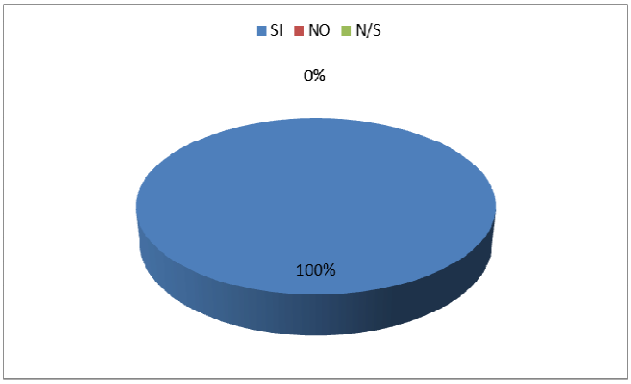
- ✓ ¿Hay algún encargado de instalar/desinstalar los programas y aplicaciones informáticas en Casa Matriz?

Tabla 20 Tabulación respuestas pregunta No. 14

Valor ponderado	Frecuencia	Porcentaje %
SI	24	100,00%
NO	0	0,00%
N/S	0	0,00%
Total	0	100,00%

Fuente: El autor

Ilustración 25 Instalación de aplicaciones



Fuente: El autor

Es claro que la entidad cuenta con una firma externa encargada de realizar las configuraciones pertinentes de acuerdo a la necesidad del proceso que se gestiona. El 100% de los entrevistados afirma conocer que solo COMSISTELCO está autorizado para llevar a cabo esta labor.

Seguridad Informática

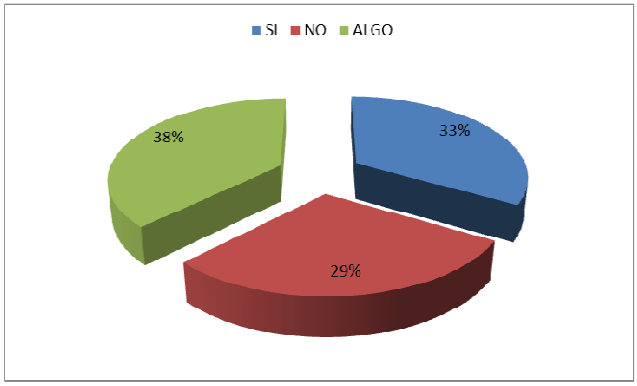
¿Conoce usted algo referente a la seguridad informática?

Tabla 21 Tabulación respuestas pregunta No. 15

Valor ponderado	Frecuencia	Porcentaje %
SI	8	33,33%
NO	7	29,17%
ALGO	9	37,50%
Total	24	100,00%

Fuente: El autor

Ilustración 26 Desconocimiento



Fuente: El autor

Siendo la seguridad un factor muy importante en el manejo de los negocios, es indudable que el desconocimiento es un ingrediente muy común en las entidades, como se puede notar el 29% no sabe que es seguridad informática y tan solo el 33% tiene nociones básicas al respecto, en tanto el 38% dice saber algo debido a sus experiencias en otras entidades o por su formación académica.

✓ Dígame que sabe al respecto

Algunos indicaron que al interior de Casa Matriz se está socializando algunas directivas en materia de seguridad y que a través del medio de comunicación de la entidad se alerta a todos los funcionarios sobre posibles fraudes electrónicos a través de mensajes enviados masivamente al correo electrónico corporativo.

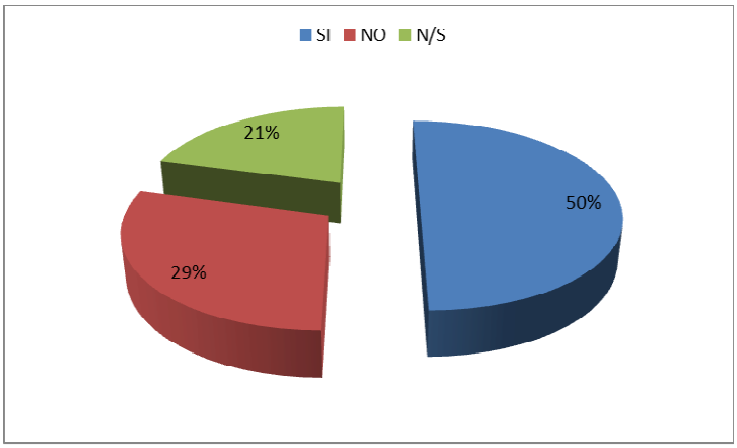
✓ ¿La compañía ha dispuesto políticas de seguridad para el manejo de las herramientas informáticas de las que disponen para la gestión de su proceso?

Tabla 22 Tabulación respuestas pregunta No. 16

Valor ponderado	Frecuencia	Porcentaje %
SI	12	50,00%
NO	7	29,17%
N/S	5	20,83%
Total	24	100,00%

Fuente: El autor

Ilustración 27 Políticas de seguridad establecidas



Fuente: El autor

✓ ¿Cuáles?

La "CARTA DE COMPROMISO DE LICENCIAMIENTO, USO DE SOFTWARE Y CUMPLIMIENTO DE POLÍTICAS INFORMÁTICAS", algunas disposiciones sobre el uso e instalaciones de software gratuito en los ordenadores de Casa Matriz, uso adecuado del correo corporativo, la conexión a un servidor proxy para evitar el ingreso a redes sociales y realizar copias de seguridad de acuerdo a la necesidad y vita útil de la información.

- ✓ Qué medidas toma para proteger la información de su área?

Se les solicita a todos los funcionarios realizar copias de seguridad en el File Server, no desconectar el proxy para acceder a redes sociales, evitar abrir correos de dudosa procedencia e informar a la Gerencia de Infraestructura si ocurre algún incidente que afecta la confidencialidad de la información.

Una vez finalizada la tabulación y análisis de las entrevistas, se concluye que en Positiva Compañía de Seguros S.A-Casa Matriz se toman algunas medidas de seguridad informática instauradas por la vicepresidencia de TIC´S con el fin de garantizar la seguridad de los activos de información más valiosos para la entidad, sin embargo, no se ve indicios de establecer un SGSI formal y documentado, razón por la cual el proyecto pretende proponer un SGSI acorde a las necesidades de la compañía y el cual será complementado con los diferentes procedimientos, manuales y directrices ya establecidas a fin de consolidar dicho sistema y que finalmente este sea auditado y certificado por el ente definido para este fin.

8.1.1.4 Observación del manejo de la información sensible de la compañía.

Como se ha mencionado en anteriores secciones de esta investigación, la entidad no cuenta con políticas de seguridad que garanticen el adecuado manejo de la información sensible o confidencial para la aseguradora y no solo es una directriz que guie tal manejo sino además, que el personal no es consciente de que es necesario cultivar la cultura de protección y buen uso de la información. Durante un día normal de trabajo se procedió a visitar la Gerencia de Gestión Financiera, Operaciones Financieras, Indemnizaciones y Afiliaciones y novedades; en donde se puedo observar que en la gran mayoría de los casos los procesos se gestionan de forma manual a pesar de contar con robustos sistemas de información y por otro lado algunas prácticas no muy seguras y la falta de concientización en materia de seguridad de la información:

- Los documentos, carpetas y otros medios de almacenamiento que contienen información sensible, no están ubicadas en un área protegida, por el contrario la mayor parte de la información está al alcance de cualquier persona que pueda ingresar a estas áreas.

- A pesar de que existe un mecanismo automático de bloqueo de los computadores que asegura el mismo cuando el funcionario no está. Se

observó que muchos de los colaboradores cuando deben retirarse de su lugar de trabajo no bloqueaban el equipo dejando a disposición de cualquiera su estación de trabajo y la información que en ese momento estaba tratando.

- Algunos usuarios apuntan sus contraseñas de ingreso a su computador, aplicaciones entre otros, en la agenda de trabajo o en memos que dejan sobre su escritorio.

- Los computadores portátiles deben ser asegurados mediante una guaya de seguridad, sin embargo, algunos de los colaboradores no hacen uso de esta, exponiéndose a que su equipo sea sustraído de forma no autorizada de las instalaciones.

Ilustración 28 Portátiles sin asegurar

Fuente: El autor

- Debido a que la información financiera es altamente sensible, se notó que muchas de las impresiones de balances de prueba, notas de estados financieros, solicitudes de pago y órdenes de pago son desechados de forma inadecuada, es decir, no son destruidos en su totalidad sino que son reutilizadas como papel reciclable.

- Por su parte las liquidaciones de incapacidades temporales y parciales permanentes se está gestionando de forma manual y a su vez se están registrando en una base de Excel que no tiene ningún respaldo y a la fecha el backup de esta se encuentra en una memoria USB que es utilizada por más de un funcionario.

- El registro de los nuevos asegurados o renovación de afiliaciones es tratada por un único funcionario que lo realiza manualmente a través de un archivo de Excel enviado a través de correo electrónico al proveedor encargado de la carga de estos datos al sistema SIARP sin ninguna medida de seguridad.

Es posible que muchas de estas acciones se mejoren sensibilizando a las personas sobre la importancia que tiene respaldar la confidencialidad, integridad y disponibilidad de la información con la cual está comprometida la organización; además, de la estructuración de un SGSI, definición y socialización de políticas de seguridad que permitan garantizar que toda la información es manejado bajo buena prácticas.

Una vez culminado el análisis y evidenciado las diferentes situaciones que afectan la seguridad de Positiva se estableció que el problema de seguridad está asociado a la falta de un Sistema de Gestión de Seguridad de la Información. Igualmente a la poca concientización, apropiación y conocimiento en materia de seguridad por parte de los colaboradores, no se dan los espacios necesarios para una participación activa de todos los funcionarios en la definición de controles de seguridad basados un análisis y evaluación de riesgos.

Por otro lado, se apreció que no hay una diferenciación clara entre seguridad informática y de la información por parte de los profesionales del área de TIC´S, y por supuesto los colaboradores del común tampoco pueden diferir entre un término y otro; además no se cuenta con un sistema apropiado para la gestión y valoración de riesgos de seguridad y por ultimo no se tiene un política de seguridad establecida y que esté alineada con la plataforma estratégica del negocio.

8.1.1.5 Declaración de aplicabilidad**-**Sistema de gestión de la Seguridad de la Información

Esta unidad pretende evidenciar los controles existentes y aquellos que son relevantes y aplicables para un adecuado SGSI en la organización y que aún no se han contemplado. En esta declaración, se encontrara las justificaciones pertinentes, motivo de selección, requisitos legales, obligaciones contractuales y

necesidades empresariales de la organización en materia de seguridad de la información.

Tabla 23 Nomenclatura motivos de selección

NOMENCLATURA	NOMBRE
L	Requerimiento regulatorio
C	Obligación contractual
N	Requerimiento del negocio
R	Análisis de riesgos

Fuente:
http://pegasus.javeriana.edu.co/~CIS0830IS12/documents/Anexo%20H%20Declaracion%20de%20Aplicabilidad.pdf

Tabla 24 Declaración de aplicabilidad

DECLARACIÓN DE APLICABILIDAD PARA POSITIVA COMPAÑÍA DE SEGUROS SA.

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD		JUSTIFICACIÓN	RAZONES PARA LA SELECCIÓN DE CONTROLES			
					L	C	N	R
A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN								
A 5.1 ORIENTACIÓN DE LA DIRECCIÓN PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	A 5.1.1 POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	1	NO	La entidad es consciente de los riesgos que pueden comprometer la seguridad informática de la misma, sin embargo, estos no han sido reconocidos y mucho menos analizados y gestionados. Es claro que es necesario implementar una política de seguridad de la información para informar y concientizar a todos los funcionarios y partes interesadas sobre los riesgos a los que está expuesta la aseguradora, así como los controles a establecer para evitar la materialización de estos. Es importante señalar que dicha política debe definir	X		X	
	A 5.1.2 REVISIÓN DE LAS POLITICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	2	NO		X		X	

Tabla 24 (continuación)

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD		JUSTIFICACIÓN	RAZONES PARA LA SELECCIÓN DE CONTROLES			
					L	C	N	R
				con claridad los responsables de su desarrollo e implementación. Una vez construida la política de seguridad de la información se debe proceder con la revisión de la misma con el fin de asegurar su idoneidad y efectividad.				
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN								
A 6.1 ORGANIZACIÓN INTERNA	A 6.1.1 ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN	3	NO	A través de la política de seguridad de la información es importante establecer el compromiso, organización y asignación de responsabilidades para el cumplimiento de la misma, igualmente mantener protegida la información mediante la revisión del SGSI, pactar acuerdos de confidencialidad, Establecer contacto con las autoridades y grupos de interés especiales, y la revisión interna de seguridad de la información, por lo anterior es vital instituir un sistema en de control interno informático.			X	
	A 6.1.2 SEPARACIÓN DE DEBERES	4	NO				X	
	A 6.1.3 CONTACTO CON LAS AUTORIDADES	5	SI		X			
	A 6.1.4 CONTACTO CON GRUPOS DE INTERÉS ESPECIAL	6	SI				X	
	A 6.1.5 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS.	7	NO					X

Tabla 24 (continuación)

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD		JUSTIFICACIÓN	RAZONES PARA LA SELECCIÓN DE CONTROLES			
					L	C	N	R
A 6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO	A 6.2.1 POLÍTICA PARA DISPOSITIVOS MÓVILES	8	SI	En Casa Matriz se prohíbe la conexión a las redes inalámbricas de internet por parte de los dispositivos móviles y equipos de terceros y funcionarios.				X
	A 6.2.2 TELETRABAJO	9	NO	Según lo establecido en la Ley 1221 de 2008 la organización cuenta con la modalidad de Teletrabajo, siendo esta una forma desempeño de actividades remuneradas, utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física de este.		X		
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS								
A 7.1 ANTES DE ASUMIR EL EMPLEO	A 7.1.1 SELECCIÓN	10	SI	La organización requiere de ciertas asesorías y consultorías razón por la cual requiere de personal externo que tiene acceso a la información de la compañía, por tanto es necesario implementar controles		X		
	A 7.1.2 TÉRMINOS Y CONDICIONES DEL EMPLEO	11	SI			X		

Tabla 24 (continuación)

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD		JUSTIFICACIÓN	RAZONES PARA LA SELECCIÓN DE CONTROLES			
					L	C	N	R
				basándose en la normatividad vigente, código de ética y buen gobierno a fin de asegurar la verificación de antecedentes, asignación de roles y responsabilidades, términos de contratación y condiciones laborales previo acceso a la información.				
A 7.2 DURANTE LA EJECUCIÓN DEL EMPLEO	A 7.2.1 RESPONSABILIDADES DE LA DIRECCIÓN	12	NO	Los colaboradores de la organización no son conscientes de los riesgos, responsabilidades y deberes con respecto a la seguridad información. No se ha capacitado al personal en temas relacionados con la seguridad de la información y tampoco existe un proceso disciplinario establecido para actuar frente alguna violación de seguridad.			X	
	A 7.2.2 TOMA DE CONCIENCIA, EDUCACIÓN, Y FORMACIÓN EN S.I.	13	NO				X	
	A.7.2.3 PROCESO DISCIPLINARIO	14	NO			X		
A 7.3 TERMINACIÓN Y CAMBIO DE EMPLEO	A7.3.1 TERMINACIÓN O CAMBIO DE RESPONSABILIDADES DE EMPLEO	15	SI	Una vez finalizado el contrato de trabajo o renuncia de un colaborador la Gerencia de Infraestructura es informada a fin de bloquear el acceso a dicho usuario y		X		

Tabla 24 (continuación)

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD		JUSTIFICACIÓN	RAZONES PARA LA SELECCIÓN DE CONTROLES			
					L	C	N	R
				retirar el equipo de cómputo de la estación de trabajo con el propósito de realizar copias de seguridad de información				
A.8 GESTION DE ACTIVOS								
A 8.1 RESPONSABILIDAD POR LOS ACTIVOS	A 8.1.1 INVENTARIO DE ACTIVOS	16	NO	Debido a que la entidad no cuenta con un SGSI formal no existe un inventario de activos de información, sin embargo, si identifica plenamente el "propietarios de estos". También existen ciertas de reglas documentadas e implementadas para el buen uso de los activos informáticos.				X
	A 8.1.2 PROPIEDAD DE LOS ACTIVOS	17	SI					X
	A 8.1.3 USO ACEPTABLE DE LOS ACTIVOS	18	SI					X
	A 8.1.4 DEVOLUCIÓN DE LOS ACTIVOS	19	SI	Finalizada la relación contractual con la entidad es responsabilidad del funcionario realizar la entrega del equipo de cómputo a la Gerencia de Infraestructura.				X
A 8.2 CLASIFICACIÓN DE LA INFORMACIÓN	A 8.2.1 CLASIFICACIÓN DE LA INFORMACIÓN	20	NO	La aseguradora posee información de diferentes niveles, sin embargo, estos no ha sido reconocidos				X
	A 8.2.2 ETIQUETADO DE LA INFORMACIÓN	21	NO					X

Tabla 24 (continuación)

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD		JUSTIFICACIÓN	RAZONES PARA LA SELECCIÓN DE CONTROLES			
					L	C	N	R
	A 8.2.3 MANEJO DE ACTIVOS	22	NO	por tal razón es primordial que esta elabore una adecuada clasificación de la información y a su vez implemente los controles apropiados para la protección de la misma				X
A 8.3 MANEJO DE MEDIOS	A 8.3.1. GESTIÓN DE MEDIOS REMOVIBLES	23	SI	Con el desarrollo de las actividades de aseguramiento se hace uso de medios para el almacenamiento e intercambio de información, tales como correo electrónico empresarial, servicios de mensajería, USB, CD, entre otros por lo tanto en Casa Matriz se han instituido directrices para el manejo adecuado de estos medios así evitar eventos como divulgación, modificación, retiro o destrucción de información no autorizada.				X
	A 8.3.2 DISPOSICIÓN DE LOS MEDIOS	24	SI					X
	A 8.3.3 TRANSFERENCIA DE MEDIOS FÍSICOS	25	SI					X
A.9 CONTROL DE ACCESO								
A 9.1 REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO	A 9.1.1 POLÍTICA DE CONTROL DE ACCESO	26	SI	Se tiene establecidas políticas de acceso a las instalaciones físicas como a los sistemas de información, tales como sistema biometría de	X		X	

Tabla 24 (continuación)

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD		JUSTIFICACIÓN	RAZONES PARA LA SELECCIÓN DE CONTROLES			
					L	C	N	R
	A 9.1.2 ACCESO A REDES Y A SERVICIOS EN RED	27	SI	autenticación, claves de acceso, validación de entrada y salida de datos , segmentación de la red, cierre de sesiones inactivas en los servidores entre otros.				X
A 9.2 GESTIÓN DE ACCESO DE USUARIOS	A 9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS	28	SI	En Casa Matriz está establecido que la responsabilidad de gestionar todo lo concerniente a acceso de usuarios está a cargo de la Gerencia de Infraestructura la cual ha dispuesto lineamientos para el alta y baja de usuarios, asignación de perfiles y privilegios y mecanismos de autenticación de usuarios.				X
	A 9.2.2 SUMINSITRO DE ACCESO DE USUARIOS	29	SI					X
	A 9.2.3 GESTIÓN DE DERECHOS DE ACCESO PRIVILEGIADO	30	SI					X
	A 9.2.4 GESTIÓN DE LA INF. DE AUTENTICACIÓN SECRETA DE USUARIOS	31	SI					X
	A 9.2.5 REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIOS	32	SI					X
	A 9.2.6 RETIRO O AJUSTE DE LOS DERECHOS DE ACCESO.	33	SI					X
A 9.3 RESPONSABILIDADES DE LOS USUARIOS	A 9.3.1 USO DE INFORMACIÓN DE AUTENTICACIÓN SECRETA	34	SI	Los usuarios en Casa Matriz con acceso a información sensible deben cambiar sus contraseñas de acceso cada 30 días calendario, está dispuesto en el sistema una alerta para que estos sepan cuando es el momento de realizar				X

Tabla 24 (continuación)

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD		JUSTIFICACIÓN	RAZONES PARA LA SELECCIÓN DE CONTROLES			
					L	C	N	R
				este cambio, dicha clave tiene ciertas características que solo son conocidas por el usuario y el técnico de soporte.				
A 9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	A 9.4.1 RESTRICCIÓN DE ACCESO A LA INFORMACIÓN	35	SI	La entidad tiene definas políticas para controlar el acceso a la información, en esta se establece los responsables de la misma, control de cambios, restricción e identificación de niveles de acceso a fin de controlar los privilegios sobre los datos.				X
	A 9.4.2 PROCEDIMIENTO DE INGRESO SEGURO.	36	SI				X	X
	A 9.4.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS.	37	SI				X	X
	A 9.4.4 USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS	38	SI				X	
	A 9.4.5 CONTROL DE ACCESO A CODIGOS FUENTE DE PROGRAMAS	39	SI				X	X
A. 10 CRIPTOGRAFIA								
A 10.1 CONTROLES CRIPTOGRAFICOS	A 10.1.1 POLÍTICA SOBRE USO DE CONTROLES CRIPTOGRÁFICOS	40	NO	Existe una directriz informal de control y uso criptográfico y la administración de claves se realiza mediante dispositivos informáticos.				X
	A 10.1.2 GESTIÓN DE LLAVES	41	NO					X
A. 11 SEGURIDAD FISICA Y DEL ENTORNO								

Tabla 24 (continuación)

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD		JUSTIFICACIÓN	RAZONES PARA LA SELECCIÓN DE CONTROLES			
					L	C	N	R
A 11.1 ÁREAS SEGURAS	A 11.1.1 PERÍMETRO DE SEGURIDAD FÍSICA	42	SI	Se tienen establecidos controles de seguridad preventivos, activos, reactivos y proactivos. El perímetro de Casa Matriz esta monitoreado por cámaras de seguridad, el acceso a las instalaciones está regulado por personal de vigilancia y recepción las 24 horas del día y la autenticación del personal se realiza mediante sistema biométrico. En tanto al ingreso de las áreas seguras se realiza una vez sea autorizado y a través de tarjeta de proximidad.			X	
	A 11.1.2 CONTROLES DE ACCESO FÍSICOS	43	SI				X	
	A 11.1.3 SEGURIDAD DE OFICINAS, RECINTOS E INSTALACIONES	44	SI				X	
	A 11.1.4 PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES	45	SI				X	
	A 11.1.5 TRABAJO EN ÁREAS SEGURAS	46	SI				X	
	A 11.1.6 ÁREAS DE DESPACHO Y CARGA	47	NO	No se cuenta con este tipo de áreas				
A 11.2 EQUIPOS	A 11.2.1 UBICACIÓN Y PROTECCION DE LOS EQUIPOS	48	SI	Están contempladas políticas y controles previamente documentados en los estándares de seguridad ESTÁNDAR DE SEGURIDAD DE LOS EQUIPOS Código: VA-OD-ESLE-01 y ESTÁNDAR DE SEGURIDAD EN EL CENTRO DE DATOS Código: VA-OD-ESCD-01, es producente realizar una			X	X
	A 11.2.2 SERVICIOS DE SUMINSITRO	49	SI				X	
	A 11.2.3 SEGURIDAD EN EL CABLEADO	50	SI				X	X
	A 11.2.4 MANTENIMIENTO DE EQUIPOS	51	SI				X	X
	A 11.2.5 RETIRO DE ACTIVOS	52	SI				X	X
	A 11.2.6 SEGURIDAD DE EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES	53	SI		X	X	X	X

Tabla 24 (continuación)

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD		JUSTIFICACIÓN	RAZONES PARA LA SELECCIÓN DE CONTROLES			
					L	C	N	R
	A 11.2.7 DISPOSICIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS	54	SI	actualización de estos documentos con el fin de garantizar que dichos controles sean los apropiados.				X
	A 11.2.8 EQUIPOS DE USUARIO DESATENDIDO	55	SI				X	X
	A 11.2.9 POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA	56	SI				X	
A.12 SEGURIDAD DE LAS OPERACIONES								
A 12.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	A 12.1.1 PROCEDIMIENTOS DE OPERACIÓN DOCUMENTADOS	57	SI	Se establecen controles para no comprometer la seguridad del sistema ni el entorno operativo. Los procedimientos informáticos están documentados en el ESTÁNDAR PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES Código: VA-OD-EPAL-01.			X	X
	A 12.1.2 GESTIÓN DE CAMBIOS	58	SI		X		X	X
	A 12.1.3 GESTIÓN DE CAPACIDAD	59	SI		X		X	
	A 12.1.4 SEPARACION DE LOS AMBIENTES DE DESARROLLO, PRUEBAS Y OPERACIÓN.	60	SI		X		X	X
A 12.2 PROTECCION CONTRA CODIGOS MALICIOSOS	A.12.2.1 CONTROLES CONTRA CÓDIGOS MALICIOSOS	61	SI	Dado la operación de la aseguradora mediante este control se garantiza que todos los servicios estarán disponibles y no se verá afectada la respuesta de los sistemas de información Los equipos de la compañía se encuentran protegidos por software de detección y reparación de virus y mensualmente se publican las estadísticas de virus como forma de			X	

Tabla 24 (continuación)

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD		JUSTIFICACIÓN	RAZONES PARA LA SELECCIÓN DE CONTROLES			
					L	C	N	R
				concienciación. La empresa cuenta con un programa de bloqueo de código móvil y de ejecutables en las estaciones de trabajo				
A 12.3 COPIAS DE RESPALDO	A 12.3.1 RESPALDO DE LA INFORMACIÓN	62	SI	Asegurar la ejecución de procedimientos de Backus y recuperación permiten restaurar en el menor tiempo la información ante la materialización de un riesgo, y así permitir que la empresa continué con sus actividades.	X	X	X	X
A 12.4 REGISTRO Y SEGUIMIENTO	A12.4.1 REGISTRO DE EVENTOS	63	NO	Se requiere de forma urgente adquirir una herramienta que permita el análisis evaluación y gestión del riesgo.			X	X
	A12.4.1 PROTECCIÓN DE LA INFORMACIÓN DE REGISTRO	64	NO				X	X
	A12.4.1 REGISTROS DEL ADMINSITRADOR Y DEL OPERADOR	65	NO				X	X
	A12.4.1 SINCRONIZACIÓN DE RELOJES	66	NO				X	X

Tabla 24 (continuación)

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD		JUSTIFICACIÓN	RAZONES PARA LA SELECCIÓN DE CONTROLES			
					L	C	N	R
A 12.5 CONTROL DE SOFTWARE OPERACIONAL	A 12.5.1 INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS	67	SI	Se desarrolló políticas de gestión y configuración de versiones. Puesta en funcionamiento de software para el control de versiones y el desarrollo y seguimiento de los requerimientos de los sistemas de información.			X	X
A 12.6 GESTION DE LA VULNERABILIDAD TÉCNICA	A 12.6.1 GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS	68	SI	Positiva cuenta con herramientas para la detección y solución de vulnerabilidades.				X
	A 12.6.2 RESTRICCIÓN SOBRE LA INSTALACION DE SOFWARE	69	SI	Solo es permitida la instalación de software debidamente licenciado, no se permite el uso de software libre				X
A 12.7 CONTROLES DE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	A 12.7 CONTROLES DE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	70	NO	Es vital formalizar el SGSI. Este a su vez debe ser revisado concienzudamente				X
A. 13 SEGURIDAD DE LAS COMUNICACIONES								
A 13.1 GESTIÓN DE LA SEGURIDAD DE LAS REDES	A 13.1.1 CONTROLES DE REDES	71	SI	Con el propósito de garantizar la confidencialidad, integridad y disponibilidad de la información tratada			X	X
	A 13.1.2 SEGURIDAD DE LOS SERVICIOS DE RED	72	SI				X	X

Tabla 24 (continuación)

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD		JUSTIFICACIÓN	RAZONES PARA LA SELECCIÓN DE CONTROLES			
					L	C	N	R
	A 13.1.3 SEPARACIÓN EN LAS REDES	73	SI	aseguradora			X	X
A 13.2 TRANSFERENCIA DE INFORMACIÓN	A 13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE TRASNFERENCIA DE INFORMACIÓN	74	NO	Debe instaurarse este tipo de controles para garantizar la confidencialidad de la información y disponibilidad de la misma.				X
	A 13.2.2 ACUERDOS SOBRE TRASNFERENCIA DE INFORMACIÓN	75	NO					X
	A 13.2.3 MENSAJERIA ELECTRÓNICA	76	SI	Se han dispuesto controles para proteger la información sensible de la empresa.				X
	A 13.2.4 ACUERDOS DE CONFIDENCIALIDAD O DE NO DIVULGACIÓN	77	SI					X
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS								
A 14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	A 14.1.1 ÁNALISIS Y ESPECIFICACIÓN DE REQUISITOS DE SI	78	SI	Se establecen controles de seguridad para avalar los requisitos del negocio antes de implementar cambios en la tecnología de la empresa.			X	X
	A 14.1.2 SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS	79	SI					X
	A 14.1.3 PROTECCIÓN DE TRANSACCIONES DE LOS SERVICIOS DE LAS APLICACIONES	80	SI					
A 14.2 CONTROL DE ACCESO AL SISTEMA OPERATIVO	A 14.2.1 POLÍTICA DE DESARROLLO SEGURO	81	SI	La entidad cuenta con controles que permiten garantizar el cumplimiento de las especificaciones técnicas y de seguridad necesarias. También controles de			X	X
	A 14.2.2 PROCEDIMIENTO DE CONTROL DE CAMBIOS EN SISTEMAS	82	SI					X
	A 14.2.3 REVISIÓN TÉCNICAS DE LAS APLICACIONES	83	SI				X	X

Tabla 24 (continuación)

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD		JUSTIFICACIÓN	RAZONES PARA LA SELECCIÓN DE CONTROLES			
					L	C	N	R
	DESPUES DE CAMBIOS EN LA PLATAFORMA DE OPERACIÓN			seguridad que regulan los cambios, revisados y sometidos a pruebas con el fin de no comprometer la seguridad del sistema ni el entorno operativo y así la fuga de información. Igualmente a través de la política de desarrollo de terceros establece y exige los lineamientos y buenas prácticas para el desarrollo y construcción de sistemas de información seguros				
	A 14.2.4 RESTRICCIONES EN LOS CAMBIOS A LOS PAQUETES DE SOFTWARE	84	SI				X	
	A 14.2.5 PRINCIPIOS DE CONSTRUCCIÓN DE LOS SISTEMAS SEGUROS	85	SI				X	
	A 14.2.6 AMBIENTE DE DESARROLLO SEGURO	86	NO	La aseguradora no considera necesario este control para la protección de la información.				X
	A 14.2.7 DESARROLLO CONTRATADO EXTERNAMENTE	87	SI	A fin de proteger el acceso al código fuente de los sistemas de información, para evitar su alteración o uso malintencionado			X	
	A 14.2.8 PRUEBAS DE SEGURIDAD DE SISTEMAS	88	SI	Se instituyo estos controles con el propósito de mantener actualizados los sistemas de información y propender por la integridad de la información contenida en estos.				X
	A 14.2.9 PRUEBAS DE ACEPTACIÓN DE SISTEMAS	89	SI	La compañía válida los nuevos sistemas de información en un servidor				X

Tabla 24 (continuación)

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD		JUSTIFICACIÓN	RAZONES PARA LA SELECCIÓN DE CONTROLES			
					L	C	N	R
				de prueba antes de ser puestos a producción.				
A 14.3 DATOS DE PRUEBA	A14.3.1 PROTECCIÓN DE DATOS DE PRUEBA	90	SI	La organización realiza pruebas en ambientes de preproducción con información modificada la cual es eliminada una vez culminan las pruebas				X
A.15 RELACIONES CON LOS PROVEEDORES								
A. 15.1 RELACIONES CON LOS PROVEEDORES	A 15.1.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES	91	SI	Positiva establece controles que le garantizan que son tenidos en cuenta los requisitos del negocio antes de gestionar compras de bienes o servicios que afecten la seguridad de la información y la infraestructura sobre la cual esta soportada. Además exige a sus proveedores el cumplimiento de buenas prácticas y de las políticas de la entidad.			X	
	A 15.1.2 TRATAMIENTO DE LA SEGURIDAD DENTRO DE LOS ACUERDOS CON PROVEEDORES	92	SI				X	
	A 15.1.3 CADENA DE SUMINISTRO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN	93	SI				X	
A 15.2 GESTIÓN DE LA PRESENTACIÓN DE SERVICIOS DE PROVEEDORES	A 15.2.1 SEGUIMIENTO Y REVISIÓN DE LOS SERVICIOS DE LOS PROVEEDORES	94	SI				X	
	A 15.2.2 GESTIÓN DE CAMBIOS EN LOS SERVICIOS DE LOS PROVEEDORES	95	SI				X	
A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION								
A 16.1 GESTION DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN	A 16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	96	NO	Debido a la falta de una política de seguridad de la información es necesaria la implementación de esta a la mayor brevedad posible.			X	

Tabla 24 (continuación)

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD		JUSTIFICACIÓN	RAZONES PARA LA SELECCIÓN DE CONTROLES			
					L	C	N	R
	A 16.1.2 REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN	97	NO	Se debe implementar procedimientos de análisis, evaluación y gestión de riesgos				X
	A 16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	98	NO					X
	A 16.1.4 EVALUACIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN Y	99	NO					X
	A 16.1.5 RESPUESTA A INCIDENTES DE SEGUIRIDAD DE LA INFORMACIÓN	100	NO					X
	A 16.1.6 APRENDIZAJE OBTENIDO DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	101	NO					X
	A 16.1.7 RECOLECCIÓN DE EVIDENCIA	102	NO					X
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DE NEGOCIO								
A 17.1 CONTINUIDAD EN SEGURIDAD DE LA INFORMACIÓN	A 17.1.1 PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	103	SI	Debido al compromiso adquirido por la aseguradora con sus clientes a través de las pólizas de seguro debe garantizar el cubrimiento y respaldo de estas por tal razón ante cualquier interrupción en las actividades del negocio por fallas tecnológicas			X	
	A 17.1.2 IMPLEMENTACIÓN DE LA CONTINUIDAD DE LA SI	104	SI				X	

Tabla 24 (continuación)

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD		JUSTIFICACIÓN	RAZONES PARA LA SELECCIÓN DE CONTROLES			
					L	C	N	R
	A 17.1.3 VERIFICACIÓN, REVISIÓN Y EVALUACIÓN DE LA CONTINUIDAD DE LA SI	105	SI	importantes o desastres, la compañía cuenta con una gestión de continuidad del negocio con el propósito de minimizar el impacto generado en su capacidad respaldar el cubrimiento de las pólizas.			X	
A 17.2 REDUNDANCIAS	A 17.2.1 DISPONIBILIDAD DE INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN	106	SI	Positiva cuenta con un data center alterno a fin de garantizar la disponibilidad de la información.			X	X
A 18.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES	A 18.1.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE Y DE LOS REQUISITOS CONTRACTUALES	107	SI	La organización desarrolla sus actividades en el marco de la legislación Colombiana, los requisitos contractuales y los propios, en tal sentido que establece controles que garantizan el cumplimiento de los mismos.			X	
	A 18.1.2 DERECHOS DE PROPIEDAD INTELECTUAL	108	SI				X	
	A 18.1.3 PROTECCIÓN DE REGISTROS	109	SI				X	
	A 18.1.4 PRIVACIDAD Y PROTECCIÓN DE INFORMACIÓN DE DATOS PERSONALES	110	SI				X	
	A 18.1.5 REGLAMENTACIÓN DE CONTROLES CRIPTOGRÁFICOS	111	NO	Existe una directriz informal de control y uso criptográfico y la administración de claves se realiza mediante dispositivos informáticos.				X

Tabla 24 (continuación)

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD		JUSTIFICACIÓN	RAZONES PARA LA SELECCIÓN DE CONTROLES			
					L	C	N	R
A. 18 CUMPLIMIENTO								
A 18.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN	A 18.2.1 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN	112	NO	Como se ha mencionado anteriormente a la falta de un SGSI y de una política de seguridad informática no se han contemplado estos controles.	X		X	
	A 18.2.2 CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD	113	NO		X		X	
	A 18.2.3 REVISIÓN DEL CUMPLIMIENTO TÉCNICO	114	NO		X		X	

Fuente: El autor

9. DISEÑO DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA POSITIVA COMPAÑÍA DE SEGUROS S.A.

9.1 Fase 2: Identificación de los activos informáticos, definición y aplicación de la metodología de análisis y gestión del riesgo.

Con el fin de dar cumplimiento a esta fase, se procede hacer un reconocimiento de los activos informáticos al interior de Casa Matriz esto permitirá identificar y determinar el tipo de activos informáticos los cuales se listan en el formato denominado “Inventario activos de información”.

9.1.1 Identificación de activos de información

Una vez realizado el recorrido por las instalaciones de Casa Matriz se realizó el levantamiento del inventario de activos de información existentes con relación directa en la operación de la entidad.

Tabla 25 Inventario de activos de información de Casa Matriz

Tipo de Activo	**Nombre de Activo en Casa Matriz-Positiva**
Software y Aplicaciones	Sistema operativo Windows XP licencias OEM. Windows Proffesional 7. Office 2007 licencia OEM Antivirus Microsoft Security Essentials Aplicaciones: SIARP, SISE, SAP, SICO, Sara, NeónWeb, Sian, Gescont, PQR, Midas (valorador de portafolio de inversiones), Aranda y Team Fundation Server (TFS)

Tabla 25 (continuación)

Tipo de Activo	**Nombre de Activo en Casa Matriz-Positiva**
Software y Aplicaciones	Sistema operativo Windows XP licencias OEM. Windows Proffesional 7. Office 2007 licencia OEM Antivirus Microsoft Security Essentials Aplicaciones: SIARP, SISE, SAP, SICO, Sara, NeónWeb, Sian, Gescont, PQR, Midas (valorador de portafolio de inversiones), Aranda y Team Fundation Server (TFS)
Hardware	350 Equipos de cómputo de escritorio 40 Portátiles 48 impresoras HP LaserJet Enterprise M4555 MFP – Multifunción (impresora / copiadora / escáner) – B/N
Instalación	CDP Principal y alterno Cables de fluido eléctrico
Servicios	Conectividad a internet (cable, VPN, Wifi)
Personal	350 Funcionarios operativos 40 Funcionarios de alta dirección 6 Funcionarios de Vigilancia

Fuente: El autor

Tabla 26 Detalle-Inventario de activos de información Casa Matriz

[S] Servicios
PÁGINA WEB Servicios en Línea: ● Pagos en Línea ● Afiliación ARL ● Aporte a Riesgos Laborales ● Gestión Positiva Crea ● Positiva Cuida ● Seguimiento Programas Otros Servicios en Línea: ● Contratación- Registro de Proveedores ● Aporte a riesgos Laborales ● Certificados de aportes ● Beneficios ● Servicios de Información- Fondo de Empleados ● Servicios al Ciudadano- Ofertas de Empleo ● Aprobación charlas PyP ● Archivos de consulta permanente expediente digital Asegurados y Pensionados ARL ● Almacenamiento de datos ● Transferencia de datos ● Servicio de directorio (1) ● Gestión de identidades (2) ● Gestión de privilegios

[D] Datos / Información
• Datos vitales (vital records) (1) • Datos de interés académico (2) • Datos de interés para la administración • Datos de gestión interna • Voz • Multimedia • Código fuente • Código ejecutable • Datos de configuración • Datos de prueba • Datos de carácter personal (3) • De nivel alto • De nivel medio • De nivel básico • Datos clasificados (4) • Secreto • Reservado • Confidencial • Difusión limitada • Sin clasificar

[SW] Aplicaciones (software)
SISTEMA DE INFORMACIÓN DE RIESGOS LABORALES SIARP: Sistema de Información que soporta los procesos de Afiliaciones, Siniestros (Accidentes de trabajo y enfermedades profesionales), Prestaciones Asistenciales y Económicas de las empresas y los afiliados al ramo de Riesgos laborales. SISTEMA DE SEGUROS SISE VIDA INDIVIDUAL Y VIDA COLECTIVO: Suscripción, Indemnización vida individual y Vida colectivo, gestión de la información contable y financiera de la Compañía. SARA: Gestión de información de empleados de planta de la compañía para registro y pago de nómina y parafiscales. SICO: Sistema e información para la gestión documental NEONWEB: Control del inventario Físico de la compañía GESCONT: Gestión de la Contratación PQR: Gestión de Peticiones Quejas y Reclamos MIDAS: Valorador del Portafolio de Inversión SIAN: Sistema de información para la administración de Nóminas de Pensionados originadas en Pensiones ley 100 y pensiones con Conmutación Pensional, con capacidad de registrar las novedades, liquidar los valores de las mesadas pensionales y generar los insumos

de información para los proceso contables y financieros.

ARANDA: Herramienta de soporte y apoyo a usuarios, a través del software “HELP DESK ARANDA”, a través del cual los usuarios de los sistemas de información reportan los incidentes y requerimientos para ser atendidos por las mesas de ayuda. Adicionalmente, se ha implementado un sistema software denominado ARANDA 360 - END POINT:, que se adquirió para cumplir con los requerimientos de seguridad informática solicitados en la Circular 052/07 de la Superintendencia Financiera para bloqueo de dispositivos, bloqueo de acceso a redes inalámbricas (WI-FI) e instalación de software entre otros.

TEAM FOUNDATION SERVER (TFS): Sistema de información colaborativo, para realizar la Gestión de configuración y cambios a aplicativos y sistemas de la Compañía. Control de código fuente y documentación asociada a los proyectos de software de informática.

[HW] Equipos informáticos (hardware)
Grandes equipos (11) Equipos de escritorio (350) portátiles (40) Almacena datos (5) Periféricos • Medios de impresión (6) • Escáner Soporte de la red (7) • Módems • Conmutadores administrables (switch) • Encaminadores (router) • Pasarelas (bridge) • Cortafuegos Punto de acceso Wireless Central telefónica

[COM] Redes de comunicaciones
• Red telefónica • ADSL • Punto a punto • Red inalámbrica • Red local • Internet

[SI] Soportes de información
Electrónicos Almacenamiento en red • CD-ROM • Dispositivos USB • DVD • Disco duro externo No electrónicos • Material impreso • Material digitalizado

[AUX] Equipamiento auxiliar
• Fuentes de alimentación • Sistemas de alimentación ininterrumpida • Generadores eléctricos • Equipos de climatización • Cableado • Discos • Suministros esenciales • Mobiliario: armarios, etc • Cajas fuertes

[L] Instalaciones
• Centro Principal procesamiento de datos • Áreas • Laboratorios de higiene y toxicología • Edificio • Centro alterno de procesamiento de datos

[P] Persona
• Usuarios internos • Operadores • Administradores de sistemas • Administradores de comunicaciones • Administradores de BBDD • Desarrolladores

Fuente: El autor

Tabla 27 Dominios y procesos seleccionados

Ref.	Control
1.	POLÍTICA DE SEGURIDAD
1.1	Conjunto de políticas para la seguridad de la información
1.2	Revisión de las políticas de seguridad de la información
2.	ASPECTOS ORGANIZACIONALES DE LA SEGURIDAD DE LA INFORMACIÓN
2.1	Asignación de responsabilidades para la seguridad de la información.
2.2	Segregación de tareas
2.3	Seguridad de la información en la gestión de proyectos
3.	DISPOSITIVOS PARA MOVILIDAD Y TELETRABAJO
3.1	Política de uso de dispositivos para la movilidad
3.2	Teletrabajo

4	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS
4.1	Seguridad en el desempeño de las funciones
4.2	Responsabilidades de gestión
4.3	Sensibilización y capacitación sobre seguridad de la información
5.	GESTIÓN DE ACTIVOS
5.1	Responsabilidades sobres los activos
5.2	Inventario de activos
5.3	Propiedades de los activos
5.4	Uso aceptable de los activos
5.5	Devolución de los activos
6.	CLASIFICACIÓN DE LA INFORMACIÓN
6.1	Directrices de clasificación
6.2	Etiquetado y manipulación de la información
7.	CONTROL DE ACCESO
7.1	Requerimientos del negocio para el control de acceso
7.2	Política de control de acceso
7.3	Gestión de acceso de usuarios
7.4	Gestión de altas/bajas
7.5	Gestión de privilegios de los perfiles de usuarios
8.	RESPONSABILIDADES DEL USUARIOS
8.1	Uso de información confidencial para la autenticación
9.	CONTROL DE ACCESO APLICACIONES Y SISTEMAS OPERATIVOS

9.1	Restricción de acceso a la información
9.2	Procedimientos seguros de inicio de sesión
9.3	Uso de herramientas de administración de sistemas
10.	CIFRADOS
10.1	Controles criptográficos
10.2	Política de uso
10.3	Gestión de claves de acceso
11.	SEGURIDAD DE LOS EQUIPOS
11.1	Emplazamiento y protección de equipos
11.2	Instalaciones de suministros
11.3	Seguridad del cableado
11.4	Mantenimiento de equipos
12.	SEGURIDAD EN LA OPERATIVIDAD
12.1	Protección contra código malicioso
12.2	Copias de seguridad
13.	SEGURIDAD DE LAS TELECOMUNICACIONES
13.1	Mensajería electrónica
13.2	Acuerdos de confidencialidad
14.	ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO
14.1	Planificación de la continuidad de la seguridad de la información
14.2	Verificación, evaluación de la continuidad de la seguridad de la información
15.	CUMPLIMIENTO DE LOS REQUISITOS LEGALES

15.1	Identificación de la legislación aplicable
15.2	Protección de los registros de la organización
15.3	Protección de datos y privacidad de la información

Fuente: MAGERIT versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro I- Método. Recuperado de: //http: www.ccn.-cert.cni.es /publico/herramientas/pilar5/magerit.

9.1.2 Definición y aplicación de la metodología de análisis y gestión de riesgos informáticos para la identificación, clasificación, valoración y tratamiento de los activos de información.

Positiva Compañía de Seguros S.A. está comprometida con la confidencialidad, integridad y disponibilidad de la información de sus grupos de interés, es por ello que eligió como método de análisis y gestión de riesgos informáticos la Metodología MAGERIT[37] versión 3.0, la cual consta de 5 pasos, a saber:

1. Determinación de los activos relevantes para la organización y su valor.
2. Establecer amenazas a las que están expuestos los activos.
3. Fijar las salvaguardas actuales y su eficacia, frente a los riesgos.
4. Estipular el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia de la amenaza.

La metodología MARGERIT 3.0 se relaciona con la norma ISO/IEC 27001 de 2013 de tal manera, que permite establecer una guía para identificar amenazas y estimar el impacto y probabilidad de manera Cualitativa. Además, admite la definición de estrategias de protección y el plan de mitigación de riesgo, incluyendo los controles a implantar para realizar el tratamiento del riesgo.

[37] AREVALO, Oscar William. "Metodología de Análisis de Riesgo de la Empresa la Casa de las Baterías S.A de C.V" Trabajo de Grado Ingeniera. El Salvador: Universidad Tecnológica del Salvador. Facultad de Ingeniería. Desarrollo de Redes. 2009. 27 p. Recuperado de: http://docplayer.es/5026447-Metodologia-de-analisis-de-riesgo-de-la-empresa-la-casa-de-las-baterias-s-a-de-c-v-catedratico-ing-rodrigo-torres.html

9.1.2.1 Valoración de los activos

Dada la identificación de los activos de información, se procede a valorar el grado de importancia y criticidad para la compañía, teniendo en cuenta los siguientes parámetros:

•Dimensión en la que el activo es relevante

•Estimación de los Valores en cada dimensión

De acuerdo a la herramienta PILAR 5.4.8 los criterios de valoración son:

Ilustración 29 Criterios de valoración

Nivel	Criterio
10	Nivel 10
9	Nivel 9
8	Nivel 8(+)
7	Alto
6	Alto(-)
5	Medio(+)
4	Medio
3	Medio(-)
2	Bajo(+)
1	Bajo
0	Depreciable

Fuente: Herramienta PILAR 5.4.8

En tanto a las dimensiones se tiene:

[D] Disponibilidad
[I] Integridad de Datos
[C] Confidencialidad de los datos
[A] Autenticidad de los usuarios de la información
[T] Trazabilidad de la información y los datos

Tabla 28 Valoración de activos

		DIMENSIONES				
ACTIVOS		[D]	[I]	[C]	[A]	[T]
[HW] equipos informáticos (hardware)	Grandes equipos (11)		[9]	[9]	[9]	[9]
	Equipos de escritorio (350)		[7]	[7]	[7]	[7]
	portátiles (40)		[6]	[7]	[6]	[6]
	Almacena datos (5)			[7]	[7]	[7]
	Periféricos					[6]
	Medios de impresión (6)	[5]				[6]
	Escáner	[5]				
	Soporte de la red (7)			[7]	[7]	[7]
	Módems	[4]				[4]
	Conmutadores administrables (switch)	[4]				[4]
	Encaminadotes (router)	[6]				[6]
	Pasarelas (bridge)	[6]				[6]
	Cortafuegos		[7]	[7]	[7]	
	Punto de acceso Wireless	[7]				[7]
	Central telefónica	[7]				[7]
[SW] aplicaciones (software)	Sistema operativo Windows 7 profesional.					[5]
	Office 2013 licence OEM					[5]
	Antivirus Microsoft Security Essentials				[5]	[5]
	SISTEMA DE INFORMACIÓN DE RIESGOS LABORALES SIARP: Sistema de Información que soporta los procesos de Afiliaciones, Siniestros (Accidentes de trabajo y enfermedades		[7]		[7]	[7]
	SISTEMA DE SEGUROS SISE VIDA INDIVIDUAL Y VIDA COLECTIVO: Suscripción, Indemnización vida individual y Vida colectivo, gestión de la información contable y financiera de la Compañía.		[7]	[7]	[7]	[7]
	SARA: Gestión de información de empleados de planta de la compañía para registro y pago de nómina y parafiscales.			[7]		[7]
	SICO: Sistema e información para la gestión documental			[7]		[7]
	NEONWEB: Control del inventario Físico de la compañía			[7]		[7]
	GESCONT: Gestión de la Contratación			[7]		[7]
	PQR: Gestión de Peticiones Quejas y Reclamos					[6]
	MIDAS: Valorador del Portafolio de Inversión		[7]	[7]		[7]
	SIAN: Sistema de información para la administración de Nóminas de Pensionados originadas en Pensiones ley 100			[7]		[7]
	ARANDA: Herramienta de soporte y apoyo a usuarios, a través del software "HELP DESK ARANDA", a través del cual los usuarios de los sistemas de información reportan los incidentes y requerimientos para ser atendidos por las mesas de ayuda. Adicionalmente, se ha implementado un sistema software denominado		[7]	[7]	[7]	[7]
	ARANDA 360 - END POINT:, que se adquirió para cumplir con los requerimientos de seguridad informática solicitados en la Circular 052/07 de la Superintendencia Financiera para bloqueo de dispositivos, bloqueo de acceso a redes inalámbricas (WI-FI) e instalación de software entre otros.		[7]	[7]	[7]	[7]
	TEAM FOUNDATION SERVER (TFS): Sistema de información colaborativo, para realizar la Gestión de configuración y cambios a aplicativos y sistemas de la Compañía. Control de código fuente y		[7]	[7]	[7]	[7]

Tabla 28 (continuación)

ACTIVOS		DIMENSIONES				
		[D]	[I]	[C]	[A]	[T]
[S] Servicios	Pagos en Línea		[4]			[4]
	Afiliación ARL		[6]	[6]		[6]
	Aporte a Riesgos Laborales	[6]				[6]
	Gestión Positiva Crea	[6]				
	Positiva Cuida	[6]		[6]		
	Seguimiento Programas					[6]
	Otros Servicios en Línea:					
	Contratación- Registro de Proveedores					[6]
	Certificados de aportes	[6]				[6]
	Beneficios					[5]
	Servicios de Información- Fondo de Empleados					[5]
	Servicios al Ciudadano- Ofertas de Empleo	[5]				
	Aprobación charlas PyP	[5]				
	Archivos de consulta permanente expediente digital Asegurados y Pensionados ARL		[7]	[7]		[7]
	Almacenamiento de datos	[7]				[7]
	Transferencia de datos		[7]	[7]		[7]
	Servicio de directorio (1)				[7]	
	Gestión de identidades (2)			[7]	[7]	[7]
	Gestión de privilegios			[7]	[7]	[7]
[COM] redes de comunicaciones	Red telefónica	[4]			[7]	[7]
	ADSL	[4]				
	Punto a punto	[4]				
	Red inalámbrica			[6]		[7]
	Red local			[6]		[7]
	Internet	[8]	[7]	[7]	[8]	[8]
[AUX] equipamiento auxiliar	Fuentes de alimentación	[4]				
	Sistemas de alimentacion ininterrumpida	[4]				
	Generadores eléctricos	[4]				
	Equipos de control de temperatura y humedad	[4]				
	Cableado	[4]				
[Media] soportes de información	**Electrónicos**					
	Almacenamiento en red			[7]		[7]
	CD ROM			[2]		
	Dispositivos USB			[2]		
	DVD			[2]		
	Disco duro externo			[2]		
	No electrónicos					
	Material impreso			[2]		
	Material digitalizado			[2]		
[D] datos / información	Datos vitales (vital records) (1)		[7]	[7]	[7]	[7]
	Datos de interés para la administración					[7]
	Datos de gestión interna					[7]
	Voz	[2]				
	Multimedia	[2]				
	Código fuente		[7]	[9]		
	Código ejecutable		[7]	[9]		
	Datos de configuración		[7]		[7]	[7]
	Datos de prueba		[7]		[7]	[7]
[P] personal	Usuarios internos			[7]		
	Administradores de sistemas			[7]		
	Administradores de comunicaciones			[7]		
	Administradores de BBDD			[7]		
	Desarrolladores			[7]		
	Investigadores			[7]		
	Directivos			[6]		
[L] instalaciones	Áreas	[6]				
	Oficinas	[6]				
	Laboratorios de higiene y toxicología	[7]				[6]
	Edificio	[7]				[7]

Fuente: El autor

9.1.2.2 Caracterización de amenazas.

Esta fase consiste en establecer las amenazas que pueden afectar a cada activo.

Las amenazas son hechos que ocurren, y es importante que de todo lo que pueda ocurrir se conozca que puede pasarle y causar daño a los activos.

Según la herramienta PILAR las amenazas están categorizadas por grupos, a saber:

[N] Desastres naturales

[I] De origen Industrial

[E] Errores o fallos no intencionados

[A] Ataques intencionados

Tabla 29 Identificación de amenazas

ACTIVOS	AMENAZA
[HW] equipos informáticos (hardware)	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales [I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad. [I. 11] Emanaciones electromagnéticas [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.24] Caída del sistema por agotamiento de recursos [E.25] Pérdida de equipos [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.11] Acceso no autorizado [A.23] Manipulación de los equipos [A.24] Denegación de servicio [A.25] Robo

Tabla 29 (continuación)

ACTIVOS	AMENAZA
[SW] aplicaciones (software)	[E.1] Errores de los usuarios [E.2] Errores del administrador [E.8] Difusión de software dañino [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [E.15] Alteración accidental de la información [E.18] Destrucción de información [E.19] Fugas de información [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.11] Acceso no autorizado [A.15] Modificación deliberada de la información [A.18] Destrucción de información [A.19] Divulgación de información [A.22] Manipulación de programas
[S] Servicios	[E.1] Errores de los usuarios [E.2] Errores del administrador [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [E.15] Alteración accidental de la información [E.18] Destrucción de información [E.19] Fugas de información [E.24] Caída del sistema por agotamiento de recursos [A.5] Suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.9] [Re-]encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado [A.18] Destrucción de información [A.19] Divulgación de información [A.24] Denegación de servicio

Tabla 29 (continuación)

ACTIVOS	AMENAZA
[COM] redes de comunicaciones	[I.8] Fallos de comunicación [E.2] Errores del administrador [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [E.14] Escapes de información [E.15] Alteración accidental de la información [E.18] Destrucción de información [E.19] Fugas de información [E.24] Caída del sistema por agotamiento de recursos [A.5] Suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.9] [Re-]encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado [A.12] Análisis de tráfico [A.14] Interceptación de información (escucha) [A.15] Modificación deliberada de la información [A.19] Divulgación de información [A.24] Denegación de servicio
[AUX] equipamiento auxiliar	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales [I. 1.2.-*.3.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad. [I.9] Interrupción de otros suministros o servicios esenciales [I. 11] Emanaciones electromagnéticas [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.24] Caída del sistema por agotamiento de recursos [E.25] Pérdida de equipos [A.7] Uso no previsto [A.11] Acceso no autorizado [A.23] Manipulación de los equipos [A.25] Robo [A.26] Ataque destructivo

Tabla 29 (continuación)

ACTIVOS	AMENAZA
[Media] soportes de información	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales [I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad. [I.10] Degradación de los soportes de almacenamiento de la información [I. 11] Emanaciones electromagnéticas [E.1] Errores de los usuarios [E.2] Errores del administrador [E.15] Alteración accidental de la información [E.18] Destrucción de información [E.19] Fugas de información [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.25] Pérdida de equipos [A.7] Uso no previsto [A.11] Acceso no autorizado [A.15] Modificación deliberada de la información [A.18] Destrucción de información [A.19] Divulgación de información [A.25] Robo [A.26] Ataque destructivo
• [D] datos / información • [keys] claves criptográficas [D] Registros de actividad [D] Datos de configuración	[E. 1] Errores de los usuarios [E. 2] Errores de administración [E. 3. 4] Errores de configuración y monitorización [E.15] Alteración accidental de la información [E.18] Destrucción de información [E.19] Fugas de información [A.3] Manipulación de los registros de actividad (log) [A.4] Manipulación de la configuración [A.5] Suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado [A.15] Modificación deliberada de la información [A.18] Destrucción de información [A.19] Divulgación de información

Tabla 29 (continuación)

ACTIVOS	AMENAZA
[P] personal	[E. 7] Deficiencia en la organización [E. 19] Fugas de información [E. 28] Indisponibilidad del personal [A. 29] Extorsión [A.30] Ingeniería social (picaresca)
• [L] instalaciones	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales [I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad. [I. 11] Emanaciones electromagnéticas [E.15] Alteración accidental de la información [E.19] Fugas de información [E.18] Destrucción de información [A.11] Acceso no autorizado [A.15] Modificación deliberada de la información [A.18] Destrucción de información [A.19] Divulgación de información [A.26] Ataque destructivo

Fuente: El autor

9.1.2.3 Valoración de las amenazas

Se utilizan dos criterios, como son: degradación, que se refiere a cuan deteriorado resultaría el activo; y probabilidad, que se refiere a la factibilidad o imposibilidad de que se materialice la amenaza.

Con esta acción se pretende cumplir dos objetivos transcendentales a saber:

- Evaluar la probabilidad de ocurrencia de cada amenaza relacionada con cada activo.
- Preciar la degradación que causaría la realización de una amenaza en cada dimensión del activo.

Tabla 30 Medición de la degradación

Criterio			Ponderación
MA	Muy Alta	Daño muy grave	80-100%
A	Alta	Daño grave	60-79%
M	Media	Daño importante	40-59%
B	Baja	Daño menor	10-39%

Fuente: Magerit versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro III- Guía de Técnicas

Tabla 31 Probabilidad

SIGLAS	**Escala de valoración**
CS	Casi Seguro
MA	Muy alto
P	Posible
PP	Poco Probable
MB	Muy bajo
MR	Muy raro

Fuente: Magerit versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro III- Guía de Técnicas

Tabla 32 Valoración de amenazas y probabilidad de ocurrencia para los activos de información

			Nivel degradación				
			Ponderación				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
[HW] Equipos informáticos (hardware)							
Servidores	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	40%				59%
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego), contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	P	40%				59%
	[I. 11] Emanaciones electromagnéticas	PP	10%				10%
	[E.23] Errores de mantenimiento / actualización de equipos (hardw	MB	10%				10%
	[E.24] Caída del sistema por agotamiento de recursos	P	59%				65%
	[E.25] Pérdida de equipos	MR	10%				10%
	[A.6] Abuso de privilegios de acceso	MB	10%				10%
	[A.7] Uso no previsto	PP	10%				10%
	[A.11] Acceso no autorizado	P	59%				65%
	[A.23] Manipulación de los equipos	P	40%				65%
	[A.24] Denegación de servicio	P	50%				65%
	[A.25] Robo	MB	5%				5%
	[A.26] Ataque destructivo	P	60%				65%
Equipos de escritorio y portatiles	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	59%				65%
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego), contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	P	40%				40%
	[I. 11] Emanaciones electromagnéticas	PP	10%				10%
	[E.23] Errores de mantenimiento / actualización de equipos (hardw	MB	5%				5%
	[E.24] Caída del sistema por agotamiento de recursos	P	53%				53%
	[E.25] Pérdida de equipos	MR	5%				5%
	[A.6] Abuso de privilegios de acceso	MB	5%				5%
	[A.7] Uso no previsto	PP	10%				10%
	[A.11] Acceso no autorizado	P	40%				40%
	[A.23] Manipulación de los equipos	P	40%				40%
	[A.24] Denegación de servicio	P	40%				40%
	[A.25] Robo	MB	5%				5%
	[A.26] Ataque destructivo	P	40%				40%

Fuente: El autor

Tabla 32 (continuación)

			Nivel degradación				
			Ponderación				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Soporte de la red Modems Routers Encaminadores	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	40%				40%
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego), contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	P	40%				40%
	[I. 11] Emanaciones electromagnéticas	MB	5%				5%
	[E.23] Errores de mantenimiento / actualización de equipos (hardw	MB	5%				5%
	[E.25] Pérdida de equipos	PP	10%				10%
	[A.7] Uso no previsto	P	40%				40%
	[A.11] Acceso no autorizado	MB	5%				5%
	[A.23] Manipulación de los equipos	MB	5%				5%
[SW] aplicaciones (software)							
SIARP	[E.1] Errores de los usuarios	MA	80%	100%	90%	80%	
	[E.2] Errores del administrador	PP	5%	10%	10%	5%	
	[E.8] Difusión de softw are dañino	PP	5%	10%	10%	5%	
	[E.9] Errores de [re-]encaminamiento	MR	10%	10%	10%	10%	
	[E.10] Errores de secuencia	MR	10%	10%	10%	10%	
	[E.15] Alteración accidental de la información	MA	80%	100%	90%	80%	
	[E.18] Destrucción de información	P	50%	50%	50%	50%	
	[E.19] Fugas de información	P	50%	50%	50%	50%	
	[E.20] Vulnerabilidades de los programas (softw are)	CS	80%	90%	80%	100%	
	[E.21] Errores de mantenimiento / actualización de programas (sof	PP	5%	10%	10%	5%	
	[A.6] Abuso de privilegios de acceso	MA	80%	100%	90%	80%	
	[A.7] Uso no previsto	MA	80%	100%	90%	80%	
	[A.11] Acceso no autorizado	P	50%	50%	50%	50%	
	[A.15] Modificación deliberada de la información	MR	10%	10%	10%	10%	
	[A.18] Destrucción de información	P	50%	50%	50%	50%	
	[A.19] Divulgación de información	MB	10%	10%	10%	10%	
	[A.22] Manipulación de programas	P	50%	50%	50%	50%	

Tabla 32 (continuación)

			Nivel degradación				
			Ponderación				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
SISE	[E.1] Errores de los usuarios	MA	80%	100%	90%	80%	
	[E.2] Errores del administrador	PP	5%	10%	10%	5%	
	[E.8] Difusión de softw are dañino	PP	5%	10%	10%	5%	
	[E.9] Errores de [re-]encaminamiento	MR	10%	10%	10%	10%	
	[E.10] Errores de secuencia	MR	10%	10%	10%	10%	
	[E.15] Alteración accidental de la información	MA	80%	100%	90%	80%	
	[E.18] Destrucción de información	P	50%	50%	50%	50%	
	[E.19] Fugas de información	P	50%	50%	50%	50%	
	[E.20] Vulnerabilidades de los programas (softw are)	CS	80%	90%	80%	100%	
	[E.21] Errores de mantenimiento / actualización de programas (sof	PP	5%	10%	10%	5%	
	[A.6] Abuso de privilegios de acceso	MA	80%	100%	90%	80%	
	[A.7] Uso no previsto	MA	80%	100%	90%	80%	
	[A.11] Acceso no autorizado	P	50%	50%	50%	50%	
	[A.15] Modificación deliberada de la información	MR	10%	10%	10%	10%	
	[A.18] Destrucción de información	P	50%	50%	50%	50%	
	[A.19] Divulgación de información	MB	10%	10%	10%	10%	
	[A.22] Manipulación de programas	P	50%	50%	50%	50%	
SICO	[E.1] Errores de los usuarios	P	50%	50%	50%	50%	
	[E.2] Errores del administrador	PP	5%	10%	10%	5%	
	[E.8] Difusión de softw are dañino	MB	10%	10%	10%	10%	
	[E.9] Errores de [re-]encaminamiento	MR	10%	10%	10%	10%	
	[E.10] Errores de secuencia	MR	10%	10%	10%	10%	
	[E.15] Alteración accidental de la información	MB	10%	10%	10%	10%	
	[E.18] Destrucción de información	MB	10%	10%	10%	10%	
	[E.19] Fugas de información	PP	5%	10%	10%	5%	
	[E.20] Vulnerabilidades de los programas (softw are)	MB	10%	10%	10%	10%	
	[E.21] Errores de mantenimiento / actualización de programas (sof	PP	5%	10%	10%	5%	
	[A.6] Abuso de privilegios de acceso	MB	10%	10%	10%	10%	
	[A.7] Uso no previsto	MB	10%	10%	10%	10%	
	[A.11] Acceso no autorizado	PP	5%	10%	10%	5%	
	[A.15] Modificación deliberada de la información	MR	10%	10%	10%	10%	
	[A.18] Destrucción de información	PP	5%	10%	10%	5%	
	[A.19] Divulgación de información	MB	10%	10%	10%	10%	
	[A.22] Manipulación de programas	PP	5%	10%	10%	5%	

Tabla 32 (continuación)

			Nivel degradación				
			Ponderación				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
SARA	[E.1] Errores de los usuarios	MA	80%	100%	90%	80%	
	[E.2] Errores del administrador	PP	5%	10%	10%	5%	
	[E.8] Difusión de softw are dañino	PP	5%	10%	10%	5%	
	[E.9] Errores de [re-]encaminamiento	MR	10%	10%	10%	10%	
	[E.10] Errores de secuencia	MR	10%	10%	10%	10%	
	[E.15] Alteración accidental de la información	MA	80%	100%	90%	80%	
	[E.18] Destrucción de información	P	50%	50%	50%	50%	
	[E.19] Fugas de información	P	50%	50%	50%	50%	
	[E.20] Vulnerabilidades de los programas (softw are)	CS	80%	90%	80%	100%	
	[E.21] Errores de mantenimiento / actualización de programas (sof	PP	5%	10%	10%	5%	
	[A.6] Abuso de privilegios de acceso	MA	80%	100%	90%	80%	
	[A.7] Uso no previsto	MA	80%	100%	90%	80%	
	[A.11] Acceso no autorizado	P	50%	50%	50%	50%	
	[A.15] Modificación deliberada de la información	MR	10%	10%	10%	10%	
	[A.18] Destrucción de información	P	50%	50%	50%	50%	
	[A.19] Divulgación de información	P	50%	50%	50%	50%	
	[A.22] Manipulación de programas	P	50%	50%	50%	50%	
NEON WEB	[E.1] Errores de los usuarios	P	50%	50%	50%	50%	
	[E.2] Errores del administrador	PP	5%	10%	10%	5%	
	[E.8] Difusión de softw are dañino	PP	5%	10%	10%	5%	
	[E.9] Errores de [re-]encaminamiento	MR	10%	10%	10%	10%	
	[E.10] Errores de secuencia	MR	10%	10%	10%	10%	
	[E.15] Alteración accidental de la información	MA	80%	100%	90%	80%	
	[E.18] Destrucción de información	P	50%	50%	50%	50%	
	[E.19] Fugas de información	P	50%	50%	50%	50%	
	[E.20] Vulnerabilidades de los programas (softw are)	CS	80%	90%	80%	100%	
	[E.21] Errores de mantenimiento / actualización de programas (sof	PP	5%	10%	10%	5%	
	[A.6] Abuso de privilegios de acceso	MA	80%	100%	90%	80%	
	[A.7] Uso no previsto	MA	80%	100%	90%	80%	
	[A.11] Acceso no autorizado	P	50%	50%	50%	50%	
	[A.15] Modificación deliberada de la información	MR	10%	10%	10%	10%	
	[A.18] Destrucción de información	P	50%	50%	50%	50%	
	[A.19] Divulgación de información	MB	10%	10%	10%	10%	
	[A.22] Manipulación de programas	P	50%	50%	50%	50%	

Tabla 32 (continuación)

			Nivel degradación				
			Ponderación				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
SIAN	[E.1] Errores de los usuarios	P	50%	50%	50%	50%	
	[E.2] Errores del administrador	PP	5%	10%	10%	5%	
	[E.8] Difusión de softw are dañino	PP	5%	10%	10%	5%	
	[E.9] Errores de [re-]encaminamiento	MR	10%	10%	10%	10%	
	[E.10] Errores de secuencia	MR	10%	10%	10%	10%	
	[E.15] Alteración accidental de la información	MA	80%	100%	90%	80%	
	[E.18] Destrucción de información	P	50%	50%	50%	50%	
	[E.19] Fugas de información	P	50%	50%	50%	50%	
	[E.20] Vulnerabilidades de los programas (softw are)	CS	80%	90%	80%	100%	
	[E.21] Errores de mantenimiento / actualización de programas (sof	PP	5%	10%	10%	5%	
	[A.6] Abuso de privilegios de acceso	MA	80%	100%	90%	80%	
	[A.7] Uso no previsto	MA	80%	100%	90%	80%	
	[A.11] Acceso no autorizado	P	50%	50%	50%	50%	
	[A.15] Modificación deliberada de la información	MR	10%	10%	10%	10%	
	[A.18] Destrucción de información	P	50%	50%	50%	50%	
	[A.19] Divulgación de información	B	10%	5%	10%	5%	
	[A.22] Manipulación de programas	P	50%	50%	50%	50%	
MIDAS	[E.1] Errores de los usuarios	MA	80%	100%	90%	80%	
	[E.2] Errores del administrador	PP	5%	10%	10%	5%	
	[E.8] Difusión de softw are dañino	PP	5%	10%	10%	5%	
	[E.9] Errores de [re-]encaminamiento	MR	10%	10%	10%	10%	
	[E.10] Errores de secuencia	MR	10%	10%	10%	10%	
	[E.15] Alteración accidental de la información	B	10%	5%	10%	5%	
	[E.18] Destrucción de información	P	50%	50%	50%	50%	
	[E.19] Fugas de información	P	50%	50%	50%	50%	
	[E.20] Vulnerabilidades de los programas (softw are)	MB	10%	10%	10%	10%	
	[E.21] Errores de mantenimiento / actualización de programas (sof	PP	5%	10%	10%	5%	
	[A.6] Abuso de privilegios de acceso	B	10%	5%	10%	5%	
	[A.7] Uso no previsto	MB	10%	10%	10%	10%	
	[A.11] Acceso no autorizado	P	50%	50%	50%	50%	
	[A.15] Modificación deliberada de la información	MR	10%	10%	10%	10%	
	[A.18] Destrucción de información	B	10%	5%	10%	5%	
	[A.19] Divulgación de información	MB	10%	10%	10%	10%	
	[A.22] Manipulación de programas	MB	10%	10%	10%	10%	

Tabla 32 (continuación)

			Nivel degradación				
			Ponderación				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
ARANDA	[E.1] Errores de los usuarios	P	50%	50%	50%	50%	
	[E.2] Errores del administrador	MB	10%	10%	10%	10%	
	[E.8] Difusión de softw are dañino	B	10%	5%	10%	5%	
	[E.9] Errores de [re-]encaminamiento	B	10%	5%	10%	5%	
	[E.10] Errores de secuencia	B	10%	5%	10%	5%	
	[E.15] Alteración accidental de la información	B	10%	5%	10%	5%	
	[E.18] Destrucción de información	MB	10%	10%	10%	10%	
	[E.19] Fugas de información	MB	10%	10%	10%	10%	
	[E.20] Vulnerabilidades de los programas (softw are)	MB	10%	10%	10%	10%	
	[E.21] Errores de mantenimiento / actualización de programas (sof	MB	10%	10%	10%	10%	
	[A.6] Abuso de privilegios de acceso	B	10%	5%	10%	5%	
	[A.7] Uso no previsto	B	10%	5%	10%	5%	
	[A.11] Acceso no autorizado	B	10%	5%	10%	5%	
	[A.15] Modificación deliberada de la información	B	10%	5%	10%	5%	
	[A.18] Destrucción de información	B	10%	5%	10%	5%	
	[A.19] Divulgación de información	B	10%	5%	10%	5%	
	[A.22] Manipulación de programas	B	10%	5%	10%	5%	
TFS	[E.1] Errores de los usuarios	P	50%	50%	50%	50%	
	[E.2] Errores del administrador	MB	10%	10%	10%	10%	
	[E.8] Difusión de softw are dañino	B	10%	5%	10%	5%	
	[E.9] Errores de [re-]encaminamiento	B	10%	5%	10%	5%	
	[E.10] Errores de secuencia	B	10%	5%	10%	5%	
	[E.15] Alteración accidental de la información	B	10%	5%	10%	5%	
	[E.18] Destrucción de información	MB	10%	10%	10%	10%	
	[E.19] Fugas de información	MB	10%	10%	10%	10%	
	[E.20] Vulnerabilidades de los programas (softw are)	MB	10%	10%	10%	10%	
	[E.21] Errores de mantenimiento / actualización de programas (sof	MB	10%	10%	10%	10%	
	[A.6] Abuso de privilegios de acceso	B	10%	5%	10%	5%	
	[A.7] Uso no previsto	B	10%	5%	10%	5%	
	[A.11] Acceso no autorizado	B	10%	5%	10%	5%	
	[A.15] Modificación deliberada de la información	B	10%	5%	10%	5%	
	[A.18] Destrucción de información	B	10%	5%	10%	5%	
	[A.19] Divulgación de información	B	10%	5%	10%	5%	
	[A.22] Manipulación de programas	B	10%	5%	10%	5%	

Tabla 32 (continuación)

			Nivel degradación				
			Ponderación				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
[S] Servicios							
Gestión de identidades	[E.1] Errores de los usuarios	P		69%		69%	
	[E.2] Errores del administrador	PP		10%		5%	
	[E.9] Errores de [re-]encaminamiento	PP		10%		5%	
	[E.10] Errores de secuencia	PP		10%		5%	
	[E.15] Alteración accidental de la información	CS		69%		80%	
	[E.18] Destrucción de información	MA		80%		90%	
	[E.19] Fugas de información	MA		80%		90%	
	[E.24] Caída del sistema por agotamiento de recursos	MA		80%		90%	
	[A.5] Suplantación de la identidad del usuario	P		69%		69%	
	[A.6] Abuso de privilegios de acceso	P		69%		69%	
	[A.7] Uso no previsto	P		69%		69%	
	[A.9] [Re-]encaminamiento de mensajes	PP		5%		5%	
	[A.10] Alteración de secuencia	MB		10%		10%	
	[A.11] Acceso no autorizado	MA		80%		90%	
	[A.18] Destrucción de información	PP		5%		5%	
	[A.19] Divulgación de información	P		69%		69%	
	[A.24] Denegación de servicio	MA		80%		90%	
Gestión de Privilegios	[E.1] Errores de los usuarios	P		69%		69%	
	[E.2] Errores del administrador	PP		5%		5%	
	[E.9] Errores de [re-]encaminamiento	PP		5%		5%	
	[E.10] Errores de secuencia	PP		5%		5%	
	[E.15] Alteración accidental de la información	CS		80%		80%	
	[E.18] Destrucción de información	MA		80%		90%	
	[E.19] Fugas de información	MA		80%		90%	
	[E.24] Caída del sistema por agotamiento de recursos	MA		80%		90%	
	[A.5] Suplantación de la identidad del usuario	P		69%		69%	
	[A.6] Abuso de privilegios de acceso	P		69%		69%	
	[A.7] Uso no previsto	P		69%		69%	
	[A.9] [Re-]encaminamiento de mensajes	PP		5%		5%	
	[A.10] Alteración de secuencia	MB		10%		10%	
	[A.11] Acceso no autorizado	MA		80%		90%	
	[A.18] Destrucción de información	PP		5%		5%	
	[A.19] Divulgación de información	P		69%		69%	
	[A.24] Denegación de servicio	MA		80%		90%	

Tabla 32 (continuación)

			Nivel degradación				
			Ponderación				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Servicio de directorio	[E.1] Errores de los usuarios	PP		5%		5%	
	[E.2] Errores del administrador	PP		5%		5%	
	[E.9] Errores de [re-]encaminamiento	PP		5%		5%	
	[E.10] Errores de secuencia	PP		5%		5%	
	[E.15] Alteración accidental de la información	MR		10%		10%	5%
	[E.18] Destrucción de información	MB		10%		10%	5%
	[E.19] Fugas de información	MB		10%		10%	5%
	[E.24] Caída del sistema por agotamiento de recursos	MB		10%		10%	5%
	[A.5] Suplantación de la identidad del usuario	P		40%		40%	40%
	[A.6] Abuso de privilegios de acceso	P		40%		40%	40%
	[A.7] Uso no previsto	P		40%		40%	40%
	[A.9] [Re-]encaminamiento de mensajes	PP		5%		5%	10%
	[A.10] Alteración de secuencia	MB		10%		10%	5%
	[A.11] Acceso no autorizado	MA		80%		90%	100%
	[A.18] Destrucción de información	PP		5%		5%	10%
	[A.19] Divulgación de información	P		40%		40%	40%
	[A.24] Denegación de servicio	MA		80%		90%	100%
Página Web	[E.1] Errores de los usuarios	P		50%	60%		69%
	[E.2] Errores del administrador	MB		10%	10%		5%
	[E.9] Errores de [re-]encaminamiento	MR		10%	10%		5%
	[E.10] Errores de secuencia	MR		10%	10%		5%
	[E.15] Alteración accidental de la información	PP		10%	5%		5%
	[E.18] Destrucción de información	P		50%	60%		69%
	[E.19] Fugas de información	P		50%	60%		69%
	[E.24] Caída del sistema por agotamiento de recursos	P		50%	60%		69%
	[A.5] Suplantación de la identidad del usuario	P		50%	60%		69%
	[A.6] Abuso de privilegios de acceso	MB		10%	10%		5%
	[A.7] Uso no previsto	PP		10%	5%		5%
	[A.9] [Re-]encaminamiento de mensajes	P		50%	60%		69%
	[A.10] Alteración de secuencia	MR		10%	10%		5%
	[A.11] Acceso no autorizado	P		50%	60%		69%
	[A.18] Destrucción de información	P		50%	60%		69%
	[A.19] Divulgación de información	MB		10%	10%		5%
	[A.24] Denegación de servicio	P		50%	60%		69%

Tabla 32 (continuación)

			Nivel degradación				
			Ponderación				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
[COM] Redes de comunicaciones							
Red Local	[I.8] Fallos de comunicación	MA	80%				80%
	[E.2] Errores del administrador	MB	5%				10%
	[E.9] Errores de [re-]encaminamiento	MR	5%				10%
	[E.10] Errores de secuencia	MR	5%				10%
	[E.14] Escapes de información	MB	5%				10%
	[E.15] Alteración accidental de la información	PP		10%			10%
	[E.18] Destrucción de información	P	60%				50%
	[E.19] Fugas de información	P	60%				50%
	[E.24] Caída del sistema por agotamiento de recursos	P	60%				50%
	[A.5] Suplantación de la identidad del usuario	P	60%				50%
	[A.6] Abuso de privilegios de acceso	MB	5%				10%
	[A.7] Uso no previsto	MB	5%				10%
	[A.9] [Re-]encaminamiento de mensajes	P	60%				50%
	[A.10] Alteración de secuencia	MR	5%				10%
	[A.11] Acceso no autorizado	P	60%				50%
	[A.12] Análisis de tráfico	MB	5%				10%
	[A.14] Interceptación de información (escucha)	PP		10%			10%
	[A.15] Modificación deliberada de la información	MR	5%				10%
	[A.19] Divulgación de información	MB	5%				10%
	[A.24] Denegación de servicio	P	60%				50%
Red Inhalambrica	[I.8] Fallos de comunicación	P	60%				50%
	[E.2] Errores del administrador	MB	5%				10%
	[E.9] Errores de [re-]encaminamiento	MR	5%				10%
	[E.10] Errores de secuencia	MR	5%				10%
	[E.14] Escapes de información	MB	5%				10%
	[E.15] Alteración accidental de la información	PP		10%			10%
	[E.18] Destrucción de información	P	60%				50%
	[E.19] Fugas de información	P	60%				50%
	[E.24] Caída del sistema por agotamiento de recursos	P	60%				50%
	[A.5] Suplantación de la identidad del usuario	P	60%				50%
	[A.6] Abuso de privilegios de acceso	MB	5%				10%
	[A.7] Uso no previsto	MB	5%				10%
	[A.9] [Re-]encaminamiento de mensajes	P	60%				50%
	[A.10] Alteración de secuencia	MR	5%				10%
	[A.11] Acceso no autorizado	P	60%				50%
	[A.12] Análisis de tráfico	MB	5%				10%
	[A.14] Interceptación de información (escucha)	PP		10%			10%
	[A.15] Modificación deliberada de la información	MR	5%				10%
	[A.19] Divulgación de información	MB	5%				10%
	[A.24] Denegación de servicio	P	60%				50%

Tabla 32 (continuación)

			Nivel degradación				
			Ponderación				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Red Telefónica	[I.8] Fallos de comunicación	MA	90%				80%
	[E.2] Errores del administrador	MB	5%				10%
	[E.9] Errores de [re-]encaminamiento	MR	5%				10%
	[E.10] Errores de secuencia	MR	5%				10%
	[E.14] Escapes de información	MB	5%				10%
	[E.15] Alteración accidental de la información	PP		10%			10%
	[E.18] Destrucción de información	P	60%				50%
	[E.19] Fugas de información	P	60%				50%
	[E.24] Caída del sistema por agotamiento de recursos	P	60%				50%
	[A.5] Suplantación de la identidad del usuario	P	60%				50%
	[A.6] Abuso de privilegios de acceso	MB	5%				10%
	[A.7] Uso no previsto	MB	5%				10%
	[A.9] [Re-]encaminamiento de mensajes	P	60%				50%
	[A.10] Alteración de secuencia	MR	5%				10%
	[A.11] Acceso no autorizado	P	60%				50%
	[A.12] Análisis de tráfico	MB	5%				10%
	[A.14] Interceptación de información (escucha)	PP		10%			10%
	[A.15] Modificación deliberada de la información	MR	5%				10%
	[A.19] Divulgación de información	MB	5%				10%
	[A.24] Denegación de servicio	P	60%				50%
Internet	[I.8] Fallos de comunicación	P	60%				50%
	[E.2] Errores del administrador	MB	5%				10%
	[E.9] Errores de [re-]encaminamiento	MR	5%				10%
	[E.10] Errores de secuencia	MR	5%				10%
	[E.14] Escapes de información	MB	5%				10%
	[E.15] Alteración accidental de la información	PP		10%			10%
	[E.18] Destrucción de información	P	60%				50%
	[E.19] Fugas de información	P	60%				50%
	[E.24] Caída del sistema por agotamiento de recursos	P	60%				50%
	[A.5] Suplantación de la identidad del usuario	P	60%				50%
	[A.6] Abuso de privilegios de acceso	MB	5%				10%
	[A.7] Uso no previsto	MB	5%				10%
	[A.9] [Re-]encaminamiento de mensajes	P	60%				50%
	[A.10] Alteración de secuencia	MR	5%				10%
	[A.11] Acceso no autorizado	P	60%				50%
	[A.12] Análisis de tráfico	MB	5%				10%
	[A.14] Interceptación de información (escucha)	PP		10%			10%
	[A.15] Modificación deliberada de la información	MR	5%				10%
	[A.19] Divulgación de información	MB	5%				10%
	[A.24] Denegación de servicio	P	60%				50%

Tabla 32 (continuación)

			Nivel degradación				
			Ponderación				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
[AUX] Equipamiento auxiliar							
Sistema de alimentación ininterrumpida	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	40%				
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	PP		10%			
	[I.9] Interrupción de otros suministros o servicios esenciales	P	40%				
	[I. 11] Emanaciones electromagnéticas	PP		10%			
	[E.23] Errores de mantenimiento / actualización de equipos (hardw	MB	5%				
	[E.24] Caída del sistema por agotamiento de recursos	MB	5%				
	[E.25] Pérdida de equipos	B	5%				
	[A.7] Uso no previsto	B	5%				
	[A.11] Acceso no autorizado	B	5%				
	[A.23] Manipulación de los equipos	B	5%				
	[A.25] Robo	MB	5%				
	[A.26] Ataque destructivo	MB	5%				
Equipo de climatización	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	40%				
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	PP		10%			
	[I.9] Interrupción de otros suministros o servicios esenciales	P	40%				
	[I. 11] Emanaciones electromagnéticas	PP		10%			
	[E.23] Errores de mantenimiento / actualización de equipos (hardw	MB	5%				
	[E.24] Caída del sistema por agotamiento de recursos	MB	5%				
	[E.25] Pérdida de equipos	B	5%				
	[A.7] Uso no previsto	B	5%				
	[A.11] Acceso no autorizado	B	5%				
	[A.23] Manipulación de los equipos	B	5%				
	[A.25] Robo	MB	5%				
	[A.26] Ataque destructivo	MB	5%				
Cableado	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	40%				
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	PP		10%			
	[I.9] Interrupción de otros suministros o servicios esenciales	P	40%				
	[I. 11] Emanaciones electromagnéticas	PP		10%			
	[E.23] Errores de mantenimiento / actualización de equipos (hardw	MB	5%				
	[E.24] Caída del sistema por agotamiento de recursos	MB	5%				
	[E.25] Pérdida de equipos	B	5%				
	[A.7] Uso no previsto	B	5%				
	[A.11] Acceso no autorizado	B	5%				
	[A.23] Manipulación de los equipos	B	5%				
	[A.25] Robo	MB	5%				
	[A.26] Ataque destructivo	MB	5%				

Tabla 32 (continuación)

			Nivel degradación				
			Ponderación				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Generadores electricos	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	40%				
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	P	40%				
	[I.9] Interrupción de otros suministros o servicios esenciales	P	40%				
	[I. 11] Emanaciones electromagnéticas	PP		10%			
	[E.23] Errores de mantenimiento / actualización de equipos (hardw	MB	5%				
	[E.24] Caída del sistema por agotamiento de recursos	P	40%				
	[E.25] Pérdida de equipos	MR	5%				
	[A.7] Uso no previsto	MB	5%				
	[A.11] Acceso no autorizado	P	40%				
	[A.23] Manipulación de los equipos	P	40%				
	[A.25] Robo	MB	5%				
	[A.26] Ataque destructivo	PP		10%			
[SI] Soportes de información							
Almacenamiento en red DVD CD USB	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P			40%		
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	P			40%		
	[I.10] Degradación de los soportes de almacenamiento de la inforr	PP			5%		
	[I. 11] Emanaciones electromagnéticas	PP			5%		
	[E.1] Errores de los usuarios	P			60%		
	[E.2] Errores del administrador	MB			10%		
	[E.15] Alteración accidental de la información	PP			5%		
	[E.18] Destrucción de información	P			60%		
	[E.19] Fugas de información	P			60%		
	[E.23] Errores de mantenimiento / actualización de equipos (hardw	MB			10%		
	[E.25] Pérdida de equipos	MR			10%		
	[A.7] Uso no previsto	MB			10%		
	[A.11] Acceso no autorizado	P			60%		
	[A.15] Modificación deliberada de la información	MB			10%		
	[A.18] Destrucción de información	P			60%		
	[A.19] Divulgación de información	MB			10%		
	[A.25] Robo	PP			5%		
	[A.26] Ataque destructivo	MB			10%		

Tabla 32 (continuación)

			Nivel degradación				
			Ponderación				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Material impreso o digitalizado	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P			60%		
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	P			60%		
	[I.10] Degradación de los soportes de almacenamiento de la inforr	PP			5%		
	[I. 11] Emanaciones electromagnéticas	PP			5%		
	[E.1] Errores de los usuarios	P			60%		
	[E.2] Errores del administrador	MB			10%		
	[E.15] Alteración accidental de la información	PP			5%		
	[E.18] Destrucción de información	P			60%		
	[E.19] Fugas de información	P			60%		
	[E.23] Errores de mantenimiento / actualización de equipos (hardw	MB			10%		
	[E.25] Pérdida de equipos	MR			10%		
	[A.7] Uso no previsto	MB			10%		
	[A.11] Acceso no autorizado	P			60%		
	[A.15] Modificación deliberada de la información	MB			10%		
	[A.18] Destrucción de información	P			60%		
	[A.19] Divulgación de información	MB			10%		
	[A.25] Robo	PP			5%		
	[A.26] Ataque destructivo	MB			10%		
[D] Datos / Información							
Datos vitales	[E. 1] Errores de los usuarios	MA	80%	80%	80%		
	[E. 2] Errores de administración	P	50%	40%	60%		
	[E. 3. 4] Errores de configuración y monitorización	P	50%	40%	60%		
	[E.15] Alteración accidental de la información	P	50%	40%	60%		
	[E.18] Destrucción de información	P	50%	40%	60%		
	[E.19] Fugas de información	P	50%	40%	60%		
	[A.3] Manipulación de los registros de actividad (log)	PP	5%	5%	5%		
	[A.4] Manipulación de la configuración	PP	5%	5%	5%		
	[A.5] Suplantación de la identidad del usuario	P	50%	40%	60%		
	[A.6] Abuso de privilegios de acceso	P	50%	40%	60%		
	[A.11] Acceso no autorizado	P	50%	40%	60%		
	[A.15] Modificación deliberada de la información	PP	5%	5%	5%		
	[A.18] Destrucción de información	PP	5%	5%	5%		
	[A.19] Divulgación de información	MB	5%	5%	5%		

Tabla 32 (continuación)

			Nivel degradación				
			Ponderación				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Código fuente	[E. 1] Errores de los usuarios	PP	5%	5%	5%		
	[E. 2] Errores de administración	PP	5%	5%	5%		
	[E. 3. 4] Errores de configuración y monitorización	PP	5%	5%	5%		
	[E.15] Alteración accidental de la información	MA	80%	80%	80%		
	[E.18] Destrucción de información	P	50%	40%	60%		
	[E.19] Fugas de información	P	50%	40%	60%		
	[A.3] Manipulación de los registros de actividad (log)	P	50%	40%	60%		
	[A.4] Manipulación de la configuración	P	50%	40%	60%		
	[A.5] Suplantación de la identidad del usuario	P	50%	40%	60%		
	[A.6] Abuso de privilegios de acceso	P	50%	40%	60%		
	[A.11] Acceso no autorizado	P	50%	40%	60%		
	[A.15] Modificación deliberada de la información	PP	5%	5%	5%		
	[A.18] Destrucción de información	PP	5%	5%	5%		
	[A.19] Divulgación de información	PP	5%	5%	5%		
Código ejecutable	[E. 1] Errores de los usuarios	PP	5%	5%	5%		
	[E. 2] Errores de administración	PP	5%	5%	5%		
	[E. 3. 4] Errores de configuración y monitorización	PP	5%	5%	5%		
	[E.15] Alteración accidental de la información	MA	80%	80%	80%		
	[E.18] Destrucción de información	P	50%	40%	60%		
	[E.19] Fugas de información	P	50%	40%	60%		
	[A.3] Manipulación de los registros de actividad (log)	P	50%	40%	60%		
	[A.4] Manipulación de la configuración	P	50%	40%	60%		
	[A.5] Suplantación de la identidad del usuario	P	50%	40%	60%		
	[A.6] Abuso de privilegios de acceso	P	50%	40%	60%		
	[A.11] Acceso no autorizado	P	50%	40%	60%		
	[A.15] Modificación deliberada de la información	PP	5%	5%	5%		
	[A.18] Destrucción de información	PP	5%	5%	5%		
	[A.19] Divulgación de información	PP	5%	5%	5%		
Datos de prueba	[E. 1] Errores de los usuarios	P	50%	40%	60%		
	[E. 2] Errores de administración	PP	5%	5%	5%		
	[E. 3. 4] Errores de configuración y monitorización	PP	5%	5%	5%		
	[E.15] Alteración accidental de la información	PP	5%	5%	5%		
	[E.18] Destrucción de información	P	50%	40%	60%		
	[E.19] Fugas de información	P	50%	40%	60%		
	[A.3] Manipulación de los registros de actividad (log)	P	50%	40%	60%		
	[A.4] Manipulación de la configuración	P	50%	40%	60%		
	[A.5] Suplantación de la identidad del usuario	P	50%	40%	60%		
	[A.6] Abuso de privilegios de acceso	MB	5%	5%	5%		
	[A.11] Acceso no autorizado	P	50%	40%	60%		
	[A.15] Modificación deliberada de la información	MB	5%	5%	5%		
	[A.18] Destrucción de información	P	50%	40%	60%		
	[A.19] Divulgación de información	MB	5%	5%	5%		

Tabla 32 (continuación)

			Nivel degradación				
			Ponderación				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
[P] Persona							
Usuarios internos y externos	[E. 7] Deficiencia en la organización	PP	5%	5%	5%		
	[E. 19] Fugas de información	PP	5%	5%	5%		
	[E. 28] Indisponibilidad del personal	P	50%	40%	60%		
	[A. 29] Extorsión	MB	5%	5%	5%		
	[A.30] Ingeniería social (picaresca)	P	50%	40%	60%		
[L] Instalaciones							
Centro Principal de procesamiento	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	40%				
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	P	40%				
	[I. 11] Emanaciones electromagnéticas	PP	10%				
	[E.15] Alteración accidental de la información	PP	10%				
	[E.19] Fugas de información	P	60%				
	[E.18] Destrucción de información	P	60%				
	[A.11] Acceso no autorizado	PP	10%				
	[A.15] Modificación deliberada de la información	MB	10%				
	[A.18] Destrucción de información	MB	10%				
	[A.19] Divulgación de información	MB	10%				
	[A.26] Ataque destructivo	PP	10%				
Centro Alterno de procesamiento	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	60%				
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	P	60%				
	[I. 11] Emanaciones electromagnéticas	PP	10%				
	[E.15] Alteración accidental de la información	PP	10%				
	[E.19] Fugas de información	P	60%				
	[E.18] Destrucción de información	P	60%				
	[A.11] Acceso no autorizado	PP	10%				
	[A.15] Modificación deliberada de la información	MB	10%				
	[A.18] Destrucción de información	MB	10%				
	[A.19] Divulgación de información	MB	10%				
	[A.26] Ataque destructivo	PP	10%				
Edificio Casa Matriz	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	60%				
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	P	60%				
	[I. 11] Emanaciones electromagnéticas	PP	10%				
	[E.15] Alteración accidental de la información	PP	10%				
	[E.19] Fugas de información	P	60%				
	[E.18] Destrucción de información	P	60%				
	[A.11] Acceso no autorizado	PP	10%				
	[A.15] Modificación deliberada de la información	MB	10%				
	[A.18] Destrucción de información	MB	10%				
	[A.19] Divulgación de información	MB	10%				
	[A.26] Ataque destructivo	PP	10%				

9.1.2.4 Evaluación y gestión del riesgo

- Identificación, análisis y evaluación de riesgos

Una vez realizado el análisis anterior se procede a reconocer la existencia de riesgos que pueden afectar significativamente la operación de la entidad o en su defecto registrar afectaciones leves.

Para esto es necesario, primero identificar las posibles causas de los riesgos empresariales, así como la diversidad de efectos a afrontar. En segunda medida para realizar una adecuada identificación de riesgos es necesario conocer detalladamente la organización así como el mercado en el que gestiona sus negocios, su entorno legal, social, político y cultural.

Las fuentes apropiadas para la identificación de riesgos son aquellos espacios internos o externos que pueden generar amenazas. El procedimiento se basa en cuestionarse que amenazas o vulnerabilidades existen por cada una.

9.1.2.4.1 Caracterización de riesgos

Con el fin de identificar los riesgos que pueden afectar los activos de información de Casa Matriz, se elaboró el registro de una serie de riesgos y los principios afectados como lo son la confidencialidad, disponibilidad, integridad y trazabilidad.

Tabla 33 Tipificación de riesgos

RIESGO	**PRINCIPIOS AFECTADOS**			
	C	**I**	**D**	**T**
Abuso de privilegios de acceso	X	X		X
Acceso no autorizado	X	X		
Debilidad en las auditorias				X
Cambio de privilegios sin autorización	X	X	X	
Denegación del servicio			X	X
Divulgación o robo de información de autenticación	X			

Tabla 33 (continuación)

RIESGO	PRINCIPIOS AFECTADOS			
	C	I	D	T
Divulgación no autorizada de información del negocio	X			
Ejecución de ingeniería social	X			
Errores del administrador de los sistemas de información	X	X	X	X
Instalación de software no autorizado		X	X	X
Interceptación de información en tránsito no autorizada	X			
Manipulación de la configuración	X			X
Modificación sin autorización		X		
Pérdida o robo de información	X		X	
Suplantación de identidad de los usuarios	X	X		X
Uso inadecuado de sistemas de información para generar fraudes	X	X		
Uso inadecuado de sistemas que generan interrupción			X	

Fuente: El autor

9.1.2.4.2 Matriz de riesgos

La matriz de riesgos es la base esencial del análisis de riesgos, esta es una herramienta grafica que permite analizar y determinar los riegos en el manejo de la información y los datos de la entidad. Los elementos de la matriz corresponden a la fórmula de **riesgo= Probabilidad de amenaza X magnitud del daño.**

La probabilidad de amenaza para el caso específico está determinado por los criterios relacionados en la Tabla No. 31 Probabilidad.

En tanto a la magnitud o impacto del riesgo sobre el activo, este este es el resultado mediante la criticidad del activo y el nivel de degradación cuando es afectada en algunas de las dimensiones. Mediante la tabla relacionada a continuación se especifica los parámetros para esta actividad.

Tabla 34 Estimación del impacto

Impacto			Degradación				
			1%	10%	50%	80%	100%
Valor	9 a 10	MA	M	A	A	MA	MA
	7 a 8	A	B	M	M	A	A
	4 a 6	M	MB	B	B	M	M
	1 a 3	B	MB	MB	MB	B	B
	0	MB	MB	MB	MB	MB	MB

Fuente: El autor

En las tablas posteriores se evidencia la magnitud del daño sobre cada activo de información y las dimensiones que afecta:

Tabla 35 Impacto sobre los activos de información

			Impacto				
			Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
[HW] Equipos informáticos (hardware)							
Servidores	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	M				M
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego), contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	P	M				M
	[I. 11] Emanaciones electromagnéticas	PP	B				B
	[E.23] Errores de mantenimiento / actualización de equipos (hardw	MB	B				B
	[E.24] Caída del sistema por agotamiento de recursos	P	M				M
	[E.25] Pérdida de equipos	MR	B				B
	[A.6] Abuso de privilegios de acceso	MB	B				B
	[A.7] Uso no previsto	PP	B				B
	[A.11] Acceso no autorizado	P	A				M
	[A.23] Manipulación de los equipos	P	A				M
	[A.24] Denegación de servicio	P	A				M
	[A.25] Robo	MB	B				B
	[A.26] Ataque destructivo	P	M				M

Tabla 35 (continuación)

			Impacto				
			Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Equipos de escritorio y portatiles	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	M				M
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego), contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	P	M				M
	[I. 11] Emanaciones electromagnéticas	PP	B				B
	[E.23] Errores de mantenimiento / actualización de equipos (hardw	MB	B				B
	[E.24] Caída del sistema por agotamiento de recursos	P	M				M
	[E.25] Pérdida de equipos	MR	B				B
	[A.6] Abuso de privilegios de acceso	MB	B				B
	[A.7] Uso no previsto	PP	B				B
	[A.11] Acceso no autorizado	P	A				M
	[A.23] Manipulación de los equipos	P	A				M
	[A.24] Denegación de servicio	P	A				M
	[A.25] Robo	MB	B				B
	[A.26] Ataque destructivo	P	M				M
Soporte de la red Modems Routers Encaminadores	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	M				M
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego), contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	P	M				M
	[I. 11] Emanaciones electromagnéticas	MB	B				B
	[E.23] Errores de mantenimiento / actualización de equipos (hardw	MB	B				B
	[E.25] Pérdida de equipos	PP	B				B
	[A.7] Uso no previsto	P	A				A
	[A.11] Acceso no autorizado	MB	B				B
	[A.23] Manipulación de los equipos	MB	B				B

Tabla 35 (continuación)

			Impacto				
			Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
[SW] aplicaciones (software)							
SIARP	[E.1] Errores de los usuarios	MA	A	A	A	A	
	[E.2] Errores del administrador	PP	B	B	B	B	
	[E.8] Difusión de softw are dañino	PP	B	B	B	B	
	[E.9] Errores de [re-]encaminamiento	MR	B	B	B	B	
	[E.10] Errores de secuencia	MR	B	B	B	B	
	[E.15] Alteración accidental de la información	MA	A	A	A	A	
	[E.18] Destrucción de información	P	M	A	M	M	
	[E.19] Fugas de información	P	M	M	A	M	
	[E.20] Vulnerabilidades de los programas (softw are)	CS	MA	MA	MA	MA	
	[E.21] Errores de mantenimiento / actualización de programas (sof	PP	B	B	B	B	
	[A.6] Abuso de privilegios de acceso	MA	A	A	A	A	
	[A.7] Uso no previsto	MA	A	A	A	A	
	[A.11] Acceso no autorizado	P	M	M	M	M	
	[A.15] Modificación deliberada de la información	MR	B	B	B	B	
	[A.18] Destrucción de información	P	M	A	M	M	
	[A.19] Divulgación de información	MB	B	B	B	B	
	[A.22] Manipulación de programas	P	A	M	M	M	
SISE	[E.1] Errores de los usuarios	MA	A	A	A	A	
	[E.2] Errores del administrador	PP	B	B	B	B	
	[E.8] Difusión de softw are dañino	PP	B	B	B	B	
	[E.9] Errores de [re-]encaminamiento	MR	B	B	B	B	
	[E.10] Errores de secuencia	MR	B	B	B	B	
	[E.15] Alteración accidental de la información	MA	A	A	A	A	
	[E.18] Destrucción de información	P	A	M	M	M	
	[E.19] Fugas de información	P	A	M	A	M	
	[E.20] Vulnerabilidades de los programas (softw are)	CS	MA	MA	MA	MA	
	[E.21] Errores de mantenimiento / actualización de programas (sof	PP	B	B	B	B	
	[A.6] Abuso de privilegios de acceso	MA	A	A	A	A	
	[A.7] Uso no previsto	MA	A	A	A	A	
	[A.11] Acceso no autorizado	P	A	M	A	M	
	[A.15] Modificación deliberada de la información	MR	B	B	B	B	
	[A.18] Destrucción de información	P	M	M	M	M	
	[A.19] Divulgación de información	MB	B	B	B	B	
	[A.22] Manipulación de programas	P	M	M	M	M	

Tabla 35 (continuación)

			Impacto				
			Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
SICO	[E.1] Errores de los usuarios	P	A	M	A	M	
	[E.2] Errores del administrador	PP	B	B	B	B	
	[E.8] Difusión de softw are dañino	MB	B	B	B	B	
	[E.9] Errores de [re-]encaminamiento	MR	B	B	B	B	
	[E.10] Errores de secuencia	MR	B	B	B	B	
	[E.15] Alteración accidental de la información	MB	B	B	B	B	
	[E.18] Destrucción de información	MB	B	B	B	B	
	[E.19] Fugas de información	PP	B	B	B	B	
	[E.20] Vulnerabilidades de los programas (softw are)	MB	B	B	B	B	
	[E.21] Errores de mantenimiento / actualización de programas (sot	PP	B	B	B	B	
	[A.6] Abuso de privilegios de acceso	MB	B	B	B	B	
	[A.7] Uso no previsto	MB	B	B	B	B	
	[A.11] Acceso no autorizado	PP	B	B	B	B	
	[A.15] Modificación deliberada de la información	MR	B	B	B	B	
	[A.18] Destrucción de información	PP	B	B	B	B	
	[A.19] Divulgación de información	MB	B	B	B	B	
	[A.22] Manipulación de programas	PP	B	B	B	B	
SARA	[E.1] Errores de los usuarios	MA	A	A	A	A	
	[E.2] Errores del administrador	PP	B	B	B	B	
	[E.8] Difusión de softw are dañino	PP	B	B	B	B	
	[E.9] Errores de [re-]encaminamiento	MR	B	B	B	B	
	[E.10] Errores de secuencia	MR	B	B	B	B	
	[E.15] Alteración accidental de la información	MA	A	A	A	A	
	[E.18] Destrucción de información	P	M	M	M	M	
	[E.19] Fugas de información	P	M	M	M	M	
	[E.20] Vulnerabilidades de los programas (softw are)	CS	MA	MA	MA	MA	
	[E.21] Errores de mantenimiento / actualización de programas (sot	PP	B	B	B	B	
	[A.6] Abuso de privilegios de acceso	MA	A	A	A	A	
	[A.7] Uso no previsto	MA	A	A	A	A	
	[A.11] Acceso no autorizado	P	M	M	M	M	
	[A.15] Modificación deliberada de la información	MR	B	B	B	B	
	[A.18] Destrucción de información	P	M	M	M	M	
	[A.19] Divulgación de información	P	M	M	M	M	
	[A.22] Manipulación de programas	P	M	M	A	M	

Tabla 35 (continuación)

			Impacto				
			Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
NEON WEB	[E.1] Errores de los usuarios	P	M	A	M	M	
	[E.2] Errores del administrador	PP	B	B	B	B	
	[E.8] Difusión de softw are dañino	PP	B	B	B	B	
	[E.9] Errores de [re-]encaminamiento	MR	B	B	B	B	
	[E.10] Errores de secuencia	MR	B	B	B	B	
	[E.15] Alteración accidental de la información	MA	A	A	A	A	
	[E.18] Destrucción de información	P	M	M	M	M	
	[E.19] Fugas de información	P	M	A	M	M	
	[E.20] Vulnerabilidades de los programas (softw are)	CS	MA	MA	MA	MA	
	[E.21] Errores de mantenimiento / actualización de programas (sof	PP	B	B	B	B	
	[A.6] Abuso de privilegios de acceso	MA	A	A	A	A	
	[A.7] Uso no previsto	MA	A	A	A	A	
	[A.11] Acceso no autorizado	P	A	M	M	M	
	[A.15] Modificación deliberada de la información	MR	B	B	B	B	
	[A.18] Destrucción de información	P	M	M	A	M	
	[A.19] Divulgación de información	MB	B	B	B	B	
	[A.22] Manipulación de programas	P	M	M	A	M	
SIAN	[E.1] Errores de los usuarios	P	A	M	M	M	
	[E.2] Errores del administrador	PP	B	B	B	B	
	[E.8] Difusión de softw are dañino	PP	B	B	B	B	
	[E.9] Errores de [re-]encaminamiento	MR	B	B	B	B	
	[E.10] Errores de secuencia	MR	B	B	B	B	
	[E.15] Alteración accidental de la información	MA	A	A	A	A	
	[E.18] Destrucción de información	P	A	M	M	M	
	[E.19] Fugas de información	P	M	M	A	M	
	[E.20] Vulnerabilidades de los programas (softw are)	CS	MA	MA	MA	MA	
	[E.21] Errores de mantenimiento / actualización de programas (sof	PP	B	B	B	B	
	[A.6] Abuso de privilegios de acceso	MA	A	A	A	A	
	[A.7] Uso no previsto	MA	A	A	A	A	
	[A.11] Acceso no autorizado	P	M	A	M	M	
	[A.15] Modificación deliberada de la información	MR	B	B	B	B	
	[A.18] Destrucción de información	P	M	A	M	M	
	[A.19] Divulgación de información	MB	B	B	B	B	
	[A.22] Manipulación de programas	P	A	M	M	M	

Tabla 35 (continuación)

			Impacto				
			Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
MIDAS	[E.1] Errores de los usuarios	MA	A	A	A	A	
	[E.2] Errores del administrador	PP	B	B	B	B	
	[E.8] Difusión de softw are dañino	PP	B	B	B	B	
	[E.9] Errores de [re-]encaminamiento	MR	B	B	B	B	
	[E.10] Errores de secuencia	MR	B	B	B	B	
	[E.15] Alteración accidental de la información	MB	B	B	B	B	
	[E.18] Destrucción de información	P	M	M	M	M	
	[E.19] Fugas de información	P	A	M	M	M	
	[E.20] Vulnerabilidades de los programas (softw are)	MB	B	B	B	B	
	[E.21] Errores de mantenimiento / actualización de programas (sof	PP	B	B	B	B	
	[A.6] Abuso de privilegios de acceso	MB	B	B	B	B	
	[A.7] Uso no previsto	MB	B	B	B	B	
	[A.11] Acceso no autorizado	P	A	M	A	M	
	[A.15] Modificación deliberada de la información	MR	B	B	B	B	
	[A.18] Destrucción de información	MB	B	B	B	B	
	[A.19] Divulgación de información	MB	B	B	B	B	
	[A.22] Manipulación de programas	MB	B	B	B	B	
ARANDA	[E.1] Errores de los usuarios	P	M	M	M	M	
	[E.2] Errores del administrador	MB	B	B	B	B	
	[E.8] Difusión de softw are dañino	MB	B	B	B	B	
	[E.9] Errores de [re-]encaminamiento	MB	B	B	B	B	
	[E.10] Errores de secuencia	MB	B	B	B	B	
	[E.15] Alteración accidental de la información	MB	B	B	B	B	
	[E.18] Destrucción de información	MB	B	B	B	B	
	[E.19] Fugas de información	MB	B	B	B	B	
	[E.20] Vulnerabilidades de los programas (softw are)	MB	B	B	B	B	
	[E.21] Errores de mantenimiento / actualización de programas (sof	MB	B	B	B	B	
	[A.6] Abuso de privilegios de acceso	MB	B	B	B	B	
	[A.7] Uso no previsto	MB	B	B	B	B	
	[A.11] Acceso no autorizado	MB	B	B	B	B	
	[A.15] Modificación deliberada de la información	MB	B	B	B	B	
	[A.18] Destrucción de información	MB	B	B	B	B	
	[A.19] Divulgación de información	MB	B	B	B	B	
	[A.22] Manipulación de programas	MB	B	B	B	B	

Tabla 35 (continuación)

			Impacto				
			Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
TFS	[E.1] Errores de los usuarios	P	M	M	A	M	
	[E.2] Errores del administrador	MB	B	B	B	B	
	[E.8] Difusión de softw are dañino	MB	B	B	B	B	
	[E.9] Errores de [re-]encaminamiento	MB	B	B	B	B	
	[E.10] Errores de secuencia	MB	B	B	B	B	
	[E.15] Alteración accidental de la información	MB	B	B	B	B	
	[E.18] Destrucción de información	MB	B	B	B	B	
	[E.19] Fugas de información	MB	B	B	B	B	
	[E.20] Vulnerabilidades de los programas (softw are)	MB	B	B	B	B	
	[E.21] Errores de mantenimiento / actualización de programas (sof	MB	B	B	B	B	
	[A.6] Abuso de privilegios de acceso	MB	B	B	B	B	
	[A.7] Uso no previsto	MB	B	B	B	B	
	[A.11] Acceso no autorizado	MB	B	B	B	B	
	[A.15] Modificación deliberada de la información	MB	B	B	B	B	
	[A.18] Destrucción de información	MB	B	B	B	B	
	[A.19] Divulgación de información	MB	B	B	B	B	
	[A.22] Manipulación de programas	MB	B	B	B	B	
[S] Servicios							
Gestión de identidades	[E.1] Errores de los usuarios	P		M		M	
	[E.2] Errores del administrador	PP		B		B	
	[E.9] Errores de [re-]encaminamiento	PP		B		B	
	[E.10] Errores de secuencia	PP		B		B	
	[E.15] Alteración accidental de la información	CS		MA		MA	
	[E.18] Destrucción de información	MA		A		A	
	[E.19] Fugas de información	MA		A		A	
	[E.24] Caída del sistema por agotamiento de recursos	MA		A		A	
	[A.5] Suplantación de la identidad del usuario	P		A		M	
	[A.6] Abuso de privilegios de acceso	P		M		M	
	[A.7] Uso no previsto	P		M		M	
	[A.9] [Re-]encaminamiento de mensajes	PP		B		B	
	[A.10] Alteración de secuencia	MB		B		B	
	[A.11] Acceso no autorizado	MA		A		A	
	[A.18] Destrucción de información	PP		B		B	
	[A.19] Divulgación de información	P		A		M	
	[A.24] Denegación de servicio	MA		A		A	

Tabla 35 (continuación)

			Impacto				
			Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Gestión de Privilegios	[E.1] Errores de los usuarios	P		M		M	
	[E.2] Errores del administrador	PP		B		B	
	[E.9] Errores de [re-]encaminamiento	PP		B		B	
	[E.10] Errores de secuencia	PP		B		B	
	[E.15] Alteración accidental de la información	CS		MA		MA	
	[E.18] Destrucción de información	MA		A		A	
	[E.19] Fugas de información	MA		A		A	
	[E.24] Caída del sistema por agotamiento de recursos	MA		A		A	
	[A.5] Suplantación de la identidad del usuario	P		A		M	
	[A.6] Abuso de privilegios de acceso	P		M		M	
	[A.7] Uso no previsto	P		A		M	
	[A.9] [Re-]encaminamiento de mensajes	PP		B		B	
	[A.10] Alteración de secuencia	MB		B		B	
	[A.11] Acceso no autorizado	MA		A		A	
	[A.18] Destrucción de información	PP		B		B	
	[A.19] Divulgación de información	P		M		M	
	[A.24] Denegación de servicio	MA		A		A	
Servicio de directorio	[E.1] Errores de los usuarios	PP		B		B	B
	[E.2] Errores del administrador	PP		B		B	B
	[E.9] Errores de [re-]encaminamiento	PP		B		B	B
	[E.10] Errores de secuencia	PP		B		B	B
	[E.15] Alteración accidental de la información	MR		B		B	B
	[E.18] Destrucción de información	MB		B		B	B
	[E.19] Fugas de información	MB		B		B	B
	[E.24] Caída del sistema por agotamiento de recursos	MB		B		B	B
	[A.5] Suplantación de la identidad del usuario	P		A		M	M
	[A.6] Abuso de privilegios de acceso	P		A		M	M
	[A.7] Uso no previsto	P		M		M	M
	[A.9] [Re-]encaminamiento de mensajes	PP		B		B	B
	[A.10] Alteración de secuencia	MB		B		B	B
	[A.11] Acceso no autorizado	MA		A		A	A
	[A.18] Destrucción de información	PP		B		B	B
	[A.19] Divulgación de información	P		M		M	M
	[A.24] Denegación de servicio	MA		A		A	A

Tabla 35 (continuación)

			Impacto				
			Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Página Web	[E.1] Errores de los usuarios	P		M	M		M
	[E.2] Errores del administrador	MB		B	B		B
	[E.9] Errores de [re-]encaminamiento	MR		B	B		B
	[E.10] Errores de secuencia	MR		B	B		B
	[E.15] Alteración accidental de la información	PP		B	B		B
	[E.18] Destrucción de información	P		M	M		M
	[E.19] Fugas de información	P		M	M		M
	[E.24] Caída del sistema por agotamiento de recursos	P		M	M		M
	[A.5] Suplantación de la identidad del usuario	P		M	M		M
	[A.6] Abuso de privilegios de acceso	MB		B	B		B
	[A.7] Uso no previsto	PP		B	B		B
	[A.9] [Re-]encaminamiento de mensajes	P		M	M		M
	[A.10] Alteración de secuencia	MR		B	B		B
	[A.11] Acceso no autorizado	P		M	M		M
	[A.18] Destrucción de información	P		M	M		M
	[A.19] Divulgación de información	MB		B	B		B
	[A.24] Denegación de servicio	P		M	M		M
[COM] Redes de comunicaciones							
Red Local	[I.8] Fallos de comunicación	MA	A				A
	[E.2] Errores del administrador	MB	B				B
	[E.9] Errores de [re-]encaminamiento	MR	B				B
	[E.10] Errores de secuencia	MR	B				B
	[E.14] Escapes de información	MB	B				B
	[E.15] Alteración accidental de la información	PP	B				B
	[E.18] Destrucción de información	P	A				M
	[E.19] Fugas de información	P	M				A
	[E.24] Caída del sistema por agotamiento de recursos	P	A				M
	[A.5] Suplantación de la identidad del usuario	P	M				A
	[A.6] Abuso de privilegios de acceso	MB	B				B
	[A.7] Uso no previsto	MB	B				B
	[A.9] [Re-]encaminamiento de mensajes	P	M				M
	[A.10] Alteración de secuencia	MR	B				B
	[A.11] Acceso no autorizado	P	A				M
	[A.12] Análisis de tráfico	MB	B				B
	[A.14] Interceptación de información (escucha)	PP	B				B
	[A.15] Modificación deliberada de la información	MR	B				B
	[A.19] Divulgación de información	MB	B				B
	[A.24] Denegación de servicio	P	M				M

Tabla 35 (continuación)

			Impacto				
			Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Red Inhalambrica	[I.8] Fallos de comunicación	P	M				M
	[E.2] Errores del administrador	MB	B				B
	[E.9] Errores de [re-]encaminamiento	MR	B				B
	[E.10] Errores de secuencia	MR	B				B
	[E.14] Escapes de información	MB	B				B
	[E.15] Alteración accidental de la información	PP	B				B
	[E.18] Destrucción de información	P	M				A
	[E.19] Fugas de información	P	A				M
	[E.24] Caída del sistema por agotamiento de recursos	P	M				M
	[A.5] Suplantación de la identidad del usuario	P	M				M
	[A.6] Abuso de privilegios de acceso	MB	B				B
	[A.7] Uso no previsto	MB	B				B
	[A.9] [Re-]encaminamiento de mensajes	P	M				M
	[A.10] Alteración de secuencia	MR	B				B
	[A.11] Acceso no autorizado	P	M				M
	[A.12] Análisis de tráfico	MB	B				B
	[A.14] Interceptación de información (escucha)	PP	B				B
	[A.15] Modificación deliberada de la información	MR	B				B
	[A.19] Divulgación de información	MB	B				B
	[A.24] Denegación de servicio	P	M				M
Red Telefónica	[I.8] Fallos de comunicación	MA	A				A
	[E.2] Errores del administrador	MB	B				B
	[E.9] Errores de [re-]encaminamiento	MR	B				B
	[E.10] Errores de secuencia	MR	B				B
	[E.14] Escapes de información	MB	B				B
	[E.15] Alteración accidental de la información	PP	B				B
	[E.18] Destrucción de información	P	M				M
	[E.19] Fugas de información	P	M				M
	[E.24] Caída del sistema por agotamiento de recursos	P	M				M
	[A.5] Suplantación de la identidad del usuario	P	M				M
	[A.6] Abuso de privilegios de acceso	MB	B				B
	[A.7] Uso no previsto	MB	B				B
	[A.9] [Re-]encaminamiento de mensajes	P	M				M
	[A.10] Alteración de secuencia	MR	B				B
	[A.11] Acceso no autorizado	P	M				M
	[A.12] Análisis de tráfico	MB	B				B
	[A.14] Interceptación de información (escucha)	PP	B				B
	[A.15] Modificación deliberada de la información	MR	B				B
	[A.19] Divulgación de información	MB	B				B
	[A.24] Denegación de servicio	P	A				A

Tabla 35 (continuación)

			Impacto				
			Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Internet	[I.8] Fallos de comunicación	P	M				A
	[E.2] Errores del administrador	MB	B				B
	[E.9] Errores de [re-]encaminamiento	MR	B				B
	[E.10] Errores de secuencia	MR	B				B
	[E.14] Escapes de información	MB	B				B
	[E.15] Alteración accidental de la información	PP	B				B
	[E.18] Destrucción de información	P	A				M
	[E.19] Fugas de información	P	M				M
	[E.24] Caída del sistema por agotamiento de recursos	P	A				A
	[A.5] Suplantación de la identidad del usuario	P	M				A
	[A.6] Abuso de privilegios de acceso	MB	B				B
	[A.7] Uso no previsto	MB	B				B
	[A.9] [Re-]encaminamiento de mensajes	P	M				M
	[A.10] Alteración de secuencia	MR	B				B
	[A.11] Acceso no autorizado	P	M				M
	[A.12] Análisis de tráfico	MB	B				B
	[A.14] Interceptación de información (escucha)	PP	B				B
	[A.15] Modificación deliberada de la información	MR	B				B
	[A.19] Divulgación de información	MB	B				B
	[A.24] Denegación de servicio	P	M				M
[AUX] Equipamiento auxiliar							
Sistema de alimentación ininterrumpida	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	M				
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	PP	B				
	[I.9] Interrupción de otros suministros o servicios esenciales	P	M				
	[I. 11] Emanaciones electromagnéticas	PP	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardw	MB	B				
	[E.24] Caída del sistema por agotamiento de recursos	MB	B				
	[E.25] Pérdida de equipos	MB	B				
	[A.7] Uso no previsto	MB	B				
	[A.11] Acceso no autorizado	MB	B				
	[A.23] Manipulación de los equipos	MB	B				
	[A.25] Robo	MB	B				
	[A.26] Ataque destructivo	MB	B				

Tabla 35 (continuación)

			Impacto				
			Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Equipo de climatización	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	M				
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	PP	B				
	[I.9] Interrupción de otros suministros o servicios esenciales	P	M				
	[I. 11] Emanaciones electromagnéticas	PP	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardw	MB	B				
	[E.24] Caída del sistema por agotamiento de recursos	MB	B				
	[E.25] Pérdida de equipos	MB	B				
	[A.7] Uso no previsto	MB	B				
	[A.11] Acceso no autorizado	MB	B				
	[A.23] Manipulación de los equipos	MB	B				
	[A.25] Robo	MB	B				
	[A.26] Ataque destructivo	MB	B				
Cableado	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	M				
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	PP	B				
	[I.9] Interrupción de otros suministros o servicios esenciales	P	M				
	[I. 11] Emanaciones electromagnéticas	PP	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardw	MB	B				
	[E.24] Caída del sistema por agotamiento de recursos	MB	B				
	[E.25] Pérdida de equipos	MB	B				
	[A.7] Uso no previsto	MB	B				
	[A.11] Acceso no autorizado	MB	B				
	[A.23] Manipulación de los equipos	MB	B				
	[A.25] Robo	MB	B				
	[A.26] Ataque destructivo	MB	B				

Tabla 35 (continuación)

			Impacto				
			Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Material impreso o digitalizado	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P			A		
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	P			M		
	[I.10] Degradación de los soportes de almacenamiento de la inforr	PP			B		
	[I. 11] Emanaciones electromagnéticas	PP			B		
	[E.1] Errores de los usuarios	P			A		
	[E.2] Errores del administrador	MB			B		
	[E.15] Alteración accidental de la información	PP			B		
	[E.18] Destrucción de información	P			M		
	[E.19] Fugas de información	P			A		
	[E.23] Errores de mantenimiento / actualización de equipos (hardw	MB			B		
	[E.25] Pérdida de equipos	MR			B		
	[A.7] Uso no previsto	MB			B		
	[A.11] Acceso no autorizado	P			M		
	[A.15] Modificación deliberada de la información	MB			B		
	[A.18] Destrucción de información	P			M		
	[A.19] Divulgación de información	MB			B		
	[A.25] Robo	PP			B		
	[A.26] Ataque destructivo	MB			B		
[D] Datos / Información							
Datos vitales	[E. 1] Errores de los usuarios	MA	A	A	A		
	[E. 2] Errores de administración	P	M	M	M		
	[E. 3. 4] Errores de configuración y monitorización	P	M	M	M		
	[E.15] Alteración accidental de la información	P	M	M	M		
	[E.18] Destrucción de información	P	M	M	M		
	[E.19] Fugas de información	P	M	M	M		
	[A.3] Manipulación de los registros de actividad (log)	PP	B	B	B		
	[A.4] Manipulación de la configuración	PP	B	B	B		
	[A.5] Suplantación de la identidad del usuario	P	A	M	A		
	[A.6] Abuso de privilegios de acceso	P	M	M	M		
	[A.11] Acceso no autorizado	P	M	A	M		
	[A.15] Modificación deliberada de la información	PP	B	B	B		
	[A.18] Destrucción de información	PP	B	B	B		
	[A.19] Divulgación de información	MB	B	B	B		

Tabla 35 (continuación)

			Impacto				
			Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Código fuente	[E. 1] Errores de los usuarios	PP	B	B	B		
	[E. 2] Errores de administración	PP	B	B	B		
	[E. 3. 4] Errores de configuración y monitorización	PP	B	B	B		
	[E.15] Alteración accidental de la información	MA	A	A	A		
	[E.18] Destrucción de información	P	M	M	M		
	[E.19] Fugas de información	P	M	M	M		
	[A.3] Manipulación de los registros de actividad (log)	P	M	M	M		
	[A.4] Manipulación de la configuración	P	M	M	M		
	[A.5] Suplantación de la identidad del usuario	P	M	M	M		
	[A.6] Abuso de privilegios de acceso	P	M	M	M		
	[A.11] Acceso no autorizado	P	M	M	M		
	[A.15] Modificación deliberada de la información	PP	B	B	B		
	[A.18] Destrucción de información	PP	B	B	B		
	[A.19] Divulgación de información	PP	B	B	B		
Código ejecutable	[E. 1] Errores de los usuarios	PP	B	B	B		
	[E. 2] Errores de administración	PP	B	B	B		
	[E. 3. 4] Errores de configuración y monitorización	PP	B	B	B		
	[E.15] Alteración accidental de la información	MA	A	A	A		
	[E.18] Destrucción de información	P	M	M	M		
	[E.19] Fugas de información	P	M	A	M		
	[A.3] Manipulación de los registros de actividad (log)	P	A	M	M		
	[A.4] Manipulación de la configuración	P	M	M	M		
	[A.5] Suplantación de la identidad del usuario	P	M	M	M		
	[A.6] Abuso de privilegios de acceso	P	M	M	M		
	[A.11] Acceso no autorizado	P	M	M	M		
	[A.15] Modificación deliberada de la información	PP	B	B	B		
	[A.18] Destrucción de información	PP	B	B	B		
	[A.19] Divulgación de información	PP	B	B	B		

Tabla 35 (continuación)

			Impacto				
			Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Datos de prueba	[E. 1] Errores de los usuarios	P	M	M	A		
	[E. 2] Errores de administración	PP	B	B	B		
	[E. 3. 4] Errores de configuración y monitorización	PP	B	B	B		
	[E.15] Alteración accidental de la información	PP	B	B	B		
	[E.18] Destrucción de información	P	M	M	M		
	[E.19] Fugas de información	P	M	M	M		
	[A.3] Manipulación de los registros de actividad (log)	P	M	M	M		
	[A.4] Manipulación de la configuración	P	M	M	M		
	[A.5] Suplantación de la identidad del usuario	P	M	M	M		
	[A.6] Abuso de privilegios de acceso	MB	B	B	B		
	[A.11] Acceso no autorizado	P	M	M	M		
	[A.15] Modificación deliberada de la información	MB	B	B	B		
	[A.18] Destrucción de información	P	M	M	M		
	[A.19] Divulgación de información	MB	B	B	B		
[P] Persona							
Usuarios internos y externos	[E. 7] Deficiencia en la organización	PP	B	B	B		
	[E. 19] Fugas de información	PP	B	B	B		
	[E. 28] Indisponibilidad del personal	P	M	M	M		
	[A. 29] Extorsión	MB	B	B	B		
	[A.30] Ingeniería social (picaresca)	P	M	A	M		
[L] Instalaciones							
Centro Principal de procesamiento	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	A				
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	P	M				
	[I. 11] Emanaciones electromagnéticas	PP	B				
	[E.15] Alteración accidental de la información	PP	B				
	[E.19] Fugas de información	P	M				
	[E.18] Destrucción de información	P	M				
	[A.11] Acceso no autorizado	PP	B				
	[A.15] Modificación deliberada de la información	MB	B				
	[A.18] Destrucción de información	MB	B				
	[A.19] Divulgación de información	MB	B				
	[A.26] Ataque destructivo	PP	B				

Tabla 35 (continuación)

			Impacto				
			Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Centro Alterno de procesamiento	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	M				
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	P	M				
	[I. 11] Emanaciones electromagnéticas	PP	B				
	[E.15] Alteración accidental de la información	PP	B				
	[E.19] Fugas de información	P	M				
	[E.18] Destrucción de información	P	M				
	[A.11] Acceso no autorizado	PP	B				
	[A.15] Modificación deliberada de la información	MB	B				
	[A.18] Destrucción de información	MB	B				
	[A.19] Divulgación de información	MB	B				
	[A.26] Ataque destructivo	PP	B				
Edificio Casa Matriz	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	M				
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	P	M				
	[I. 11] Emanaciones electromagnéticas	PP	B				
	[E.15] Alteración accidental de la información	PP	B				
	[E.19] Fugas de información	P	M				
	[E.18] Destrucción de información	P	M				
	[A.11] Acceso no autorizado	PP	B				
	[A.15] Modificación deliberada de la información	MB	B				
	[A.18] Destrucción de información	MB	B				
	[A.19] Divulgación de información	MB	B				
	[A.26] Ataque destructivo	PP	B				

Fuente: El autor

9.1.2.4.3 Calculo del riesgo potencial

La valoración del riesgo se da mediante la toma de valores de la probabilidad de ocurrencia por cada amenaza y el impacto sobre cada dimensión, de acuerdo a la tabla relacionada a continuación:

Tabla 36 Criterios para la valoración del riesgo

Riesgo		Probabilidad					
		CS	MA	P	PP	MB	MR
Impacto	MA	MA	MA	MA	B	MB	MB
	A	MA	MA	A	M	B	MB
	M	A	A	M	M	B	MB
	B	A	M	B	B	MB	MB
	MB	B	B	B	MB	MB	MB

Fuente: El autor

Tabla 37 Estimación del riesgo

			Impacto					Riesgo				
			Dimensiones					Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
[HW] Equipos informáticos (hardware)												
Servidores	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	M				M	M				M
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego), contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	P	M				M	M				M
	[I. 11] Emanaciones electromagnéticas	PP	B				B	B				B
	[E.23] Errores de mantenimiento / actualización de equipos (hardw	MB	B				B	MB				MB
	[E.24] Caída del sistema por agotamiento de recursos	P	M				M	M				M
	[E.25] Pérdida de equipos	MR	B				B	MB				MB
	[A.6] Abuso de privilegios de acceso	MB	B				B	MB				MB
	[A.7] Uso no previsto	PP	B				B	B				B
	[A.11] Acceso no autorizado	P	A				M	A				M
	[A.23] Manipulación de los equipos	P	A				M	A				M
	[A.24] Denegación de servicio	P	A				M	A				M
	[A.25] Robo	MB	B				B	MB				MB
	[A.26] Ataque destructivo	P	M				M	M				M

Tabla 37 (continuación)

			Impacto					Riesgo				
			Dimensiones					Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Equipos de escritorio y portatiles	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	M				M	M				M
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego), contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	P	M				M	M				M
	[I. 11] Emanaciones electromagnéticas	PP	B				B	B				B
	[E.23] Errores de mantenimiento / actualización de equipos (hardw	MB	B				B	MB				MB
	[E.24] Caída del sistema por agotamiento de recursos	P	M				M	M				M
	[E.25] Pérdida de equipos	MR	B				B	MB				MB
	[A.6] Abuso de privilegios de acceso	MB	B				B	MB				MB
	[A.7] Uso no previsto	PP	B				B	B				B
	[A.11] Acceso no autorizado	P	A				M	A				M
	[A.23] Manipulación de los equipos	P	A				M	A				M
	[A.24] Denegación de servicio	P	A				M	A				M
	[A.25] Robo	MB	B				B	MB				MB
	[A.26] Ataque destructivo	P	M				M	M				M
Soporte de la red Modems Routers Encaminadores	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	M				M	M				M
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego), contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	P	M				M	M				M
	[I. 11] Emanaciones electromagnéticas	MB	B				B	MB				MB
	[E.23] Errores de mantenimiento / actualización de equipos (hardw	MB	B				B	MB				MB
	[E.25] Pérdida de equipos	PP	B				B	B				B
	[A.7] Uso no previsto	P	A				A	A				A
	[A.11] Acceso no autorizado	MB	B				B	MB				MB
	[A.23] Manipulación de los equipos	MB	B				B	MB				MB

Tabla 37 (continuación)

			Impacto					Riesgo				
			Dimensiones					Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
[SW] aplicaciones (software)												
SIARP	[E.1] Errores de los usuarios	MA	A	A	A	A		MA	MA	MA	MA	
	[E.2] Errores del administrador	PP	B	B	B	B		B	B	B	B	
	[E.8] Difusión de softw are dañino	PP	B	B	B	B		B	B	B	B	
	[E.9] Errores de [re-]encaminamiento	MR	B	B	B	B		MB	MB	MB	MB	
	[E.10] Errores de secuencia	MR	B	B	B	B		MB	MB	MB	MB	
	[E.15] Alteración accidental de la información	MA	A	A	A	A		MA	MA	MA	MA	
	[E.18] Destrucción de información	P	M	A	M	M		M	A	M	M	
	[E.19] Fugas de información	P	M	M	A	M		M	M	A	M	
	[E.20] Vulnerabilidades de los programas (softw are)	CS	MA	MA	MA	MA		MA	MA	MA	MA	
	[E.21] Errores de mantenimiento / actualización de programas (sof	PP	B	B	B	B		B	B	B	B	
	[A.6] Abuso de privilegios de acceso	MA	A	A	A	A		MA	MA	MA	MA	
	[A.7] Uso no previsto	MA	A	A	A	A		MA	MA	MA	MA	
	[A.11] Acceso no autorizado	P	M	M	M	M		M	M	M	M	
	[A.15] Modificación deliberada de la información	MR	B	B	B	B		MB	MB	MB	MB	
	[A.18] Destrucción de información	P	M	A	M	M		M	A	M	M	
	[A.19] Divulgación de información	MB	B	B	B	B		MB	MB	MB	MB	
	[A.22] Manipulación de programas	P	A	M	M	M		A	M	M	M	
SISE	[E.1] Errores de los usuarios	MA	A	A	A	A		MA	MA	MA	MA	
	[E.2] Errores del administrador	PP	B	B	B	B		B	B	B	B	
	[E.8] Difusión de softw are dañino	PP	B	B	B	B		B	B	B	B	
	[E.9] Errores de [re-]encaminamiento	MR	B	B	B	B		MB	MB	MB	MB	
	[E.10] Errores de secuencia	MR	B	B	B	B		MB	MB	MB	MB	
	[E.15] Alteración accidental de la información	MA	A	A	A	A		MA	MA	MA	MA	
	[E.18] Destrucción de información	P	A	M	M	M		A	M	M	M	
	[E.19] Fugas de información	P	A	M	A	M		A	M	A	M	
	[E.20] Vulnerabilidades de los programas (softw are)	CS	MA	MA	MA	MA		MA	MA	MA	MA	
	[E.21] Errores de mantenimiento / actualización de programas (sof	PP	B	B	B	B		B	B	B	B	
	[A.6] Abuso de privilegios de acceso	MA	A	A	A	A		MA	MA	MA	MA	
	[A.7] Uso no previsto	MA	A	A	A	A		MA	MA	MA	MA	
	[A.11] Acceso no autorizado	P	A	M	A	M		A	M	A	M	
	[A.15] Modificación deliberada de la información	MR	B	B	B	B		MB	MB	MB	MB	
	[A.18] Destrucción de información	P	M	M	M	M		M	M	M	M	
	[A.19] Divulgación de información	MB	B	B	B	B		MB	MB	MB	MB	
	[A.22] Manipulación de programas	P	M	M	M	M		M	M	M	M	

Tabla 37 (continuación)

			Impacto					Riesgo				
			Dimensiones					Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
SICO	[E.1] Errores de los usuarios	P	A	M	A	M		A	M	A	M	
	[E.2] Errores del administrador	PP	B	B	B	B		B	B	B	B	
	[E.8] Difusión de softw are dañino	MB	B	B	B	B		MB	MB	MB	MB	
	[E.9] Errores de [re-]encaminamiento	MR	B	B	B	B		MB	MB	MB	MB	
	[E.10] Errores de secuencia	MR	B	B	B	B		MB	MB	MB	MB	
	[E.15] Alteración accidental de la información	MB	B	B	B	B		MB	MB	MB	MB	
	[E.18] Destrucción de información	MB	B	B	B	B		MB	MB	MB	MB	
	[E.19] Fugas de información	PP	B	B	B	B		B	B	B	B	
	[E.20] Vulnerabilidades de los programas (softw are)	MB	B	B	B	B		MB	MB	MB	MB	
	[E.21] Errores de mantenimiento / actualización de programas (sof	PP	B	B	B	B		B	B	B	B	
	[A.6] Abuso de privilegios de acceso	MB	B	B	B	B		MB	MB	MB	MB	
	[A.7] Uso no previsto	MB	B	B	B	B		MB	MB	MB	MB	
	[A.11] Acceso no autorizado	PP	B	B	B	B		B	B	B	B	
	[A.15] Modificación deliberada de la información	MR	B	B	B	B		MB	MB	MB	MB	
	[A.18] Destrucción de información	PP	B	B	B	B		B	B	B	B	
	[A.19] Divulgación de información	MB	B	B	B	B		MB	MB	MB	MB	
	[A.22] Manipulación de programas	PP	B	B	B	B		B	B	B	B	
SARA	[E.1] Errores de los usuarios	MA	A	A	A	A		MA	MA	MA	MA	
	[E.2] Errores del administrador	PP	B	B	B	B		B	B	B	B	
	[E.8] Difusión de softw are dañino	PP	B	B	B	B		B	B	B	B	
	[E.9] Errores de [re-]encaminamiento	MR	B	B	B	B		MB	MB	MB	MB	
	[E.10] Errores de secuencia	MR	B	B	B	B		MB	MB	MB	MB	
	[E.15] Alteración accidental de la información	MA	A	A	A	A		MA	MA	MA	MA	
	[E.18] Destrucción de información	P	M	M	M	M		M	M	M	M	
	[E.19] Fugas de información	P	M	M	M	M		M	M	M	M	
	[E.20] Vulnerabilidades de los programas (softw are)	CS	MA	MA	MA	MA		MA	MA	MA	MA	
	[E.21] Errores de mantenimiento / actualización de programas (sof	PP	B	B	B	B		B	B	B	B	
	[A.6] Abuso de privilegios de acceso	MA	A	A	A	A		MA	MA	MA	MA	
	[A.7] Uso no previsto	MA	A	A	A	A		MA	MA	MA	MA	
	[A.11] Acceso no autorizado	P	M	M	M	M		M	M	M	M	
	[A.15] Modificación deliberada de la información	MR	B	B	B	B		MB	MB	MB	MB	
	[A.18] Destrucción de información	P	M	M	M	M		M	M	M	M	
	[A.19] Divulgación de información	P	M	M	M	M		M	M	M	M	
	[A.22] Manipulación de programas	P	M	M	A	M		M	M	A	M	

Tabla 37 (continuación)

			Impacto					Riesgo				
			Dimensiones					Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
NEON WEB	[E.1] Errores de los usuarios	P	M	A	M	M		M	A	M	M	
	[E.2] Errores del administrador	PP	B	B	B	B		B	B	B	B	
	[E.8] Difusión de softw are dañino	PP	B	B	B	B		B	B	B	B	
	[E.9] Errores de [re-]encaminamiento	MR	B	B	B	B		MB	MB	MB	MB	
	[E.10] Errores de secuencia	MR	B	B	B	B		MB	MB	MB	MB	
	[E.15] Alteración accidental de la información	MA	A	A	A	A		MA	MA	MA	MA	
	[E.18] Destrucción de información	P	M	M	M	M		M	M	M	M	
	[E.19] Fugas de información	P	M	A	M	M		M	A	M	M	
	[E.20] Vulnerabilidades de los programas (softw are)	CS	MA	MA	MA	MA		MA	MA	MA	MA	
	[E.21] Errores de mantenimiento / actualización de programas (sof	PP	B	B	B	B		B	B	B	B	
	[A.6] Abuso de privilegios de acceso	MA	A	A	A	A		MA	MA	MA	MA	
	[A.7] Uso no previsto	MA	A	A	A	A		MA	MA	MA	MA	
	[A.11] Acceso no autorizado	P	A	M	M	M		A	M	M	M	
	[A.15] Modificación deliberada de la información	MR	B	B	B	B		MB	MB	MB	MB	
	[A.18] Destrucción de información	P	M	M	A	M		M	M	A	M	
	[A.19] Divulgación de información	MB	B	B	B	B		MB	MB	MB	MB	
	[A.22] Manipulación de programas	P	M	M	A	M		M	M	A	M	
SIAN	[E.1] Errores de los usuarios	P	A	M	M	M		A	M	M	M	
	[E.2] Errores del administrador	PP	B	B	B	B		B	B	B	B	
	[E.8] Difusión de softw are dañino	PP	B	B	B	B		B	B	B	B	
	[E.9] Errores de [re-]encaminamiento	MR	B	B	B	B		MB	MB	MB	MB	
	[E.10] Errores de secuencia	MR	B	B	B	B		MB	MB	MB	MB	
	[E.15] Alteración accidental de la información	MA	A	A	A	A		MA	MA	MA	MA	
	[E.18] Destrucción de información	P	A	M	M	M		A	M	M	M	
	[E.19] Fugas de información	P	M	M	A	M		M	A	M	M	
	[E.20] Vulnerabilidades de los programas (softw are)	CS	MA	MA	MA	MA		MA	MA	MA	MA	
	[E.21] Errores de mantenimiento / actualización de programas (sof	PP	B	B	B	B		B	B	B	B	
	[A.6] Abuso de privilegios de acceso	MA	A	A	A	A		MA	MA	MA	MA	
	[A.7] Uso no previsto	MA	A	A	A	A		MA	MA	MA	MA	
	[A.11] Acceso no autorizado	P	M	A	M	M		M	A	M	M	
	[A.15] Modificación deliberada de la información	MR	B	B	B	B		MB	MB	MB	MB	
	[A.18] Destrucción de información	P	M	A	M	M		M	A	M	M	
	[A.19] Divulgación de información	MB	B	B	B	B		MB	MB	MB	MB	
	[A.22] Manipulación de programas	P	A	M	M	M		A	M	M	M	

Tabla 37 (continuación)

			Impacto					Riesgo				
			Dimensiones					Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
MIDAS	[E.1] Errores de los usuarios	MA	A	A	A	A		MA	MA	MA	MA	
	[E.2] Errores del administrador	PP	B	B	B	B		B	B	B	B	
	[E.8] Difusión de software dañino	PP	B	B	B	B		B	B	B	B	
	[E.9] Errores de [re-]encaminamiento	MR	B	B	B	B		MB	MB	MB	MB	
	[E.10] Errores de secuencia	MR	B	B	B	B		MB	MB	MB	MB	
	[E.15] Alteración accidental de la información	MB	B	B	B	B		MB	MB	MB	MB	
	[E.18] Destrucción de información	P	M	M	M	M		M	M	M	M	
	[E.19] Fugas de información	P	A	M	M	M		A	M	M	M	
	[E.20] Vulnerabilidades de los programas (software)	MB	B	B	B	B		MB	MB	MB	MB	
	[E.21] Errores de mantenimiento / actualización de programas (sof	PP	B	B	B	B		B	B	B	B	
	[A.6] Abuso de privilegios de acceso	MB	B	B	B	B		MB	MB	MB	MB	
	[A.7] Uso no previsto	MB	B	B	B	B		MB	MB	MB	MB	
	[A.11] Acceso no autorizado	P	A	M	A	M		A	M	A	M	
	[A.15] Modificación deliberada de la información	MR	B	B	B	B		MB	MB	MB	MB	
	[A.18] Destrucción de información	MB	B	B	B	B		MB	MB	MB	MB	
	[A.19] Divulgación de información	MB	B	B	B	B		MB	MB	MB	MB	
	[A.22] Manipulación de programas	MB	B	B	B	B		MB	MB	MB	MB	
ARANDA	[E.1] Errores de los usuarios	P	M	M	M	M		M	M	M	M	
	[E.2] Errores del administrador	MB	B	B	B	B		MB	MB	MB	MB	
	[E.8] Difusión de software dañino	MB	B	B	B	B		MB	MB	MB	MB	
	[E.9] Errores de [re-]encaminamiento	MB	B	B	B	B		MB	MB	MB	MB	
	[E.10] Errores de secuencia	MB	B	B	B	B		MB	MB	MB	MB	
	[E.15] Alteración accidental de la información	MB	B	B	B	B		MB	MB	MB	MB	
	[E.18] Destrucción de información	MB	B	B	B	B		MB	MB	MB	MB	
	[E.19] Fugas de información	MB	B	B	B	B		MB	MB	MB	MB	
	[E.20] Vulnerabilidades de los programas (software)	MB	B	B	B	B		MB	MB	MB	MB	
	[E.21] Errores de mantenimiento / actualización de programas (sof	MB	B	B	B	B		MB	MB	MB	MB	
	[A.6] Abuso de privilegios de acceso	MB	B	B	B	B		MB	MB	MB	MB	
	[A.7] Uso no previsto	MB	B	B	B	B		MB	MB	MB	MB	
	[A.11] Acceso no autorizado	MB	B	B	B	B		MB	MB	MB	MB	
	[A.15] Modificación deliberada de la información	MB	B	B	B	B		MB	MB	MB	MB	
	[A.18] Destrucción de información	MB	B	B	B	B		MB	MB	MB	MB	
	[A.19] Divulgación de información	MB	B	B	B	B		MB	MB	MB	MB	
	[A.22] Manipulación de programas	MB	B	B	B	B		MB	MB	MB	MB	

Tabla 37 (continuación)

			Impacto					Riesgo				
			Dimensiones					Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
TFS	[E.1] Errores de los usuarios	P	M	M	A	M		M	M	A	M	
	[E.2] Errores del administrador	MB	B	B	B	B		MB	MB	MB	MB	
	[E.8] Difusión de softw are dañino	MB	B	B	B	B		MB	MB	MB	MB	
	[E.9] Errores de [re-]encaminamiento	MB	B	B	B	B		MB	MB	MB	MB	
	[E.10] Errores de secuencia	MB	B	B	B	B		MB	MB	MB	MB	
	[E.15] Alteración accidental de la información	MB	B	B	B	B		MB	MB	MB	MB	
	[E.18] Destrucción de información	MB	B	B	B	B		MB	MB	MB	MB	
	[E.19] Fugas de información	MB	B	B	B	B		MB	MB	MB	MB	
	[E.20] Vulnerabilidades de los programas (softw are)	MB	B	B	B	B		MB	MB	MB	MB	
	[E.21] Errores de mantenimiento / actualización de programas (sof	MB	B	B	B	B		MB	MB	MB	MB	
	[A.6] Abuso de privilegios de acceso	MB	B	B	B	B		MB	MB	MB	MB	
	[A.7] Uso no previsto	MB	B	B	B	B		MB	MB	MB	MB	
	[A.11] Acceso no autorizado	MB	B	B	B	B		MB	MB	MB	MB	
	[A.15] Modificación deliberada de la información	MB	B	B	B	B		MB	MB	MB	MB	
	[A.18] Destrucción de información	MB	B	B	B	B		MB	MB	MB	MB	
	[A.19] Divulgación de información	MB	B	B	B	B		MB	MB	MB	MB	
	[A.22] Manipulación de programas	MB	B	B	B	B		MB	MB	MB	MB	
[S] Servicios												
Gestión de identidades	[E.1] Errores de los usuarios	P		M		M			M		M	
	[E.2] Errores del administrador	PP		B		B			B		B	
	[E.9] Errores de [re-]encaminamiento	PP		B		B			B		B	
	[E.10] Errores de secuencia	PP		B		B			B		B	
	[E.15] Alteración accidental de la información	CS		MA		MA			MA		MA	
	[E.18] Destrucción de información	MA		A		A			MA		MA	
	[E.19] Fugas de información	MA		A		A			MA		MA	
	[E.24] Caída del sistema por agotamiento de recursos	MA		A		A			MA		MA	
	[A.5] Suplantación de la identidad del usuario	P		A		M			A		M	
	[A.6] Abuso de privilegios de acceso	P		M		M			M		M	
	[A.7] Uso no previsto	P		M		M			M		M	
	[A.9] [Re-]encaminamiento de mensajes	PP		B		B			B		B	
	[A.10] Alteración de secuencia	MB		B		B			MB		MB	
	[A.11] Acceso no autorizado	MA		A		A			MA		MA	
	[A.18] Destrucción de información	PP		B		B			B		B	
	[A.19] Divulgación de información	P		A		M			A		M	
	[A.24] Denegación de servicio	MA		A		A			MA		MA	

Tabla 37 (continuación)

			Impacto					Riesgo				
			Dimensiones					Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Gestión de Privilegios	[E.1] Errores de los usuarios	P		M		M			M		M	
	[E.2] Errores del administrador	PP		B		B			B		B	
	[E.9] Errores de [re-]encaminamiento	PP		B		B			B		B	
	[E.10] Errores de secuencia	PP		B		B			B		B	
	[E.15] Alteración accidental de la información	CS		MA		MA			MA		MA	
	[E.18] Destrucción de información	MA		A		A			MA		MA	
	[E.19] Fugas de información	MA		A		A			MA		MA	
	[E.24] Caída del sistema por agotamiento de recursos	MA		A		A			MA		MA	
	[A.5] Suplantación de la identidad del usuario	P		A		M			A		M	
	[A.6] Abuso de privilegios de acceso	P		M		M			M		M	
	[A.7] Uso no previsto	P		A		M			A		M	
	[A.9] [Re-]encaminamiento de mensajes	PP		B		B			B		B	
	[A.10] Alteración de secuencia	MB		B		B			MB		MB	
	[A.11] Acceso no autorizado	MA		A		A			MA		MA	
	[A.18] Destrucción de información	PP		B		B			B		B	
	[A.19] Divulgación de información	P		M		M			M		M	
	[A.24] Denegación de servicio	MA		A		A			MA		MA	
Servicio de directorio	[E.1] Errores de los usuarios	PP		B		B	B		B		B	B
	[E.2] Errores del administrador	PP		B		B	B		B		B	B
	[E.9] Errores de [re-]encaminamiento	PP		B		B	B		B		B	B
	[E.10] Errores de secuencia	PP		B		B	B		B		B	B
	[E.15] Alteración accidental de la información	MR		B		B	B		MB		MB	MB
	[E.18] Destrucción de información	MB		B		B	B		MB		MB	MB
	[E.19] Fugas de información	MB		B		B	B		MB		MB	MB
	[E.24] Caída del sistema por agotamiento de recursos	MB		B		B	B		MB		MB	MB
	[A.5] Suplantación de la identidad del usuario	P		A		M	M		A		M	M
	[A.6] Abuso de privilegios de acceso	P		A		M	M		A		M	M
	[A.7] Uso no previsto	P		M		M	M		M		M	M
	[A.9] [Re-]encaminamiento de mensajes	PP		B		B	B		B		B	B
	[A.10] Alteración de secuencia	MB		B		B	B		MB		MB	MB
	[A.11] Acceso no autorizado	MA		A		A	A		MA		MA	MA
	[A.18] Destrucción de información	PP		B		B	B		B		B	B
	[A.19] Divulgación de información	P		M		M	M		M		M	M
	[A.24] Denegación de servicio	MA		A		A	A		MA		MA	MA

Tabla 37 (continuación)

			Impacto					Riesgo				
			Dimensiones					Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Página Web	[E.1] Errores de los usuarios	P		M	M		M		M	M		M
	[E.2] Errores del administrador	MB		B	B		B		MB	MB		MB
	[E.9] Errores de [re-]encaminamiento	MR		B	B		B		MB	MB		MB
	[E.10] Errores de secuencia	MR		B	B		B		MB	MB		MB
	[E.15] Alteración accidental de la información	PP		B	B		B		B	B		B
	[E.18] Destrucción de información	P		M	M		M		M	M		M
	[E.19] Fugas de información	P		M	M		M		M	M		M
	[E.24] Caída del sistema por agotamiento de recursos	P		M	M		M		M	M		M
	[A.5] Suplantación de la identidad del usuario	P		M	M		M		M	M		M
	[A.6] Abuso de privilegios de acceso	MB		B	B		B		MB	MB		MB
	[A.7] Uso no previsto	PP		B	B		B		B	B		B
	[A.9] [Re-]encaminamiento de mensajes	P		M	M		M		M	M		M
	[A.10] Alteración de secuencia	MR		B	B		B		MB	MB		MB
	[A.11] Acceso no autorizado	P		M	M		M		M	M		M
	[A.18] Destrucción de información	P		M	M		M		M	M		M
	[A.19] Divulgación de información	MB		B	B		B		MB	MB		MB
	[A.24] Denegación de servicio	P		M	M		M		M	M		M
[COM] Redes de comunicaciones												
Red Local	[I.8] Fallos de comunicación	MA	A				A	MA				MA
	[E.2] Errores del administrador	MB	B				B	MB				MB
	[E.9] Errores de [re-]encaminamiento	MR	B				B	MB				MB
	[E.10] Errores de secuencia	MR	B				B	MB				MB
	[E.14] Escapes de información	MB	B				B	MB				MB
	[E.15] Alteración accidental de la información	PP	B				B	B				B
	[E.18] Destrucción de información	P	A				M	A				M
	[E.19] Fugas de información	P	M				A	M				M
	[E.24] Caída del sistema por agotamiento de recursos	P	A				M	A				M
	[A.5] Suplantación de la identidad del usuario	P	M				A	M				M
	[A.6] Abuso de privilegios de acceso	MB	B				B	MB				MB
	[A.7] Uso no previsto	MB	B				B	MB				MB
	[A.9] [Re-]encaminamiento de mensajes	P	M				M	M				M
	[A.10] Alteración de secuencia	MR	B				B	MB				MB
	[A.11] Acceso no autorizado	P	A				M	A				M
	[A.12] Análisis de tráfico	MB	B				B	MB				MB
	[A.14] Interceptación de información (escucha)	PP	B				B	B				B
	[A.15] Modificación deliberada de la información	MR	B				B	MB				MB
	[A.19] Divulgación de información	MB	B				B	MB				MB
	[A.24] Denegación de servicio	P	M				M	M				M

Tabla 37 (continuación)

			Impacto					Riesgo				
			Dimensiones					Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Red Inhalambrica	[I.8] Fallos de comunicación	P	M				M	M				M
	[E.2] Errores del administrador	MB	B				B	MB				MB
	[E.9] Errores de [re-]encaminamiento	MR	B				B	MB				MB
	[E.10] Errores de secuencia	MR	B				B	MB				MB
	[E.14] Escapes de información	MB	B				B	MB				MB
	[E.15] Alteración accidental de la información	PP	B				B	B				B
	[E.18] Destrucción de información	P	M				A	M				M
	[E.19] Fugas de información	P	A				M	A				M
	[E.24] Caída del sistema por agotamiento de recursos	P	M				M	M				M
	[A.5] Suplantación de la identidad del usuario	P	M				M	M				M
	[A.6] Abuso de privilegios de acceso	MB	B				B	MB				MB
	[A.7] Uso no previsto	MB	B				B	MB				MB
	[A.9] [Re-]encaminamiento de mensajes	P	M				M	M				M
	[A.10] Alteración de secuencia	MR	B				B	MB				MB
	[A.11] Acceso no autorizado	P	M				M	M				M
	[A.12] Análisis de tráfico	MB	B				B	MB				MB
	[A.14] Interceptación de información (escucha)	PP	B				B	B				B
	[A.15] Modificación deliberada de la información	MR	B				B	MB				MB
	[A.19] Divulgación de información	MB	B				B	MB				MB
	[A.24] Denegación de servicio	P	M				M	M				M
Red Telefónica	[I.8] Fallos de comunicación	MA	A				A	MA				MA
	[E.2] Errores del administrador	MB	B				B	MB				MB
	[E.9] Errores de [re-]encaminamiento	MR	B				B	MB				MB
	[E.10] Errores de secuencia	MR	B				B	MB				MB
	[E.14] Escapes de información	MB	B				B	MB				MB
	[E.15] Alteración accidental de la información	PP	B				B	B				B
	[E.18] Destrucción de información	P	M				M	M				M
	[E.19] Fugas de información	P	M				M	M				M
	[E.24] Caída del sistema por agotamiento de recursos	P	M				M	M				M
	[A.5] Suplantación de la identidad del usuario	P	M				M	M				M
	[A.6] Abuso de privilegios de acceso	MB	B				B	MB				MB
	[A.7] Uso no previsto	MB	B				B	MB				MB
	[A.9] [Re-]encaminamiento de mensajes	P	M				M	M				M
	[A.10] Alteración de secuencia	MR	B				B	MB				MB
	[A.11] Acceso no autorizado	P	M				M	M				M
	[A.12] Análisis de tráfico	MB	B				B	MB				MB
	[A.14] Interceptación de información (escucha)	PP	B				B	B				B
	[A.15] Modificación deliberada de la información	MR	B				B	MB				MB
	[A.19] Divulgación de información	MB	B				B	MB				MB
	[A.24] Denegación de servicio	P	A				A	A				A

Tabla 37 (continuación)

			Impacto					Riesgo				
			Dimensiones					Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Internet	[I.8] Fallos de comunicación	P	M				A	M				M
	[E.2] Errores del administrador	MB	B				B	MB				MB
	[E.9] Errores de [re-]encaminamiento	MR	B				B	MB				MB
	[E.10] Errores de secuencia	MR	B				B	MB				MB
	[E.14] Escapes de información	MB	B				B	MB				MB
	[E.15] Alteración accidental de la información	PP	B				B	B				B
	[E.18] Destrucción de información	P	A				M	A				M
	[E.19] Fugas de información	P	M				M	M				M
	[E.24] Caída del sistema por agotamiento de recursos	P	A				A	A				A
	[A.5] Suplantación de la identidad del usuario	P	M				A	M				M
	[A.6] Abuso de privilegios de acceso	MB	B				B	MB				MB
	[A.7] Uso no previsto	MB	B				B	MB				MB
	[A.9] [Re-]encaminamiento de mensajes	P	M				M	M				M
	[A.10] Alteración de secuencia	MR	B				B	MB				MB
	[A.11] Acceso no autorizado	P	M				M	M				M
	[A.12] Análisis de tráfico	MB	B				B	MB				MB
	[A.14] Interceptación de información (escucha)	PP	B				B	B				B
	[A.15] Modificación deliberada de la información	MR	B				B	MB				MB
	[A.19] Divulgación de información	MB	B				B	MB				MB
	[A.24] Denegación de servicio	P	M				M	M				M
[AUX] Equipamiento auxiliar												
Sistema de alimentación ininterrumpida	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	M					M				
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	PP	B					B				
	[I.9] Interrupción de otros suministros o servicios esenciales	P	M					M				
	[I. 11] Emanaciones electromagnéticas	PP	B					B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardw	MB	B					MB				
	[E.24] Caída del sistema por agotamiento de recursos	MB	B					MB				
	[E.25] Pérdida de equipos	MB	B					MB				
	[A.7] Uso no previsto	MB	B					MB				
	[A.11] Acceso no autorizado	MB	B					MB				
	[A.23] Manipulación de los equipos	MB	B					MB				
	[A.25] Robo	MB	B					MB				
	[A.26] Ataque destructivo	MB	B					MB				

Tabla 37 (continuación)

			Impacto					Riesgo				
			Dimensiones					Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Equipo de climatización	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	M					M				
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	PP	B					B				
	[I.9] Interrupción de otros suministros o servicios esenciales	P	M					M				
	[I. 11] Emanaciones electromagnéticas	PP	B					B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardw	MB	B					MB				
	[E.24] Caída del sistema por agotamiento de recursos	MB	B					MB				
	[E.25] Pérdida de equipos	MB	B					MB				
	[A.7] Uso no previsto	MB	B					MB				
	[A.11] Acceso no autorizado	MB	B					MB				
	[A.23] Manipulación de los equipos	MB	B					MB				
	[A.25] Robo	MB	B					MB				
	[A.26] Ataque destructivo	MB	B					MB				
Cableado	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	M					M				
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	PP	B					B				
	[I.9] Interrupción de otros suministros o servicios esenciales	P	M					M				
	[I. 11] Emanaciones electromagnéticas	PP	B					B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardw	MB	B					MB				
	[E.24] Caída del sistema por agotamiento de recursos	MB	B					MB				
	[E.25] Pérdida de equipos	MB	B					MB				
	[A.7] Uso no previsto	MB	B					MB				
	[A.11] Acceso no autorizado	MB	B					MB				
	[A.23] Manipulación de los equipos	MB	B					MB				
	[A.25] Robo	MB	B					MB				
	[A.26] Ataque destructivo	MB	B					MB				

Tabla 37 (continuación)

			Impacto					Riesgo				
			Dimensiones					Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Generadores electricos	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	A					A				
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	P	M					M				
	[I.9] Interrupción de otros suministros o servicios esenciales	P	M					M				
	[I. 11] Emanaciones electromagnéticas	PP	B					B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardw	MB	B					MB				
	[E.24] Caída del sistema por agotamiento de recursos	P	M					M				
	[E.25] Pérdida de equipos	MR	B					MB				
	[A.7] Uso no previsto	MB	B					MB				
	[A.11] Acceso no autorizado	P	M					M				
	[A.23] Manipulación de los equipos	P	M					M				
	[A.25] Robo	MB	B					MB				
	[A.26] Ataque destructivo	PP	B					B				
[SI] Soportes de información												
Almacenamiento en red DVD CD USB	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P			A					A		
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	P			M					M		
	[I.10] Degradación de los soportes de almacenamiento de la inforr	PP			B					B		
	[I. 11] Emanaciones electromagnéticas	PP			B					B		
	[E.1] Errores de los usuarios	P			M					M		
	[E.2] Errores del administrador	MB			B					MB		
	[E.15] Alteración accidental de la información	PP			B					B		
	[E.18] Destrucción de información	P			M					M		
	[E.19] Fugas de información	P			M					M		
	[E.23] Errores de mantenimiento / actualización de equipos (hardw	MB			B					MB		
	[E.25] Pérdida de equipos	MR			B					MB		
	[A.7] Uso no previsto	MB			B					MB		
	[A.11] Acceso no autorizado	P			M					M		
	[A.15] Modificación deliberada de la información	MB			B					MB		
	[A.18] Destrucción de información	P			M					M		
	[A.19] Divulgación de información	MB			B					MB		
	[A.25] Robo	PP			B					B		
	[A.26] Ataque destructivo	MB			B					MB		

Tabla 37 (continuación)

			Impacto					Riesgo				
			Dimensiones					Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Material impreso o digitalizado	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P			A					A		
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	P			M					M		
	[I.10] Degradación de los soportes de almacenamiento de la inforr	PP			B					B		
	[I. 11] Emanaciones electromagnéticas	PP			B					B		
	[E.1] Errores de los usuarios	P			A					A		
	[E.2] Errores del administrador	MB			B					MB		
	[E.15] Alteración accidental de la información	PP			B					B		
	[E.18] Destrucción de información	P			M					M		
	[E.19] Fugas de información	P			A					A		
	[E.23] Errores de mantenimiento / actualización de equipos (hardw	MB			B					MB		
	[E.25] Pérdida de equipos	MR			B					MB		
	[A.7] Uso no previsto	MB			B					MB		
	[A.11] Acceso no autorizado	P			M					M		
	[A.15] Modificación deliberada de la información	MB			B					MB		
	[A.18] Destrucción de información	P			M					M		
	[A.19] Divulgación de información	MB			B					MB		
	[A.25] Robo	PP			B					B		
	[A.26] Ataque destructivo	MB			B					MB		
[D] Datos / Información												
Datos vitales	[E. 1] Errores de los usuarios	MA	A	A	A			MA	MA	MA		
	[E. 2] Errores de administración	P	M	M	M			M	M	M		
	[E. 3. 4] Errores de configuración y monitorización	P	M	M	M			M	M	M		
	[E.15] Alteración accidental de la información	P	M	M	M			M	M	M		
	[E.18] Destrucción de información	P	M	M	M			M	M	M		
	[E.19] Fugas de información	P	M	M	M			M	M	M		
	[A.3] Manipulación de los registros de actividad (log)	PP	B	B	B			B	B	B		
	[A.4] Manipulación de la configuración	PP	B	B	B			B	B	B		
	[A.5] Suplantación de la identidad del usuario	P	A	M	A			A	M	A		
	[A.6] Abuso de privilegios de acceso	P	M	M	M			M	M	M		
	[A.11] Acceso no autorizado	P	M	A	M			M	A	M		
	[A.15] Modificación deliberada de la información	PP	B	B	B			B	B	B		
	[A.18] Destrucción de información	PP	B	B	B			B	B	B		
	[A.19] Divulgación de información	MB	B	B	B			MB	MB	MB		

Tabla 37 (continuación)

			Impacto					Riesgo				
			Dimensiones					Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Código fuente	[E. 1] Errores de los usuarios	PP	B	B	B			B	B	B		
	[E. 2] Errores de administración	PP	B	B	B			B	B	B		
	[E. 3. 4] Errores de configuración y monitorización	PP	B	B	B			B	B	B		
	[E.15] Alteración accidental de la información	MA	A	A	A			MA	MA	MA		
	[E.18] Destrucción de información	P	M	M	M			M	M	M		
	[E.19] Fugas de información	P	M	M	M			M	M	M		
	[A.3] Manipulación de los registros de actividad (log)	P	M	M	M			M	M	M		
	[A.4] Manipulación de la configuración	P	M	M	M			M	M	M		
	[A.5] Suplantación de la identidad del usuario	P	M	M	M			M	M	M		
	[A.6] Abuso de privilegios de acceso	P	M	M	M			M	M	M		
	[A.11] Acceso no autorizado	P	M	M	M			M	M	M		
	[A.15] Modificación deliberada de la información	PP	B	B	B			B	B	B		
	[A.18] Destrucción de información	PP	B	B	B			B	B	B		
	[A.19] Divulgación de información	PP	B	B	B			B	B	B		
Código ejecutable	[E. 1] Errores de los usuarios	PP	B	B	B			B	B	B		
	[E. 2] Errores de administración	PP	B	B	B			B	B	B		
	[E. 3. 4] Errores de configuración y monitorización	PP	B	B	B			B	B	B		
	[E.15] Alteración accidental de la información	MA	A	A	A			MA	MA	MA		
	[E.18] Destrucción de información	P	M	M	M			M	M	M		
	[E.19] Fugas de información	P	M	A	M			M	A	M		
	[A.3] Manipulación de los registros de actividad (log)	P	A	M	M			A	M	M		
	[A.4] Manipulación de la configuración	P	M	M	M			M	M	M		
	[A.5] Suplantación de la identidad del usuario	P	M	M	M			M	M	M		
	[A.6] Abuso de privilegios de acceso	P	M	M	M			M	M	M		
	[A.11] Acceso no autorizado	P	M	M	M			M	M	M		
	[A.15] Modificación deliberada de la información	PP	B	B	B			B	B	B		
	[A.18] Destrucción de información	PP	B	B	B			B	B	B		
	[A.19] Divulgación de información	PP	B	B	B			B	B	B		

Tabla 37 (continuación)

			Impacto					Riesgo				
			Dimensiones					Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Datos de prueba	[E. 1] Errores de los usuarios	P	M	M	A			M	M	A		
	[E. 2] Errores de administración	PP	B	B	B			B	B	B		
	[E. 3. 4] Errores de configuración y monitorización	PP	B	B	B			B	B	B		
	[E.15] Alteración accidental de la información	PP	B	B	B			B	B	B		
	[E.18] Destrucción de información	P	M	M	M			M	M	M		
	[E.19] Fugas de información	P	M	M	M			M	M	M		
	[A.3] Manipulación de los registros de actividad (log)	P	M	M	M			M	M	M		
	[A.4] Manipulación de la configuración	P	M	M	M			M	M	M		
	[A.5] Suplantación de la identidad del usuario	P	M	M	M			M	M	M		
	[A.6] Abuso de privilegios de acceso	MB	B	B	B			MB	MB	MB		
	[A.11] Acceso no autorizado	P	M	M	M			M	M	M		
	[A.15] Modificación deliberada de la información	MB	B	B	B			MB	MB	MB		
	[A.18] Destrucción de información	P	M	M	M			M	M	M		
	[A.19] Divulgación de información	MB	B	B	B			MB	MB	MB		
[P] Persona												
Usuarios internos y externos	[E. 7] Deficiencia en la organización	PP	B	B	B			B	B	B		
	[E. 19] Fugas de información	PP	B	B	B			B	B	B		
	[E. 28] Indisponibilidad del personal	P	M	M	M			M	M	M		
	[A. 29] Extorsión	MB	B	B	B			MB	MB	MB		
	[A.30] Ingeniería social (picaresca)	P	M	A	M			M	A	M		
[L] Instalaciones												
Centro Principal de procesamiento	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	A					A				
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	P	M					M				
	[I. 11] Emanaciones electromagnéticas	PP	B					B				
	[E.15] Alteración accidental de la información	PP	B					B				
	[E.19] Fugas de información	P	M					M				
	[E.18] Destrucción de información	P	M					M				
	[A.11] Acceso no autorizado	PP	B					B				
	[A.15] Modificación deliberada de la información	MB	B					MB				
	[A.18] Destrucción de información	MB	B					MB				
	[A.19] Divulgación de información	MB	B					MB				
	[A.26] Ataque destructivo	PP	B					B				

Tabla 37 (continuación)

			Impacto					Riesgo				
			Dimensiones					Dimensiones				
Activos	**Amenazas**	**Probabili**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Centro Alterno de procesamiento	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	M					M				
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	P	M					M				
	[I. 11] Emanaciones electromagnéticas	PP	B					B				
	[E.15] Alteración accidental de la información	PP	B					B				
	[E.19] Fugas de información	P	M					M				
	[E.18] Destrucción de información	P	M					M				
	[A.11] Acceso no autorizado	PP	B					B				
	[A.15] Modificación deliberada de la información	MB	B					MB				
	[A.18] Destrucción de información	MB	B					MB				
	[A.19] Divulgación de información	MB	B					MB				
	[A.26] Ataque destructivo	PP	B					B				
Edificio Casa Matriz	[N. 1. 2.-*] De origen natural (agua y fuego)-Desastres naturales	P	M					M				
	[I. 1.2.-*.4.5.6 y 7] De origen Industrial (agua y fuego)-Desastres industriales, contaminación mecánica, electromecánica, avería de origen físico y lógico, Corte de suministro eléctrico y condiciones de inadecuadas de temperatura y humedad.	P	M					M				
	[I. 11] Emanaciones electromagnéticas	PP	B					B				
	[E.15] Alteración accidental de la información	PP	B					B				
	[E.19] Fugas de información	P	M					M				
	[E.18] Destrucción de información	P	M					M				
	[A.11] Acceso no autorizado	PP	B					B				
	[A.15] Modificación deliberada de la información	MB	B					MB				
	[A.18] Destrucción de información	MB	B					MB				
	[A.19] Divulgación de información	MB	B					MB				
	[A.26] Ataque destructivo	PP	B					B				

Fuente: El autor

Dado el análisis de riesgos anterior, se identifica los activos con mayor riesgo, dentro de los cuales se encuentran: los sistemas de información operacionales (SIARP, SISE, MIDAS y NEON); los servicios como: la gestión de identidades y privilegios, la red local, red telefónica, y los datos críticos de la entidad a saber: datos vitales, código fuente y código ejecutable.

Establecido el nivel del riesgo al que están expuestos los ya mencionados activos informáticos se procede a la selección de controles basados en la norma ISO/IEC 27002:2013 a fin de que las amenazas no se materialicen o si se da el caso, el impacto sobre el activo sea el menor posible.

Se propone el plan de tratamiento para los riesgos con nivel Muy alto y Alto, en la tabla No. 38

Tabla 38 Plan de tratamiento

ACTIVOS AFECTADOS	AMENAZA	RIESGO	PLAN DE TTO	DRESCRIPCION DEL PLAN DE ACCION	RESPONSABLE
Área de informática, bases de datos, cuartos de Rack, Data center alterna, Directorio Activo, Equipos de seguridad perimetral, Servidores de Administración, Servidores de Bases de datos de producción, Servidores de aplicaciones de producción, Plataforma de correo	Acceso no autorizado	Muy Alto	Mitigar el riesgo	Gestionar pruebas de hacking ético trimestrales, Monitorear los Logs mediante aplicaciones para este fin (adquirirlas)	Gerencia de infraestructura
Bases de datos, inventario de activos, Servidores administración	Fugas de Información	Muy Alto	Eliminar el riesgo	Implementar políticas de control de acceso, contraseñas seguras y pantalla y escritorio limpio	Gerencia de infraestructura
Bases de datos, Equipos de seguridad perimetral, servidores de producción (Administración, bases de datos, aplicaciones), plataforma de correo	Ataques internos o externos (Hacking, ingeniería social)	Alto	Mitigar el riesgo	Realizar pruebas de hacking ético para validar el grado de vulnerabilidad de los sistemas de información	Gerencia de infraestructura
Bases de datos, inventario de activos, Servidores de producción (Administración, bases de datos, aplicaciones),plata forma de correo	Suplantación de la identidad del usuario	Alto	Eliminar el riesgo	Revisar bimestralmente la gestión de usuarios (estado, privilegios, perfiles, control de acceso y aplicaciones)	Gerencia de infraestructura
Bases de datos, Data center, directorio activo, Red LAN, red WAN, servidores de producción (Administración, bases de datos, aplicaciones), plataforma de Correo, Equipos de seguridad perimetral	Errores del Usuario	Muy Alto	Eliminar el riesgo	Capacitar periódicamente al equipo de la Vicepresidencia de TICS, aplicar el control de cambios y validar la aprobación por el comité	Gerencia de infraestructura
Red LAN, Red WAN, Correo	Interceptación no autorizada de información en transito	Alto	Mitigar el riesgo	Implementar la política de cifrado de información y adquirir las herramientas necesarias para ello	Gerencia de infraestructura

Tabla 38 (continuación)

ACTIVOS AFECTADOS	AMENAZA	RIESGO	PLAN DE TTO	DRESCRIPCION DEL PLAN DE ACCION	RESPONSABLE
Bases de datos, inventario de activos, servidores de administración, servidores de bases de datos de producción, servidores de aplicaciones de producción.	alteración accidental de la información	Muy Alto	Eliminar el riesgo	verificar la eficiencia en la gestión de usuarios, velar por que todo cambio en las aplicaciones o sistemas	Gerencia de infraestructura
Bases de datos, Data center alterno, inventario de activos, Red LAN, Red WAN, servidores de bases de datos de producción, servidores de administración, servidores de aplicación producción, plataforma de correo.	Uso inadecuado de sistemas que generan interrupción.	Alto	Evitar el riesgo	Validar la oportunidad de la política de uso adecuado de los sistemas de información	Gerencia de infraestructura
Data center alterno, inventario de activos, servidores de Administración, servidores de bases de datos de producción, servidores de aplicaciones de producción, plataforma de Correo	abuso de privilegios	Muy Alto	Eliminar el riesgo	Restringir la información y evitar el uso de los superusuarios	Gerencia de infraestructura
Bases de datos, inventario de activos, servidores de administración, servidores de bases de datos de producción, servidores de aplicaciones de producción, Plataforma de correo.	Uso no previsto	Muy Alto	Eliminar el riesgo	Promocionar el uso de contraseñas seguras Efectividad del Anti-spam	Gerencia de infraestructura Gerencia de Talento Humano.
Instalaciones de casa matriz Data center alterno Centro de operaciones alterno	De origen industrial	Alto	Mitigar el riesgo	efectuar las pruebas de contingencia trimestrales en el centro alterno de operaciones	Gerencia de Logística
Inventario de Activos, computadores, portátiles	vulnerabilidades de los programas	Muy Alto	Eliminar el riesgo	Verificar el cumplimiento de la política que restringe la configuración de los programas	Gerencia de soporte
Bases de datos, Data center alterno, inventario de activos, Red LAN, Red WAN, servidores de producción	Interceptación en los servicios	Alto	Eliminar el riesgo	Asegurar que todos los cambios en producción son aprobados por el comité	Gerencia de soporte

Fuente: El autor

9.1.2.5 Caracterización de las Salvaguardas

Las salvaguardas o contra medidas son procedimientos tecnológicos que tienen como finalidad reducir la probabilidad de ocurrencia de las amenazas y restringir el daño causado.

9.1.2.5.1 Identificación de las salvaguardas:

Se seleccionan las salvaguardas de acuerdo a los siguientes criterios:

1. Tipo de activos a proteger, 2. Dimensión o dimensiones de seguridad que requieren protección 3. Amenazas de las que necesitamos protegernos 4. Si existen salvaguardas alternativas.

Ilustración 30 Identificación de salvaguardas

Protecciones generales u Horizontales
Protección de los datos / información
Protección de las claves criptográficas
Protección de los servicios
Protección de los equipos (hardware)
Protección de las comunicaciones
Protección en los puntos de interconexión con otros sistemas
Protección de los soportes de información
Protección de los elementos auxiliares
AUX.power Suministro eléctrico
Seguridad física
Salvaguardas relativas al persona

Fuente: El autor

- Las salvaguardas seleccionadas en materia de protección general se encuentran las herramientas de análisis de vulnerabilidades, de logs, Gestión de vulnerabilidades y de registro y control, pues como ya se ha mencionado anteriormente la entidad cuenta con la detección de incidentes pero no cuenta con herramientas para gestionar los riesgos que puedan afectar sus activos de información. Es por esta razón que las herramientas en mención le permitirán a la Positiva Compañía de Seguros S.A. gestionar

el riesgo de manera apropiada y tomar decisiones encaminadas a la mitigación de los mismos.

- Por su parte la protección de datos/ información y las claves criptográficas fueron seleccionadas las salvaguardas de Cifrado en la información, aseguramiento de la integridad, uso de firmas electrónicas y Gestión de clave criptográficas debido a que los código fuente, código ejecutable y las bases de pruebas se gestionan en un servidor al que tienen acceso muchos usuarios, y es susceptible a ataques externos.

- Protección de aplicaciones informáticas

Positiva Compañía de Seguros S.A. carece de políticas en materia de seguridad informática por tal razón se establece

- ✓ Políticas sobre el uso autorizado de aplicaciones y cumplimiento de los derechos de autor
- ✓ Determinación de procedimiento para la realización de copias de seguridad y cifrado de las mismas

- Aplicación de perfiles de seguridad, aunque la entidad cuenta con algunas restricciones se seleccionó esta salvaguarda para afrontar amenazas tales como Errores de usuarios, difusión de código dañino, vulnerabilidades del software para las plataformas Positiva cuida y expediente digital, Errores de mantenimiento y uso no previsto. Esta salvaguarda además debe permitir lograr la seguridad en los ficheros de datos de aplicación, ficheros de configuración y asegurar los mecanismos de comunicación entre procesos.

- Protección de equipos informáticos: Dado que la entidad cuenta con 60 estaciones de trabajo fijas y algunas externas se adoptaron las salvaguardas adecuadas para la protección de estos equipos, a saber:

- Disposición de normas para el bueno uso y procedimientos de uso para los equipos informáticos.

- Igualmente se aplican perfiles de seguridad: con el fin de minimizar las amenazas como errores del administrador del sistema, de bases de datos, uso no previsto y acceso no autorizado.

- Protección física: Aunque la entidad bajo análisis cuenta con sistema biométrico, tarjetas de aproximación y otros mecanismos de identificación de funcionarios es necesario tener en cuenta las salvaguardas de aseguramiento de la disponibilidad y terminación con el fin de proteger el acceso no autorizado e innecesario los servidores de datos.

- Protección de las instalaciones: Este factor cuenta con salvaguardas de reforzamiento de la seguridad del perímetro de la organización.

- Protección de comunicaciones: Como la información tratada obedece a un sector altamente sensible y blanco de ataques cibernéticos es necesario garantizar la confidencialidad e integridad de la misma por tanto la entidad debe tener en cuenta las salvaguardas de: aseguramiento de disponibilidad, autenticación del canal, protección de la integridad de los datos intercambiados, protección criptográfica de la confidencialidad de los datos intercambiados y seguridad en la red local y móvil; esto además de enfrentar amenazas tales como: Errores de re-encaminamiento, de secuencia, alteraciones en la información , uso no previsto, re encaminamiento de mensajes, alteración de secuencia y acceso no autorizado.

- Protección de los soportes de información: Para este aspecto se eligió la salvaguarda de aseguramiento de la disponibilidad y protección criptográfica del contenido, también se dictaminan políticas relacionadas a la protección criptográfica de los contenidos.

- Gestión del personal: En términos de personal es necesario sensibilizar a todos los colaboradores sobre la seguridad informática, establecer políticas de confidencialidad y exclusividad, gestión de contratos y determinación de procedimientos sobre el uso adecuado de los activos informáticos.

9.1.2.5.2 Valoración de las Salvaguardas

Consiste en determinar la eficacia de las salvaguardas, mediante los criterios descritos en la siguiente tabla:

Tabla 39 Criterios de valoración

Eficacia	Nivel	Madurez	Estado	Significado
0%	L0	Inexistente	Inexistente	Procedimiento: No se realiza Elementos: No se tiene Documentos: No se tienen
10%	L1	Iniciando	Iniciando	Procedimiento: Se está empezando hacer o solo una parte las gestiona Elementos: Se tienen pero no son usados Documentos: En preparación
50%	L2	Reproducible pero intuitivo	Parcialmente realizado	Procedimiento: Se realizan de la misma forma pero no está documentado Elementos: Existen pero están en proceso de adaptación Documentos: Se están elaborando
90%	L3	Proceso definido	En funcionamiento	Procedimiento: Se realizan de la misma forma y está documentado Elementos: Se tienen y funcionan correctamente Documentos: Existen
95%	L4	Gestionado y medible	Monitorizado	Procedimiento: Son medibles por indicadores Elementos: Indicadores Documentos: Soportados por indicadores
100%	L5	Optimizado	Mejora continua	Procedimiento: Se revisan indicadores, se proponen mejores y se aplican Elementos: Indicadores y mejoras Documentos: Indicadores y mejoras documentadas

Fuente: Herramienta PILAR 5.2.9

Tabla 40 Estimación de las salvaguardas

TIPO DE SALVAGUARDA	EFICACIA	NIVEL	MADUREZ	ESTADO
Protecciones generales u Horizontales				
H.tools.VA Herramienta de análisis de vulnerabilidad	50%	L2	REPRODUCIBLE, PERO INTUITIVO	INICIADO
H.tools.LA Herramienta para análisis de logs	50%	L2	REPRODUCIBLE, PERO INTUITIVO	INICIADO
H.VM Gestión de vulnerabilidades	50%	L2	REPRODUCIBLE, PERO INTUITIVO	INICIADO
H.AU Registro y auditoría	50%	L2	REPRODUCIBLE, PERO INTUITIVO	INICIADO
Protección de los datos / información				
D.A Copias de seguridad de los datos (backup)	50%	L2	REPRODUCIBLE, PERO INTUITIVO	INICIADO
D.I Aseguramiento de la integridad	10%	L1	INICIAL/AD HOC	INICIANDO
D.C Cifrado de la información	10%	L1	INICIAL/AD HOC	INICIANDO
D.DS Uso de firmas electrónicas	10%	L1	INICIAL/AD HOC	INICIANDO
D.TS Uso de servicios de fechado electrónico (time st	10%	L1	INICIAL/AD HOC	INICIANDO
Protección de las claves criptográficas				
K Gestión de claves criptográficas	10%	L1	INICIAL/AD HOC	INICIANDO
K.IC Gestión de claves de cifra de información	10%	L1	INICIAL/AD HOC	INICIANDO
K.DS Gestión de claves de firma de información	10%	L1	INICIAL/AD HOC	INICIANDO
K.disk Gestión de claves para contenedores criptográ	10%	L1	INICIAL/AD HOC	INICIANDO
K.comms Gestión de claves de comunicaciones	10%	L1	INICIAL/AD HOC	INICIANDO
K.509 Gestión de certificados	10%	L1	INICIAL/AD HOC	INICIANDO
Protección de los servicios				
S Protección de los Servicios	50%	L2	REPRODUCIBLE, PERO INTUITIVO	INICIADO
S.A Aseguramiento de la disponibilidad	50%	L2	REPRODUCIBLE, PERO INTUITIVO	INICIADO
S.start Aceptación y puesta en operación	50%	L2	REPRODUCIBLE, PERO INTUITIVO	INICIADO
S.SC Se aplican perfiles de seguridad	90%	L3	PROCESO DEFINIDO	EN FUNCIONAMIENTO
S.CM Gestión de cambios (mejoras y sustituciones)	90%	L3	PROCESO DEFINIDO	EN FUNCIONAMIENTO
S.www Protección de servicios y aplicaciones web	90%	L3	PROCESO DEFINIDO	EN FUNCIONAMIENTO
S.email Protección del correo electrónico	90%	L3	PROCESO DEFINIDO	EN FUNCIONAMIENTO
S.dir Protección del directorio	50%	L2	REPRODUCIBLE, PERO INTUITIVO	INICIADO
S.dns Protección del servidorde nombres de dominio	50%	L2	REPRODUCIBLE, PERO INTUITIVO	INICIADO
6.5. Protección de las aplicaciones (software)	50%	L2	REPRODUCIBLE, PERO INTUITIVO	INICIADO
SW Protección de las Aplicaciones Informáticas	50%	L2	REPRODUCIBLE, PERO INTUITIVO	INICIADO
SW.A Copias de seguridad (backup)	50%	L2	REPRODUCIBLE, PERO INTUITIVO	INICIADO
SW.start Puesta en producción	50%	L2	REPRODUCIBLE, PERO INTUITIVO	INICIADO
SW.SC Se aplican perfiles de seguridad	90%	L3	PROCESO DEFINIDO	EN FUNCIONAMIENTO
SW.op Explotación / Producción	90%	L3	PROCESO DEFINIDO	EN FUNCIONAMIENTO
SW.CM Cambios (actualizaciones y mantenimiento)	90%	L3	PROCESO DEFINIDO	EN FUNCIONAMIENTO

Tabla 40 (continuación)

TIPO DE SALVAGUARDA	EFICACIA	NIVEL	MADUREZ	ESTADO
Protección de los equipos (hardware)				
HW Protección de los Equipos Informáticos	10%	L1	INICIAL/AD HOC	INICIANDO
HW.start Puesta en producción	50%	L2	REPRODUCIBLE, PERO INTUITIVO	INICIADO
HW.SC Se aplican perfiles de seguridad	10%	L1	INICIAL/AD HOC	INICIANDO
HW.A Aseguramiento de la disponibilidad	10%	L1	INICIAL/AD HOC	INICIANDO
HW.op Operación	50%	L2	REPRODUCIBLE, PERO INTUITIVO	INICIADO
HW.CM Cambios (actualizaciones y mantenimiento)	10%	L1	INICIAL/AD HOC	INICIANDO
Protección de las comunicaciones				
COM Protección de las Comunicaciones	50%	L2	REPRODUCIBLE, PERO INTUITIVO	INICIADO
COM.start Entrada en servicio	50%	L2	REPRODUCIBLE, PERO INTUITIVO	INICIADO
COM.SC Se aplican perfiles de seguridad	10%	L1	INICIAL/AD HOC	INICIANDO
COM.A Aseguramiento de la disponibilidad	10%	L1	INICIAL/AD HOC	INICIANDO
COM.aut Autenticación del canal	10%	L1	INICIAL/AD HOC	INICIANDO
COM.I Protección de la integridad de los datos interc	10%	L1	INICIAL/AD HOC	INICIANDO
COM.C Protección criptográfica de la confidencialidad	10%	L1	INICIAL/AD HOC	INICIANDO
COM.internet Internet: uso de ? acceso a	50%	L2	REPRODUCIBLE, PERO INTUITIVO	INICIADO
COM.wifi Seguridad Wireless (WiFi)	50%	L2	REPRODUCIBLE, PERO INTUITIVO	INICIADO
COM.DS Segregación de las redes en dominios	50%	L2	REPRODUCIBLE, PERO INTUITIVO	INICIADO
Protección en los puntos de interconexión con otros sistemas				
IP Puntos de interconexión: conexiones entre zonas	90%	L3	PROCESO DEFINIDO	EN FUNCIONAMIENTO
IP.SPP Sistema de protección perimetral	90%	L3	PROCESO DEFINIDO	EN FUNCIONAMIENTO
IP.BS Protección de los equipos de frontera	90%	L3	PROCESO DEFINIDO	EN FUNCIONAMIENTO
Protección de los soportes de información				
MP Protección de los Soportes de Información	10%	L1	INICIAL/AD HOC	INICIANDO
MP.A Aseguramiento de la disponibilidad	10%	L1	INICIAL/AD HOC	INICIANDO
MP.IC Protección criptográfica del contenido	10%	L1	INICIAL/AD HOC	INICIANDO
Protección de los elementos auxiliares				
AUX Elementos Auxiliares	90%	L3	PROCESO DEFINIDO	EN FUNCIONAMIENTO
AUX.A Aseguramiento de la disponibilidad	90%	L3	PROCESO DEFINIDO	EN FUNCIONAMIENTO
AUX.start Instalación	90%	L3	PROCESO DEFINIDO	EN FUNCIONAMIENTO
AUX.power Suministro eléctrico				
AUX.AC Climatización	90%	L3	PROCESO DEFINIDO	EN FUNCIONAMIENTO
AUX.wires Protección del cableado	90%	L3	PROCESO DEFINIDO	EN FUNCIONAMIENTO
Seguridad física – Protección de las instalaciones				
Protección de las Instalaciones	90%	L3	PROCESO DEFINIDO	EN FUNCIONAMIENTO
L.A Aseguramiento de la disponibilidad	50%	L2	REPRODUCIBLE, PERO INTUITIVO	INICIADO
L.end Terminación	50%	L2	REPRODUCIBLE, PERO INTUITIVO	INICIADO
Salvaguardas relativas al persona				
PS Gestión del Personal	10%	L1	INICIAL/AD HOC	INICIANDO
PS.AT Formación y concienciación	10%	L1	INICIAL/AD HOC	INICIANDO
PS.A Aseguramiento de la disponibilidad	10%	L1	INICIAL/AD HOC	INICIANDO

Fuente: El autor.

9.2 Fase 3: Determinar y evaluar la aplicabilidad de los controles de seguridad de la información bajo la norma ISO/IEC 27002:2013

9.2.1 Diagnóstico inicial grado de cumplimiento objetivos de controles y controles

A través de una lista de chequeo, estructurada mediante secciones en las que se evaluaban algunos objetivos de control y controles y con elección de respuesta en la escala SI, NO y N/S, se llevó a cabo, el diagnostico con respecto al cumplimiento de los requerimientos establecidos en el Anexo A del estándar ISO/IEC 27001:2013, a continuación el análisis:

- **Análisis de las respuestas obtenidas**

El primer aspecto evaluado corresponde a la política de seguridad de la información, los entrevistados coincidieron en que, no hay definida una política de seguridad de la información, que oriente el manejo de los recursos informáticos de la entidad, y reconocen que es importante que se establezca y se incorporen algunos otros lineamientos que existen en la entidad como la política de Continuidad del negocio, política de copias de respaldo, política administración de estaciones de trabajo entre otras que aunque están documentadas deben ser reevaluadas para determinar su pertinencia y que a su vez pueden complementar y dar soportar a la política de seguridad de la información que se determine en el futuro.

Dado que a su cargo están las gerencias que gestionan todo el tema informático en la entidad, se acordó que se realizara al interior de estas áreas una reunión con algunos profesionales para encomendarles la labor de proponer una política de seguridad de la información, la cual será debatida en el comité primario que se realiza cada mes por área y una vez se llegue a un consenso y se precise la política esta será presentada en el comité de presidencia para que esta sea considerada por los directivos y a su vez se realice la gestión de aprobación por parte de la Junta Directiva.

Seguidamente, el tema tratado corresponde a los objetivos de control denominado organización de la seguridad de la información, en este caso, se puedo apreciar que en la entidad no se cuenta con un espacio específico para la gestión de actividades de seguridad de la información, pues hasta el momento ha sido un tema de poco interés por parte de la organización, sin embargo, y debido a las

exigencias propias de la actividad de la aseguradora, se ha generado la necesidad de considerar el tema. En tanto a los aspectos cuestionados en esta sección, se verifico que la aseguradora, nunca ha tenido un asesoramiento en materia de seguridad informática y tampoco ha sido contemplado en las ultimas contrataciones, por su parte en materia contractual, tampoco son exigidas clausulas o manifiestos de seguridad de la información a los proveedores que contratan con Positiva dado que no están divisados como un requisito esencial.

El siguiente objetivo de control analizado en el cuestionario corresponde a la clasificación de activos informáticos, en este se pudo establecer, que la entidad cuenta con un inventario de bienes informáticos realizado en 2008 y del cual no se ha realizado ninguna actualización, no es un inventario formal y debidamente documentado por tanto no se considera. Los gerentes reconocen que esta labor es de suma importancia y a la cual no se le deben dar más largas.

El Gerente de Soporte TI, informa que esta tarea se ha venido desarrollando por parte de los funcionarios a su cargo, pero se han dado ciertos inconvenientes como el cambio de personal y esta actividad se ha retrasado pues es un compromiso que esta gerencia había adquirido tiempo atrás y a la fecha no se ha culminado; igualmente indica que se busca que este inventario sea automático y que refleje la actualidad de los bienes y su necesidad de protección.

- **Políticas de personal respecto a la seguridad de la información**

Debido a que en la entidad no se tiene una cultura de seguridad de la información los incidentes de seguridad no son reportados pues a pesar de tener herramientas que permiten el reporte de estos, no son conocidos por los usuarios y tampoco han sido capacitados para ello, es un compromiso que en el momento de la aplicación de este cuestionario es aceptado por el gerente de infraestructura pues es función de este, socializar los mecanismos de gestión de incidentes con los que cuenta la entidad y a su vez promocionar una cultura de seguridad de la información de todos los usuarios de los sistemas de información.

La aplicación de los acuerdos de confidencialidad de la información son meramente un requisito al momento de la firma del contrato, pero no se da la importancia que tiene este como medida de prevención para contrarrestar la fuga de información que pueda suscitarse.

Seguridad física y ambiental: Afortunadamente existen en Casa Matriz, controles de autenticación de personal y control de acceso a las áreas seguras mediante tarjetas de proximidad y sistema biométrico; en tanto a la oportuna respuesta a

incidentes de tipo físico se está preparado para afrontar cualquier falla materializada en el entorno, pues se cuenta con un data center alterno que permite gestionar los procesos críticos para la operación de forma tal que se pueda continuar prestando los servicios sin interrupción alguna.

Gestión de las comunicaciones de datos y operaciones en los sistemas informáticos.

Las preguntas formuladas en este aparte, permitieron identificar que la entidad cuenta con antivirus actualizado periódicamente y antispyware, igualmente tiene un registro de los accesos a los sistemas de información en el que se indica el usuario, la hora y fecha de acceso y el tiempo dentro de la aplicación, las modificaciones o tareas efectuadas y los reportes gestionados.

Existe un compromiso con respecto al uso de los recursos informáticos que es acatado por todos los colaboradores; no obstante, a la fecha se ha detectado que el uso de internet representa un verdadero abuso por parte de los usuarios pues se invierte demasiado tiempo destinado para las labores asignadas a consulta de temas que no están relacionados con la compañía, por lo cual se dispuso de un informe mensual en el que se registra el usuario y el tiempo que dura en internet el cual es remitido a cada vicepresidente para que tome las medidas pertinentes.

En cuanto a los medios de almacenamiento está prohibido el uso de medios particulares que no estén avalados por la gerencia de infraestructura, únicamente se permite el almacenamiento de la información en los discos duros de los equipos de cómputo y en el fileserver.

- **Control de acceso:** Los gerentes indican que todas las aplicaciones utilizadas en Casa Matriz requieren de un usuario y contraseña, la cual es bloqueada cuando el usuario intenta ingresar sin éxito más de tres veces, para desbloquear el usuario, la persona debe colocar un caso Aranda dirigido a la mesa de ayuda para que sea reestablecida la contraseña. Las claves de acceso nuevas son gestionadas por la gerencia de Soporte TI, las cuales son genéricas y deben cambiarse en el primer inicio de sesión. Cuando un funcionario sale a vacaciones el acceso es bloqueado y reestablecido una vez se haya finalizado el periodo de descanso, esto se da previa autorización del gerente de área o vicepresidente según sea el caso, si por el contrario el colaborador finaliza su relación contractual debe solicitar mediante caso Aranda su baja como usuario del sistema de información con visto bueno del jefe inmediato o quien haga las veces.

Las conexiones remotas son realizadas mediante VPN facilitadas por la entidad, y solo tienen acceso a estas, los funcionarios autorizados por los jefes inmediatos y previa justificación del uso de este medio, los ingresos son monitoreados por la Gerencia de Infraestructura.

Desarrollo y mantenimiento de sistemas informáticos

Aquí se formularon preguntas como:

En cuanto al desarrollo de aplicaciones ¿se tienen controles de validación de datos de entrada y de salida? A la cual contestaron los gerentes, que efectivamente existe un control de validación de datos previamente establecidos por la Vicepresidencia de TIC´S y avalados por la Junta Directiva de la entidad. Igualmente están debidamente documentados en el estándar "VA-OD-ESSI-02 Estándar de Seguridad de los Sistemas de información", aunque fueron enfáticos en indicar que esta documentación es de años atrás y que debe ser revisada.

En tanto al cifrado de la información, indicaron que los controles establecidos no son los más oportunos y que deben rediseñarse y documentarse adecuadamente pues es importante que la información de la entidad se encripte para evitar que esta sea violada o manipulada por personas inescrupulosas.

Se encuentran implementados y total funcionamiento los controles que evitan el acceso no autorizado a los códigos fuente de las aplicaciones; los controles de cambio en las aplicaciones son debidamente gestionados, soportados y registrados por parte de las dos gerencias.

Los códigos fuente desarrollados por personal externo son validados, probados y avalados antes de ser puestos en producción como medida de seguridad, esto se encuentra documentado en el VTI-OD-EAET-01_ESTANDAR DE ASEGURAMIENTO DE ESTACIONES DE TRABAJO.

Gestión de incidentes: Existen controles y herramientas para la gestión de incidentes. El VTI-OD-EGI-05 Estándar de Gestión de Incidentes, creado por la Gerencia de infraestructura, es la guía en la que se establecen formalmente los reportes de incidentes, el procedimiento a seguir, la herramienta dispuesta para tal fin y las pautas de levantamiento de información, análisis e investigación de todo lo concerniente a las causas que originaron el incidente informático; no obstante, no se ha definido un equipo que se haga cargo de brindar respuestas una vez se dé el reporte del incidente, en este caso se cuenta con las medidas pero no con el personal calificado para que gestione esta labor, es relevante evaluar la creación

de un equipo que se haga cargo de la gestión de incidentes informáticos, pues aunque esté debidamente documentado, las acciones no son realizadas, por tanto se puede concluir que este control no cumple a cabalidad con los requisitos establecidos en la norma ISO/IEC 27002:2013.

Plan de continuidad: Dado que Positiva es una entidad con participación estatal, está obligada a contar con un plan de continuidad del negocio para garantizar la prestación de sus servicios, y la recuperación de su operación ante cualquier incidente de tipo natural, político, social o técnico.

Dicho plan, está contemplado por cada proceso crítico, es decir, que por cada proceso existe una guía para la recuperación de las actividades. Anualmente se realizan dos ejercicios de prueba de continuidad del negocio, en el centro de operaciones alterno ubicado en el segundo piso del edificio de compensar, allí se tiene dispuestos las elementos necesarios para que en caso de emergencia Positiva pueda continuar su negocio sin ninguna interrupción y se pueda recuperar en el menor tiempo posible.

La activación del plan de contingencia precisa las acciones a tomar una vez se dé la perturbación en los servicios críticos de Casa Matriz. Generalmente se involucran las acciones para informar al personal de recuperación de desastres, llevar a cabo una evaluación del entorpecimiento y activar el plan.

- El plan solo será activado en el momento en que ocurra alguno de estos eventos:
- El tipo de desastre admita una limitación de los servicios en más de 4 horas.
- Desastres naturales (Inundaciones, Terremotos, Huracanes, etc.).
- Las instalaciones de Casa Matriz se encuentren totalmente destruidas.

- **Cumplimiento legal:** Positiva dada su naturaleza está obligada a adoptar todas las medidas legislativas que regulen sus operaciones y la interacción con otros entes, por tanto y de acuerdo a lo mencionado por los gerentes, se estableció que toda la normatividad regulatoria está debidamente identificada, socializada y acatada en todas las regionales, sucursales y por supuesta en Casa Matriz. Aquel que incurra en el incumplimiento de cualquier ley, será severamente penalizado, pues Positiva es garante del cumplimiento de las leyes.

En tanto a la normatividad regulatoria sobre la protección y privacidad de datos es de interés colectivo, por tanto todos los funcionarios conocen de esta normatividad, saben de su aplicación y acatamiento.

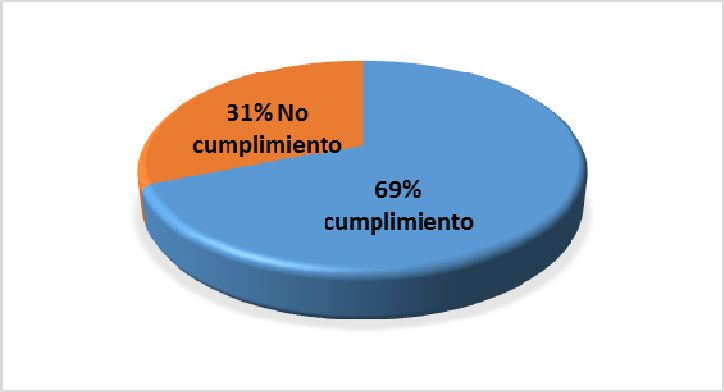
Mediante la entrevista efectuada al Gerente de Infraestructura y al Gerente de Soporte TIC´S se evidencia que la entidad aplica algunos controles, de acuerdo a la norma, sin embargo, muchos de ellos no están documentados y debidamente soportados, o en su defecto deben rediseñarse pues no solo los apropiados para la protección del bien informático sobre el cual se están efectuando.

9.2.2 Grado de cumplimiento del anexo A ISO/IEC 27001/2013, de acuerdo a la declaración de aplicabilidad

Mediante la declaración de aplicabilidad, se estableció que la entidad ha implementado cerca de 78 controles y ha dejado de efectuar 36, es decir, que Positiva cuenta con un nivel de cumplimiento del 69% con relación a lo determinado en el Anexo A de la norma ISO/IEC 27001:2013.

El estado de cumplimiento de los controles de dicho anexo, permite conocer el grado de madurez de la entidad con respecto a la seguridad de la información, resguardo de los bienes informáticos, acatamiento de la normatividad y por supuesto los riesgos a enfrentar a partir de los controles efectuados. El resultado obtenido es el representado en la siguiente gráfica:

Ilustración 31 Nivel de cumplimiento



Fuente: El autor

Por lo anterior, se puede concluir que la implementación del Sistema de Gestión de Seguridad de la información requerirá de adecuaciones, mejoras y adquisición de herramientas tecnológicas con el propositivo de garantizar la efectividad del mismo.

El SISTEMA SANSI[38] es un método de seguridad de la información manejado por la estrategia GEL en la cual se define el nivel de riesgo de las organizaciones, según el cumplimiento de los controles establecidos en la norma ISO/IEC 27002:2013. Estos tienen una valoración de Alto, Medio y Bajo. Positiva basada en esta clasificación definió la siguiente tabla de medición:

Tabla 41 Nivel de cumplimiento de controles Vs Nivel de riesgo

Grado de cumplimiento	Grado del riesgo	Implicaciones
Alto	Bajo	Los controles de seguridad efectuados demuestran un alto grado de protección de los activos de información. Esto simboliza para la compañía un riesgo bajo.
Medio	Medio	Existen controles definidos e implantados, sin embargo, algunos no están documentos o no son los apropiados y deben ser reevaluados. Es vital una verificación en un corto periodo de tiempo a fin de mejorar la efectividad y cumplimiento. Esto significa que el riesgo es medio pues se perciben vulnerabilidades en algunas de las medidas instauradas y esto puede desencadenar amenazas internas o externas.
Bajo	Alto	La falta de controles o el bajo nivel de cumplimiento en los mismos, significa un riesgo ALTO para la compañía. Es importante efectuar controles en un corto plazo con el objetivo de cerrar las brechas encontradas.

Fuente: El autor

[38] Modelo de Seguridad de la Información, SISTEMA SANSI - SGSI – Modelo de Seguridad de la información para la estrategia de gobierno en línea, Pág., 4

De acuerdo a la anterior tabla, se puede deducir que Positiva Compañía de Seguros S.A.-Casa Matriz con un 69% de cumplimiento, se encuentra en un grado medio de implementación con respecto a lo establecido en el estándar ISO/IEC 27002:2013 y en un nivel de riesgo medio con relación al nivel de protección y efectividad de los controles ya realizados.

9.2.3 Verificación de aplicabilidad de los objetivos de control y controles establecidos en la norma ISO/IEC 27002:2013

La verificación se basa en la declaración de aplicabilidad y los criterios descritos en la siguiente tabla:

Tabla 42 Criterios de aplicabilidad

Códigos	Significado
D	El control se documentó e implementó
MD	El Control se lleva a cabo, pero el proceso debe ser documentado a fin de garantizar la repetitividad del mismo y aminorar los riesgos.
RD	El control no cumple las normas y es necesario rediseñarlo para cumplir con estas
PNP	El proceso no está implementado. (Control requerido, no documentado y no implementado)
NA (Not Aplicable)	El control no es aplicable para la entidad

Fuente: El autor

Tabla 43 Estado de adopción de los objetivos de control y controles de acuerdo a la norma ISO/IEC 27002:2013

ANEXO	TITULO DEL CONTROL	Status
A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
5.1	**INFORMACIÓN POLÍTICA DE SEGURIDAD**	
5.1.1	POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	**PNP**
5.1.2	REVISIÓN DE LAS POLITICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	**PNP**
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		
6.1	**ORGANIZACIÓN INTERNA**	
6.1.1	ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN	**PNP**
6.1.2	SEPARACIÓN DE DEBERES	**RD**
6.1.3	CONTACTO CON LAS AUTORIDADES	**MD**
6.1.4	CONTACTO CON GRUPOS DE INTERÉS ESPECIAL	**MD**
6.1.5	SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS.	**PNP**
6.2	**DISPOSITIVOS MÓVILES Y TELETRABAJO**	
6.2.1	POLÍTICA PARA DISPOSITIVOS MÓVILES	**MD**
6.2.2	TELETRABAJO	**PNP**
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS		
A 7.1 ANTES DE ASUMIR EL EMPLEO		
7.1.1	SELECCIÓN	**D**
7.1.2	TÉRMINOS Y CONDICIONES DEL EMPLEO	**D**
A 7.2 DURANTE LA EJECUCIÓN DEL EMPLEO		
7.2.1	RESPONSABILIDADES DE LA DIRECCIÓN	**RD**
7.2.2	TOMA DE CONCIENCIA, EDUCACIÓN, Y FORMACIÓN EN S.I.	**PNP**
7.2.3	PROCESO DISCIPLINARIO	**MD**
A 7.3 TERMINACIÓN Y CAMBIO DE EMPLEO		
7.3	TERMINACIÓN O CAMBIO DE RESPONSABILIDADES DE EMPLEO	**D**
A.8 GESTION DE ACTIVOS		
A 8.1 RESPONSABILIDAD POR LOS ACTIVOS		
A 8.1.1	INVENTARIO DE ACTIVOS	**PNP**
A 8.1.2	PROPIEDAD DE LOS ACTIVOS	**RD**

ANEXO	TITULO DEL CONTROL	Status
A 8.1.3	USO ACEPTABLE DE LOS ACTIVOS	**MD**
A 8.1.4	DEVOLUCIÓN DE LOS ACTIVOS	**RD**
A 8.2 CLASIFICACIÓN DE LA INFORMACIÓN		
A 8.2.1	CLASIFICACIÓN DE LA INFORMACIÓN	**RD**
A 8.2.2	ETIQUETADO DE LA INFORMACIÓN	**PNP**
A 8.2.3	MANEJO DE ACTIVOS	**PNP**
A 8.3 MANEJO DE MEDIOS		
A 8.3.1.	GESTIÓN DE MEDIOS REMOVIBLES	**PNP**
A 8.3.2	DISPOSICIÓN DE LOS MEDIOS	**RD**
A 8.3.3	TRANSFERENCIA DE MEDIOS FÍSICOS	**PNP**
A.9 CONTROL DE ACCESO		
A 9.1 REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO		
A 9.1.1	POLÍTICA DE CONTROL DE ACCESO	**MD**
A 9.1.2	ACCESO A REDES Y A SERVICIOS EN RED	**RD**
A 9.2 GESTIÓN DE ACCESO DE USUARIOS		
A 9.2.1	REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS	**MD**
A 9.2.2	SUMINSITRO DE ACCESO DE USUARIOS	**MD**
A 9.2.3	GESTIÓN DE DERECHOS DE ACCESO PRIVILEGIADO	**MD**
A 9.2.4	GESTIÓN DE LA INF. DE AUTENTICACIÓN SECRETA DE USUARIOS	**MD**
A 9.2.5	REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIOS	**MD**
A 9.2.6	RETIRO O AJUSTE DE LOS DERECHOS DE ACCESO.	**MD**
A 9.3 RESPONSABILIDADES DE LOS USUARIOS		
A 9.3.1	USO DE INFORMACIÓN DE AUTENTICACIÓN SECRETA	**MD**
A 9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES		
A 9.4.1	RESTRICCIÓN DE ACCESO A LA INFORMACIÓN	**MD**
A 9.4.2	PROCEDIMIENTO DE INGRESO SEGURO.	**MD**
A 9.4.3	SISTEMA DE GESTIÓN DE CONTRASEÑAS.	**D**
A 9.4.4	USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS	**MD**
A 9.4.5	CONTROL DE ACCESO A CODIGOS FUENTE DE PROGRAMAS	**MD**

ANEXO	TITULO DEL CONTROL	Status
A. 10 CRIPTOGRAFIA		
A 10.1 CONTROLES CRIPTOGRAFICOS		
A 10.1.1	POLÍTICA SOBRE USO DE CONTROLES CRIPTOGRÁFICOS	**RD**
A 10.1.2	GESTIÓN DE LLAVES	**RD**
A. 11 SEGURIDAD FISICA Y DEL ENTORNO		
A 11.1 ÁREAS SEGURAS		
A 11.1.1	PERÍMETRO DE SEGURIDAD FÍSICA	**D**
A 11.1.2	CONTROLES DE ACCESO FÍSICOS	**MD**
A 11.1.3	SEGURIDAD DE OFICINAS, RECINTOS E INSTALACIONES	**MD**
A 11.1.4	PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES	**MD**
A 11.1.5	TRABAJO EN ÁREAS SEGURAS	**MD**
A 11.1.6	ÁREAS DE DESPACHO Y CARGA	**NA**
A 11.2 EQUIPOS		
A 11.2.1	UBICACIÓN Y PROTECCION DE LOS EQUIPOS	**MD**
A 11.2.2	SERVICIOS DE SUMINSITRO	**MD**
A 11.2.3	SEGURIDAD EN EL CABLEADO	**MD**
A 11.2.4	MANTENIMIENTO DE EQUIPOS	**MD**
A 11.2.5	RETIRO DE ACTIVOS	**RD**
A 11.2.6	SEGURIDAD DE EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES	**MD**
A 11.2.7	DISPOSICIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS	**RD**
A 11.2.8	EQUIPOS DE USUARIO DESATENDIDO	**RD**
A 11.2.9	POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA	**RD**
A.12 SEGURIDAD DE LAS OPERACIONES		
A 12.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES		
A 12.1.1	PROCEDIMIENTOS DE OPERACIÓN DOCUMENTADOS	**D**
A 12.1.2	GESTIÓN DE CAMBIOS	**D**
A 12.1.3	GESTIÓN DE CAPACIDAD	**D**
A 12.1.4	SEPARACION DE LOS AMBIENTES DE DESARROLLO, PRUEBAS Y OPERACIÓN.	**D**

ANEXO	TITULO DEL CONTROL	Status
A 12.2 PROTECCION CONTRA CODIGOS MALICIOSOS		
A.12.2.1	CONTROLES CONTRA CÓDIGOS MALICIOSOS	**D**
A 12.3 COPIAS DE RESPALDO		
A 12.3.1	RESPALDO DE LA INFORMACIÓN	**D**
A 12.4 REGISTRO Y SEGUIMIENTO		
A12.4.1	REGISTRO DE EVENTOS	**RD**
A12.4.1	PROTECCIÓN DE LA INFORMACIÓN DE REGISTRO	**RD**
A12.4.1	REGISTROS DEL ADMINSITRADOR Y DEL OPERADOR	**RD**
A12.4.1	SINCRONIZACIÓN DE RELOJES	**RD**
A 12.5 CONTROL DE SOFTWARE OPERACIONAL		
A 12.5.1	INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS	**RD**
A 12.6 GESTION DE LA VULNERABILIDAD TÉCNICA		
A 12.6.1	GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS	**RD**
A 12.6.2	RESTRICCIÓN SOBRE LA INSTALACION DE SOFWARE	**RD**
A 12.7 CONTROLES DE AUDITORIAS DE SISTEMAS DE INFORMACIÓN		
A 12.7	CONTROLES DE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	**PNP**
A. 13 SEGURIDAD DE LAS COMUNICACIONES		
A 13.1 GESTIÓN DE LA SEGURIDAD DE LAS REDES		
A 13.1.1	CONTROLES DE REDES	**MD**
A 13.1.2	SEGURIDAD DE LOS SERVICIOS DE RED	**MD**
A 13.1.3	SEPARACIÓN EN LAS REDES	**MD**
A 13.2 TRANSFERENCIA DE INFORMACIÓN		
A 13.2.1	POLÍTICAS Y PROCEDIMIENTOS DE TRASNFERENCIA DE INFORMACIÓN	**PNP**
A 13.2.2	ACUERDOS SOBRE TRASNFERENCIA DE INFORMACIÓN	**PNP**
A 13.2.3	MENSAJERIA ELECTRÓNICA	**D**
A 13.2.4	ACUERDOS DE CONFIDENCIALIDAD O DE NO DIVULGACIÓN	**D**
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS		
A 14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN		
A 14.1.1	ÁNALISIS Y ESPECIFICACIÓN DE REQUISITOS DE SI	**MD**
A 14.1.2	SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS	**MD**

ANEXO	TITULO DEL CONTROL	Status
A 14.1.3	PROTECCIÓN DE TRANSACCIONES DE LOS SERVICIOS DE LAS APLICACION	**MD**
A 14.2 CONTROL DE ACCESO AL SISTEMA OPERATIVO		
A 14.2.1	POLÍTICA DE DESARROLLO SEGURO	**MD**
A 14.2.2	PROCEDIMIENTO DE CONTROL DE CAMBIOS EN SISTEMAS	**MD**
A 14.2.3	REVISIÓN TÉCNICAS DE LAS APLICACIONES DESPUES DE CAMBIOS EN LA	**MD**
A 14.2.4	RESTRICCIONES EN LOS CAMBIOS A LOS PAQUETES DE SOFTWARE	**MD**
A 14.2.5	PRINCIPIOS DE CONSTRUCCIÓN DE LOS SISTEMAS SEGUROS	**MD**
A 14.2.6	AMBIENTE DE DESARROLLO SEGURO	**PNP**
A 14.2.7	DESARROLLO CONTRATADO EXTERNAMENTE	**MD**
A 14.2.8	PRUEBAS DE SEGURIDAD DE SISTEMAS	**MD**
A 14.2.9	PRUEBAS DE ACEPTACIÓN DE SISTEMAS	**MD**
A 14.3 DATOS DE PRUEBA		
A14.3.1	PROTECCIÓN DE DATOS DE PRUEBA	**RD**
A.15 RELACIONES CON LOS PROVEEDORES		
A. 15.1 RELACIONES CON LOS PROVEEDORES		
15.1.1	SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES	**MD**
15.1.2	TRATAMIENTO DE LA SEGURIDAD DENTRO DE LOS ACUERDOS CON PROVEEDORES	**MD**
15.1.3	CADENA DE SUMINISTRO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN	**MD**
A 15.2 GESTIÓN DE LA PRESENTACIÓN DE SERVICIOS DE PROVEEDORES		
15.2.1	SEGUIMIENTO Y REVISIÓN DE LOS SERVICIOS DE LOS PROVEEDORES	**MD**
15.2.2	GESTIÓN DE CAMBIOS EN LOS SERVICIOS DE LOS PROVEEDORES	**MD**
A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION		
16,1	**GESTION DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN**	
16.1.1	RESPONSABILIDADES Y PROCEDIMIENTOS	**PNP**

ANEXO	TITULO DEL CONTROL	Status
16.1.2	REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN	**PNP**
16.1.3	REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	**PNP**
16.1.4	EVALUACIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN Y	**PNP**
16.1.5	RESPUESTA A INCIDENTES DE SEGUIRIDAD DE LA INFORMACIÓN	**PNP**
16.1.6	APRENDIZAJE OBTENIDO DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	**PNP**
16.1.7	RECOLECCIÓN DE EVIDENCIA	**PNP**
A.17 ASPECTOS DE SEGURIDD DE LA INFORMACIÓN		
17.1 CONTINUIDD EN SEGURIDD DE L INFORMCIÓN		
17.1.1	PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	**D**
17.1.2	IMPLEMENTACIÓN DE LA CONTINUIDAD DE LA SI	**D**
17.1.3	VERIFICACIÓN, REVISIÓN Y EVALUACIÓN DE LA CONTINUIDAD DE LA SI	**D**
17.2 REDUNDNCIS		
17.2.1	DISPONIBILIDAD DE INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN	**D**
A. 18 CUMLPIMIENTO		
18.1 CUMPLIMIENTO DE REQUISITOS LEGLES Y CONTRCTULES		
18.1.1	IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE Y DE LOS REQUISITOS CONTRACTUALES.	**RD**
18.1.2	DERECHOS DE PROPIEDAD INTELECTUAL	**RD**
18.1.3	PROTECCIÓN DE REGISTROS	**RD**
18.1.4	PRIVACIDAD Y PROTECCIÓN DE INFORMACIÓN DE DATOS PERSONALES	**RD**
18.1.5	REGLAMENTACIÓN DE CONTROLES CRIPTOGRÁFICOS	**RD**
18.2 REVISIONES DE SEGURIDD DE L INFORMCIÓN		
18.2.1	REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN	**PNP**
18.2.2	CUMPLIMIENTO CON LAS POLÍTICAS	**PNP**
18.2.3	REVISIÓN DEL CUMPLIMIENTO TÉCNICO	**PNP**

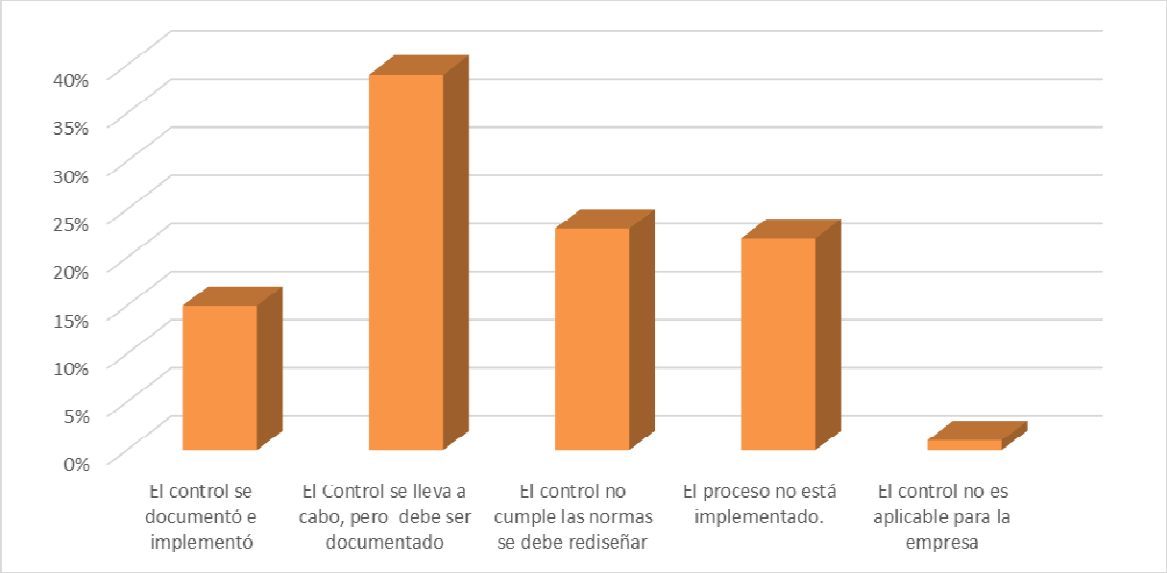
Fuente: El autor

Tabla 44 Resumen estado de adopción objetivos de control y controles

Cantidad	Códigos Status	Significado	Contribución %
17	D	El control se documentó e implementó	15%
45	MD	El Control se lleva a cabo, el proceso debe ser documentado a fin de garantizar la repetitividad del mismo y aminorar los riesgos.	39%
26	RD	El control no cumple las normas y es necesario rediseñarlo para cumplir con estas	23%
25	PNP	El proceso no está implementado. (Control requerido, no documentado y no implementado)	22%
1	NA (Not Aplicable)	El control no es aplicable para la empresa	1%
114		TOTALES	100%

Fuente: El autor

Ilustración 32 Análisis estado de implementación



Fuente: El autor

De acuerdo a la gráfica anterior, el 39% de los controles están en funcionamiento, es decir, que en Casa Matriz sean acatado de acuerdo a lo dispuesto en el estándar ISO/IEC 27002:2013, no obstante, no se encuentran documentos y debidamente soportados, por tanto es indispensable iniciar con el proceso de documentación de estos, y así garantizar el cumplimiento de las disposiciones de la norma antes mencionada. El nivel de cumplimiento en este caso es medio y representa para la entidad un grado bajo de riesgo. Es una alerta para que se preparen los elementos necesarios y así evitar que en el futuro se convierta en un riego de nivel medio o alto.

Con un 23%, el grado de cumplimiento es bajo y con respecto al riesgo es un nivel alto, lo que indica que en Casa Matriz a pesar de haber implementado controles, estos no cumplen con las especificaciones de la norma, razón por la cual es preciso rediseñarlos teniendo en cuenta los resultados del análisis de riesgos y los requerimientos de protección del bien informático. Pues la entidad puede enfrentarse a graves consecuencias y posibles pérdidas de información, deterioro y vulnerabilidades de los bienes informáticos.

Por su parte el 22% de los controles requeridos no se encuentran implementados y claramente son necesarios para salvaguardar los activos y mitigar el impacto de los riesgos que pueden afectarlos, es una alerta máxima que está a la vista de la entidad y por tanto debe encaminar sus esfuerzos en la establecimiento de los controles y documentarlos siguiendo lo dispuesto en la norma.

Es importante resalta que aquí, una vez más, el nivel de cumplimiento es bajo y el grado del riesgo es sumamente alto; claramente es un riesgo que la entidad no debe estar dispuesta asumir pues los activos de información pueden resultar seriamente deteriorados lo que puede llevar a la compañía a incurrir en altos costos financieros.

En tanto a los objetivos de control y controles aplicados se cuenta con un 15% de controles en total funcionamiento y debidamente documentados, es un porcentaje muy bajo frente al grado de cumplimiento que se requiere por el sistema SANSI. Tan solo el 1% constituye el control que no aplica en la entidad pues no se requiere para el desarrollo de la operación y no hace parte de la actividad.

Conforme al análisis anterior se evidenció que existe una gran brecha entre lo requerido por el estándar y lo aplicado en Casa Matriz, esto quiere decir, que es necesario retomar los requisitos dispuestos en la norma, verificar y validar que se cuenta con las herramientas y personal preciso para iniciar la labor de documentar

los 45 controles que se aplican pero no cuentan con soporte documental, reevaluar los 26 controles que no cumplen con la normatividad, implementar y documentar los 25 controles obligatorios y que muy seguramente son vitales para evitar las vulnerabilidades en los sistemas de información.

9.3 ALCANCE DEL SGSI

El alcance del Sistema de Gestión de Seguridad de la Información, se limita temporalmente a la Casa Matriz de Positiva Compañía de Seguros S.A., pues es allí, donde se toman las decisiones y se gestiona todo lo concerniente a la administración de la entidad

Dicho sistema tiene aplicación en la sede de Casa Matriz, ubicada en la ciudad de Bogotá, involucrando todos los procesos y actividades desarrolladas allí.

9.3.1 OBJETIVOS DEL SGSI

Positiva Compañía de Seguros S.A. en cumplimiento de su misión, visión y objetivos estratégicos establece los siguientes objetivos para el SGSI:

1. Aumentar y mantener el nivel de satisfacción de los clientes internos y externos de Positiva Compañía de Seguros S.A.-Casa Matriz.

2. Mejorar los controles implementados por la entidad.

3. Incrementar el nivel competitivo de los funcionarios

4. Asegurar el acceso a la información conforme a los niveles y criterios de seguridad establecidos por Positiva y la normatividad aplicable.

5. Conservar la integridad de la información de la compañía, incluyendo las exigencias de seguridad aplicables y los resultados de la evaluación y el tratamiento de los riesgos identificados.

6. Garantizar que la información esté disponible para los usuarios y procesos en el momento en que sea requerida.

Política del Sistema de Gestión de Seguridad de la Información

De acuerdo al numeral 5.2 “Política” de la norma ISO/IEC 27001:2013, los directivos de la organización instituyen la política de seguridad de la información según el propósito de Positiva, la siguiente es la política general del Sistema de Gestión de Seguridad de la Información definida por la alta dirección de la entidad:

9.4 POLITICA DEL SGSI PARA POSITIVA COMPAÑÍA DE SEGUROS S.A.- CASA MATRIZ

La Dirección de Positiva Compañía de Seguros S.A. reconoce la importancia de identificar y salvaguardar los activos de información de la entidad, con el fin de impedir la pérdida, divulgación, alteración y utilización no autorizada de la información relacionada con los asegurados, colaboradores, pólizas, estrategias, y otros datos concernientes a la operación de la compañía.

En consecuencia, se compromete a instaurar, conservar y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI) asegurando así, la confidencialidad, disponibilidad e integridad de la información de todos los grupos de interés reconocidos por la compañía.

Para esto, Positiva Compañía de Seguros S.A.:

- *Periódicamente instaurará objetivos relacionados con la Seguridad de la Información.*
- *Promoverá la tipificación y acatamiento de las necesidades del negocio, obligaciones contractuales, reglamentarias y legales en materia de seguridad.*
- *Establecerá un procedimiento de Identificación y Evaluación de Riesgos a fin de desarrollar las acciones pertinentes para tratar los riesgos que se consideren inadmisibles.*
- *Mantendrá buenas prácticas de seguridad de la información que garanticen la disponibilidad, integridad y confidencialidad de la información, generando así un nivel de confianza mayor dentro de los grupos de interés.*
- *Reforzará la cultura de seguridad de la información en los funcionarios de la Entidad.*
- *Garantizara la continuidad del negocio.*

9.4.1 APLICACIÓN DE LA POLITICA DE SGSI

La política aplica a la Casa Matriz de Positiva Compañía de Seguros S.A, los colaboradores, proveedores, terceros y demás partes interesadas.

9.5 ALCANCE POLITICA SEGURIDAD DE LA INFORMACIÓN

En el marco de la protección, preservación y administración de la integridad, confidencialidad y disponibilidad de la información física y digital resultante de la de los procesos gestionados por Positiva Compañía de Seguros S.A.- Casa Matriz se establece la siguiente política general:

9.5.1 OBJETIVO POLITICA SEGURIDAD DE LA INFORMACIÓN

Establecer la política de seguridad de la información para Positiva Compañía de Seguros S.A.-Casa Matriz, a fin de regular la gestión en materia de seguridad de la información al interior de esta.

9.5.2 POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Para Positiva Compañía de Seguros S.A-Casa Matriz la información es un activo primordial para la prestación de los servicios y la toma de decisiones, motivo por el cual, se compromete con la protección de los bienes informáticos de mayor relevancia y así encaminar sus esfuerzos hacia la continuidad del negocio, la gestión de riesgos y el fortalecimiento de la cultura en seguridad informática.

Positiva Compañía de Seguros S.A.-Casa Matriz, analizo sus necesidades y con base a esto, decidió que es necesaria la implementación de una guía de gestión de seguridad de la información como instrumento para identificar y disminuir los riesgos que puedan afectar la información, además, de propender por la disminución de costos operativos y financieros, constituir una cultura de seguridad y asegurar el cumplimiento de las obligaciones legales, contractuales y de negocio. Los colaboradores, terceros y proveedores que tengan responsabilidad sobre los sistemas de procesamiento de datos de Positiva, están obligados a

acoger los lineamientos contenidos y relacionados en la Política de seguridad de la información definida.

Otras disposiciones en materia de seguridad de la información

1. Se creará el Comité de Seguridad de la Información, el cual será el responsable del mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información de Positiva Compañía de Seguros S.A.-Casa Matriz
2. Los bienes informáticos serán identificados y clasificados a fin de instaurar los dispositivos de protección apropiados.
3. Los compromisos frente a la seguridad de la información serán determinados, compartidos, socializados y admitidos por todos los que son considerados usuarios de los sistemas de tratamiento de información en la entidad.
5. Exclusivamente se permitirá el uso de software licenciado y adquirido legalmente por la compañía.
7. Los funcionarios, proveedores y terceros tienen la obligación de reportar cualquier incidente de seguridad, evento sospechoso o mal uso de los recursos informáticos que estos identifiquen.
8. Periódicamente se diseñaran auditorías y se establecerán controles sobre el SGSI de Positiva compañía de Seguros S.A.
9. El personal de la entidad será capacitado regularmente en materia de seguridad de la información a fin de proteger la información de amenazas originadas por estos.
10. Positiva Compañía de Seguros S.A. asegurará el cumplimiento de las obligaciones legales, regulatorias y contractuales determinadas.

9.5.3 COMPROMISO DE LA DIRECCIÓN

La Junta Directiva de Positiva Compañía de Seguros S.A, una vez analizados los documentos pertinentes, ratifica la Política de Seguridad de la Información como parte del compromiso adquirido y como soporte en el diseño e implementación de lineamientos encaminados a garantizar la seguridad de la información de la aseguradora. La Junta Directiva y la Alta Dirección de la compañía manifiestan su compromiso mediante:

- La consideración y consentimiento de las Políticas de Seguridad de la Información.

- El fomento de una cultura de seguridad.
- Proporcionar los medios necesarios para la socialización de la política de seguridad y del SGSI a toda la organización.
- Disponer de los recursos necesarios para efectuar y conservar las políticas de seguridad de la información.
- Validar el acatamiento de las políticas definidas.

9.5.4 SANCIONES A LAS INFRACCIONES DE LAS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

El incumplimiento de las políticas de seguridad previamente establecidas, serán sancionadas de acuerdo a la gravedad de las mismas. Las medidas sancionatorias definidas son:

- Medidas administrativas:

Memorando con copia a la hoja de vida
Traslado forzoso
Pérdida de derechos como: bonificación por desempeño, cancelación de créditos educativos y prima extralegal.

- Medidas legales:

Denuncia por la vía legal
Inhabilitación para contratar con el estado
Penas de cárcel

- Medidas Disciplinarias

Suspensión por una semana sin remuneración
Despido inmediato
Multas económicas

9.5.5 POLITICA PARA EL USO DE DISPOSITIVOS MÓVILES

- La administración de los recursos móviles pertenecientes a la entidad estará a cargo de la Vicepresidencia de TIC´S.
- Se prohíbe el uso de dispositivos móviles pertenecientes al personal dentro de las estaciones de trabajo.
- La Vicepresidencia de TIC´S elaborará y mantendrá un procedimiento de instalación y configuración de las aplicaciones de los dispositivos móviles y a su vez, se encargara de divulgarlo a todo el personal de Casa Matriz.
- Se prohíbe el acceso a los funcionarios a la red WIFI de la entidad
- La Vicepresidencia de TIC´S debe establecer un sistema de cifrado de la memoria de almacenamiento de los dispositivos móviles institucionales a fin de impedir la copia o extracción de los datos contenidos en esta.
- Los usuarios de los dispositivos móviles no podrán generar cambios a la configuración de estos sin previa autorización.

9.5.6 POLITICA PARA EL USO DE CONEXIONES REMOTAS

Positiva Compañía de Seguros S.A establecerá los contextos y requerimientos para las conexiones remotas a la plataforma tecnológica de la compañía; así mismo, proveerá los materiales y controles necesarios para que estas conexiones se ejecuten de forma segura.

La Vicepresidencia de Riesgos junto con la Vicepresidencia de TIC´S, deberán analizar y avalar las conexiones remotas a la plataforma tecnológica.

- La Gerencia de Infraestructura TIC´S debe establecer las metodologías y controles de seguridad para las conexiones remotas a la plataforma tecnológica.
- La Gerencia de Infraestructura TIC´S debe limitar las conexiones remotas a los recursos tecnológicos de la plataforma y permitir únicamente el acceso al personal autorizado.
- La Gerencia de Infraestructura TIC´S debe validar de manera permanente la efectividad de los controles aplicados sobre las conexiones remotas.
- La Oficina de Control Interno dentro de su injerencia, deber efectuar auditorías sobre los controles instaurados para las conexiones remotas.

- Los usuarios autorizados para realizar conexiones remotas deben obedecer los requisitos de uso para dichas conexiones.

9.5.7 POLITICA DE SEGURIDAD PARA EL PERSONAL

Debido a la importancia que tiene contar con personal altamente calificado, Positiva garantiza que la vinculación de personal se realiza siguiendo un proceso de selección formal y bajo los lineamientos legales vigentes orientados a las funciones y cargos que deben desempeñar los nuevos funcionarios.

- La Gerencia de Talento Humano verificará y validará la información suministrada por el candidato a ocupar un cargo en Positiva, antes de su vinculación definitiva.
- La Gerencia de Talento Humano es la encargada de hacer que los funcionarios firmen el Acuerdo de Confidencialidad y de Admisión de Políticas de Seguridad de la Información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.
- Lo anterior aplica para los contratistas, consultores y demás terceros con vinculación directa.

9.5.8 POLITICA DE DESVINCULACIÓN, VACIONACIONES, LICENCIAS O CAMBIO DE LABORES DE LOS FUNCIONARIOS DE PLANTA Y TERCEROS

- La Gerencia de Talento Humano es la encargada de realizar los procesos de desvinculación, licencias, vacaciones o cambio de labores de los colaboradores aplicando los procedimientos y controles para tal fin.

- Los Supervisores de Contrato, deben monitorear y reportar oportunamente la desvinculación o cambio de labores del personal provisto por terceros a la Vicepresidencia de Riesgos.

- La Gerencia de Riesgos debe confirmar las novedades de desvinculación o cambio de labores y consecutivamente solicitar la modificación o inhabilitación de usuarios a la Gerencia de Soporte TIC´S.

9.5.9 POLITICA DE GESTIÓN DE ACTIVOS DE LA INFORMACIÓN

Positiva como dueña de la información física y digital tratada mediante la plataforma tecnológica, concederá responsabilidad a las áreas sobre los activos de información, garantizando el cumplimiento de las políticas que regulan el uso apropiado de la misma.

La información sensible de Positiva, así como los medios de almacenamiento y procesamiento de esta, se les asignara un responsable, serán inventariados y consecutivamente clasificados, según las exigencias y los criterios que determine la Gerencia de Riesgos.

- Las Vicepresidencias, Gerencias y Oficinas Asesoras de Positiva, son las dueñas de la información física y electrónica, por tanto deben ejercer control sobre esta, aprobando o no el acceso.
- Los activos de información deben estar inventariados por las áreas o procesos dueños de estos.
- Los activos de información deben contar con un monitoreo permanente a fin de validar los perfiles de acceso a la información.
- Todos los recursos de procesamiento de información están sujetos a revisiones de cumplimiento por parte de la Gerencia de Riesgos y a auditorías por parte de la Oficina de Control Interno.
- La Gerencia de Infraestructura TIC´S es la propietaria de los activos de información concernientes a la plataforma tecnológica de Positiva por tanto debe garantizar una adecuada manipulación y gestión.
- La Gerencia de Infraestructura TIC´S junto con el Comité de Control de Cambios, son los únicos que están facultados para autorizar la instalación, cambio o eliminación de elementos de la plataforma tecnológica de Positiva.
- Es responsabilidad de la Gerencia de Soporte TIC´S preparar las estaciones de trabajo fijas o portátiles de los colaboradores y de hacer entrega de las mismas.
- La Gerencia de Soporte TIC´S es la encargada de recoger los equipos fijos o portátiles para la reasignación o disposición final, y generar copias de seguridad de la información.

- La Gerencia de Riesgos periódicamente debe efectuar sobre todos los procesos un análisis de riesgos de seguridad y definir las condiciones de uso y protección de los activos de información.
- Los recursos tecnológicos, deben ser manejados de acuerdo a los lineamientos éticos estipulados en el Código de ética y buen gobierno y no deben ser utilizados para fines personales o diferentes para los cuales fueron asignados.

9.5.10 POLITICA DE CLASIFICACIÓN Y UTILIZACIÓN DE LA INFORMACIÓN

La información que resulte de los procesos gestionados por Positiva, debe ser reconocida, catalogada y argumentada de acuerdo a los lineamientos establecidos por el Comité de Seguridad de la Información. Una vez identificada Positiva dispondrá de las herramientas necesarias para controlarla y preservar la confidencialidad, disponibilidad, integridad y trazabilidad de la misma.

- Es responsabilidad del Comité de Seguridad de la Información determinar los parámetros de clasificación de la información para que sean avalados por la Junta Directiva.
- La Gerencia de Riesgos es la encargada de construir la guía de clasificación de la información, socializarla a todos los funcionarios de Casa Matriz y velar por su cumplimiento.
- La Gerencia de Infraestructura TIC´S debe suministrar las técnicas de cifrado de la información, así como gestionar el software manejado para tal fin.
- Es labor de la Gerencia de Infraestructura TIC´S la depuración de la información contenida en la plataforma tecnológica.
- Los dueños de los activos de información tienen el compromiso de clasificarla basados en la guía de clasificación de la Información definida, igualmente son responsables de realizar un seguimiento periódico y de hacer las reclasificaciones pertinentes.
- Es obligación de todos los usuarios cumplir con los lineamientos estipulados en la guía de clasificación de la Información.
- Toda información física y digital ha de ser preservada, mediante controles de acceso físico, condiciones de almacenamiento y depurada apropiadamente una vez finalice el tiempo de almacenamiento.

9.5.11 POLITICA DE USO DE MEDIOS DE ALMACENAMIENTO Y PERIFERICOS

El uso de periféricos y medios de almacenamiento estarán sujetos a las disposiciones determinadas por la Gerencia de Riesgos y Gerencia de Infraestructura TIC´S, según la necesidad de uso para el cumplimiento de las funciones asignadas.

- La Gerencia de Riesgos y Gerencia de Infraestructura TIC´S estarán a cargo de establecer los requisitos de uso de periféricos y medios de almacenamiento.
- Los controles que reglamenten el uso de periféricos y medios de almacenamiento serán determinados por la Gerencia de Infraestructura TIC´S.
- La Gerencia de Infraestructura TIC´S debe crear y utilizar lineamientos para la disposición segura de los medios de almacenamiento cuando estos sean dados de baja o reasignados.
- El Personal de planta como contratistas, proveedores o terceros no están autorizados para modificar la configuración de periféricos y medios de almacenamiento establecidos por la Gerencia de Infraestructura TIC´S.
- Se prohíbe el uso de medios de almacenamiento particulares en la plataforma tecnológica de Positiva.

9.5.12 POLITICAS DE CONTROL DE ACCESO

9.5.12.1 POLITICA DE CONTROL DE ACCESO A LA RED Y RECURSOS DE RED

La Gerencia de Infraestructura TIC´S, tiene como obligación la protección de la red y recursos de red contra accesos no autorizados mediante controles de acceso lógico.

- La labor principal de esta unidad de negocio, es determinar un procedimiento de autorización y controles para restringir el acceso a las redes de datos y los recursos de red de Positiva. A su vez, debe garantizar

que las redes inalámbricas tengan métodos de autenticación para evitar accesos no autorizados.

- Todos los usuarios deben contar con la debida autorización para la creación de cuentas de usuario y el acuerdo de confidencialidad firmado preliminarmente.

9.5.12.2 POLITICA DE ADMINISTRACIÓN DE ACCESO DE USUARIOS

- Positiva Compañía de Seguros S.A. facilita a los colaboradores y contratistas los recursos tecnológicos necesarios para ejercer las funciones asignadas, por tal razón no se permite conectar o instalar dispositivos fijos o móviles, que no sean autorizados por la Gerencia de Infraestructura.
- La Gerencia de Infraestructura proporcionara a los usuarios las claves de acceso a los servicios de red y sistemas de información previamente autorizados. Es de aclarar que las claves son de uso personal e intransferible.
- Únicamente el personal de COMSISTELCO es el designado por la Gerencia de Infraestructura para instalar software o hardware en los equipos y servidores en Positiva.
- La conexión remota a la red de Positiva debe darse a través de un enlace VPN debidamente avalado, registrado y auditado.

9.5.12.3 POLITICA DE ESTABLECIMIENTO, USO Y RESGUARDO DE CLAVES DE ACCESO

- Vigilar que los usuarios hagan uso de buenas prácticas de seguridad en la elección, uso y defensa de las contraseñas, pues este es el medio de autenticación a través del cual puede acceder a los servicios informáticos.
- Es compromiso de todo el personal el buen uso de las claves o contraseñas de acceso para el manejo de los equipos o servicios informáticos de la Entidad.
- El cambio o la reseteo de la contraseña solo puede ser requerido por el titular de la cuenta.
- Finalizar las sesiones activas cuando finalice, o asegurarlas con el mecanismo de bloqueo cuando no estén en uso.

- El acceso a todo usuario que intente el ingreso, sin éxito, durante tres veces será bloqueado.
- Solo la Gerencia de Soporte TI está facultada para bloquear o desbloquear las claves de acceso previa solicitud formal.

9.5.12.4 POLITICA DE CONTROL DE ACCESO A SISTEMAS Y APLICATIVOS

- Todas las áreas que gestionan información en Positiva son propietarias de los sistemas de información y aplicativos que soportan los procesos, por tanto deben custodiar de forma controlada la asignación, modificación e invalidación de privilegios de accesos.

- La Gerencia de infraestructura, es responsable de la gestión de dichos sistemas de información y aplicativos, por tanto debe propender por la debida protección contra accesos no autorizados mediante elementos de control de acceso lógico. Igualmente, vigilará que los desarrolladores, internos como externos, adopten las buenas prácticas de desarrollo y así evitar accesos no autorizados a los sistemas.

9.5.13 POLITICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

- La Gerencia de Soporte TI es la encargada de asegurar que los sistemas de información, contemplan controles y cumplen con las directrices de seguridad de la información.
- En cuanto a los desarrollos propios, es necesario comprobar que están debidamente documentados, que las versiones se resguardan apropiadamente en diferentes medios y se realizan copias de respaldo alternas.
- Desplegar tácticas para indagar sobre la seguridad en los sistemas de información.
- Las nuevas adquisiciones de hardware y software que se vayan a conectar a la plataforma tecnológica de Positiva, deberán ser administrados por la Gerencia de Infraestructura.

- La Gerencia de Infraestructura o de Soporte TI serán las únicas autorizadas para realizar copias de seguridad de un software original.
- La instalación del software en los equipos de Positiva, se realizará únicamente mediante la Gerencia de Soporte.
- En las máquinas de Positiva solo se podrá utilizar software licenciado.
- Si se requiere la compra o actualización de software, debe hacerse mediante la Gerencia de Soporte una vez esto sea justificado.

9.5.14 POLITICA DE CRIPTOGRAFIA

Positiva vigilara que la información clasificada como confidencial sea cifrada en el momento en que sea almacenada o trasmitida.

- Es función de la Gerencia de Infraestructura validar que todos los sistemas y aplicativos informáticos que soliciten trasmitir información confidencial cuente con elementos de cifrado de datos.
- La Gerencia de Infraestructura debe crear y definir un procedimiento para el uso y la gestión de llaves de cifrado.
- Es labor de la Gerencia de Infraestructura instituir modelos para la aplicación de controles criptográficos.

9.5.15 POLITICA SEGURIDAD FISICA Y AMBIENTAL

AREAS SEGURAS

- Positiva a través de su Vicepresidencia Administrativa y Financiera garantizara la seguridad física en Casa Matriz, a fin de prevenir e imposibilitar accesos no autorizados, perjuicios e interrupción en los servicios.
- Los recursos físicos como las instalaciones, equipos, cableado, expedientes, medios de almacenamiento, entre otros, estarán protegidos mediante mecanismos autenticación de identidad, sistema biométrico y tarjetas de proximidad.
- En tanto a los recursos TIC manejados en el tratamiento de la información se ubicaran en lugares de acceso restringido y protegidos por mecanismos de seguridad que controlan el acceso.

- Mediante las diferentes Gerencias se debe reconocer y garantizar el control sobre aspectos ambientales que puedan entorpecer el adecuado funcionamiento de los recursos tecnológicos en el tratamiento y almacenamiento de la información.
- Todas las áreas de Casa Matriz deben establecer los niveles de seguridad física y avalar o negar la autorización de acceso.

9.5.16 POLITICA CONTRA SOFTWARE MALICIOSO

- Es obligación de la Gerencia de Soporte suministrar elementos tales como antivirus, antimalware, antispam, antispyware que minimicen el riesgo de infección por software malicioso y protejan la seguridad de la información contenida y gestionada en la plataforma tecnológica.
- La Gerencia de Soporte debe garantizar que la información almacenada en la plataforma tecnológica es analizada por el antivirus, involucrando la remitida por correo electrónico.
- Los antivirus, antispyware, antispam, antimalware, deben contar con las últimas actualizaciones y parches de seguridad, para aminorar las vulnerabilidades de la plataforma tecnológica.
- Está prohibido a los usuarios realizar cualquier modificación a la configuración de los antivirus.

9.5.17 POLITICA MANEJO CORPORATIVO (OUTLOOK)

- EL usuario solicitará a la Gerencia de Infraestructura de TIC´S la creación de una cuenta de correo, mediante el formato establecido para tal fin.
- La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión y posteriormente debe cambiarse.
- La composición de las contraseñas deber contener mínimo 6 caracteres alfanuméricos con uso de mayúsculas y minúsculas obligatorias.
- La contraseña se debe cambiar cada 30 días, y no debe ser igual a las últimas tres contraseñas utilizadas.
- Con el fin de garantizar la seguridad del sistema de correo, una vez el usuario ingrese a la red, debe mantener bloqueado su equipo cada vez que se retire de éste.
- La información del Outlook debe conservarse mediante el procedimiento de copias de seguridad previamente establecidos.

- Se prohíbe él envió de cadenas, chistes, videos, fotos y demás material que produzca traumatismos en la red, al crear congestión en la misma.

9.5.18 POLITICA DE USO DE FILESERVER

Es deber de los colaboradores acoger la políticas definidas con integridad y dar a los recursos uso racional y eficiente.

- Los usuarios manejarán los recursos puestos a su disposición para el intercambio de información únicamente relacionada con la operación de la entidad. Asimismo deberán realizar un uso eficiente de la red de datos, para evitar la congestión de la misma.
- La Gerencia de Infraestructura de TI proporciona el servicio (FileServer), el cual es para el almacenamiento de información que requiere ser consultada, modificada y borrada, según los privilegios otorgados por las áreas.
- El uso autorizado protegerá el acceso a los documentos almacenados en este servidor por lo que se prohíbe a los usuarios de positiva el acceso o intento de acceso a Gerencias o áreas no autorizadas dentro del servicio.
- La Gerencia de Infraestructura de TI no tendrá injerencia en la manipulación de los archivos que se encuentran las carpetas designadas.
- El uso de carpetas compartidas es responsabilidad del usuario y debe realizar bajo la autorización de la Gerencia de Infraestructura TI
- Es prohibido el uso de recursos compartidos para archivos de audio y video que queden fuera de los lineamientos corporativos.
- La información contenida en el FileServer, es propiedad de Positiva por lo tanto, está sujeta a verificación, validación y auditoria.
- Será asignado un espacio de almacenamiento o “Cuotas” para cada vicepresidencia que requiera almacenar información crítica. Es responsabilidad de cada área de Casa Matriz clasificar la información de acuerdo a su pertinencia y criticidad para ser almacenada en el FileServer.
- Es obligación de cada área gestionar de forma oportuna y eficiente el espacio de almacenamiento otorgado. .
- La Gerencia de Infraestructura de TI es la encargada de realizar, recuperar y conservar las copias de seguridad requeridas por cada área de Casa Matriz.

9.5.19 POLITICA DE USO DE INTERNET

A continuación se describen las políticas a cumplir por todos los colaboradores de Positiva.

- Para la creación de cuentas de usuario que requieran de acceso a la red, internet y correo electrónico debe ser autorizada por el Gerente de la respectiva dependencia, Regional o en su defecto por el Vicepresidente correspondiente.
- Está estrictamente prohibido el uso inadecuado del servicio de internet en casos como los siguientes: Acceso a internet para actividades ilegales o ilícitas (amenazas, estafas, pornografía, entre otros), para uso privado (recreación o actividades no relacionadas con la compañía) y para vulnerar otras redes o realizar ataques informáticos.
- Evadir las medidas de seguridad en los recursos de la red de la compañía u otros sistemas de conexión que accedan a internet, es una conducta indebida y será sancionada de acuerdo con los aspectos disciplinarios y legales de Positiva.
- Todos los usuarios se comprometen a respetar la política anti-spam de Positiva Compañía de Seguros.
- Es ilegal divulgar datos de carácter personal.
- Queda totalmente prohibido interferir el uso de recursos, mediante actividades que interrumpan en el uso efectivo de los recursos de la red.

9.5.20 POLITICA DE ESCRITORIO Y PANTALLA LIMPIA

- Los funcionarios de Positiva están obligados a mantener el escritorio de su equipo de cómputo, libre de información competente a la entidad a fin de evitar que esta pueda ser utilizada de forma inapropiada o copiada por terceros o personas no autorizadas.
- Todos los colaboradores de Positiva deben bloquear la pantalla del equipo con un protector de pantalla corporativo, en el momento en que tengan que retirarse del puesto de trabajo.
- Los documentos impresos categorizados como confidenciales no deben dejarse sin protección.

10. CONCLUSIONES

- El diseño de un Sistema de Gestión de Seguridad de la Información basado en el estándar ISO/IEC 27001:2013, permite identificar los aspectos relevantes a tener en cuenta a la hora de establecer un modelo de seguridad de la información sólido y sostenible.

- La puesta en marcha de un Sistema de Gestión de Seguridad de la Información, inicia con un claro compromiso por parte de los directivos de la entidad, pues desde allí se fortalece la cultura de seguridad de la información tan fundamental de cara a la protección de los datos organizacionales.

- La declaración de aplicabilidad de la norma ISO/IEC 27001 evidencio el grado de madurez de Positiva frente a la administración de seguridad de la información, el cual se ubicó en el nivel medio y el grado de cumplimiento de los requisitos del estándar corresponde al 69% de lo requerido; esto es una alerta para que la entidad adopte medidas oportunas y fortalezca la cultura de seguridad de la información, pues de esta depende el éxito del SGSI por implementar y el consecución de los resultados estimados.

- El proceso de identificación de activos informáticos evidencio activos críticos que la organización desconocía y a su vez permitió estudiar las medidas apropiadas para protegerlos oportunamente.

- La aplicación de la metodología de análisis de riesgos Magerit, permitió a la aseguradora reconocer oportunamente la probabilidad y el impacto una vez se ha materializado una amenaza sobre los activos informáticos; a su vez establecer los controles apropiados para mitigar o contrarrestar el daño según corresponda.

- El hecho de que Positiva no contara con una política de seguridad de la información correspondía a no tener un lineamiento que guiara apropiadamente la gestión de los activos de información y los datos tratados por la misma, representaba un riesgo inminente que podía comprometer seriamente la confiabilidad de los asegurados, proveedores y colaboradores al no contar con un respaldo que garantizara la protección de la información.

- La ausencia de controles en materia de intercambio de información con terceros, representa un alto riesgos para la organización pues puede afectar considerablemente la relación con sus grupos de interés y la pérdida de confianza de los mismos, igualmente puede tener un impacto significativo en la reputación de la aseguradora que le costaría su participación en el mercado asegurador.

- La implementación de controles, el rediseño de algunos y la documentación de otros le permitirá a la entidad mejorar su nivel de madurez frente a la administración de seguridad de la información, el cumplimiento de los requisitos establecidos en el estándar ISO/IEC 27002 y al acatamiento de la Estrategia de Gobierno en Línea definida por el gobierno Nacional.

11. RESULTADOS Y DISCUSIONES

Los resultados logrados mediante el desarrollo del presente proyecto de grado, obedecen básicamente a la concientización de las directivas y a la entidad en general acerca de la importancia que tiene el diseño y la implementación de un Sistema de Gestión de Seguridad de la Información a fin de proteger el bien más preciado, la información.

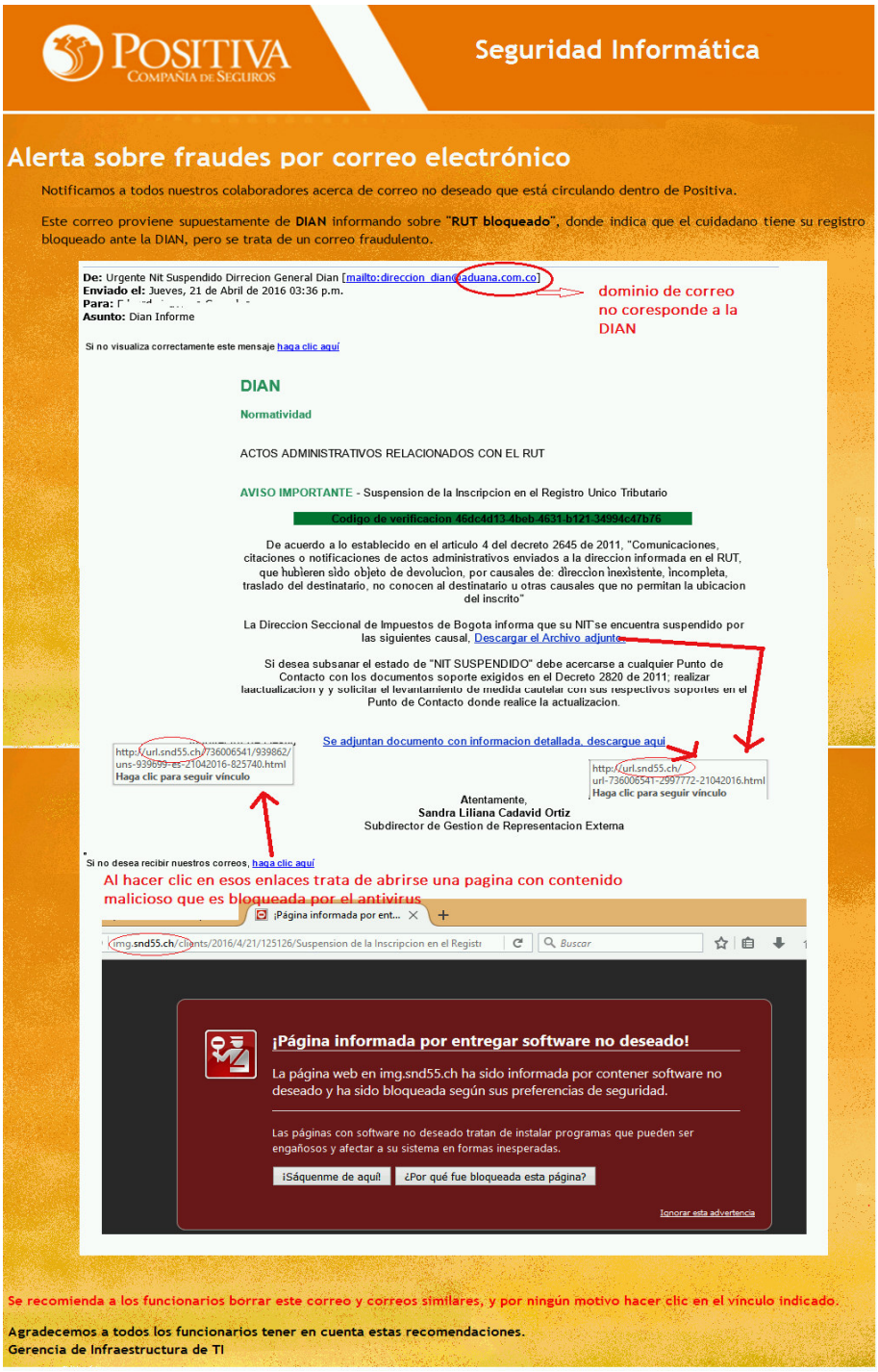
La ejecución de la presente investigación se dio con el diagnostico en materia de seguridad de la información al interior de Casa Matriz, en dicho diagnostico se evidencio la falta de una política de seguridad de la información, lineamientos y la aplicación de algunos controles para mitigar o evitar la ocurrencia de alguna amenaza que pudiera afectar los activos de información. Mediante la declaración inicial de aplicabilidad del estándar ISO/IEC 27001:2013 se estableció el grado de cumplimiento por parte de la entidad con respecto a los requerimientos de dicha norma, el cual fue establecido en el nivel medio; además, fue posible, reconocer que muchos de los controles establecidos y en funcionamiento no cumplían con la documentación necesaria, en tanto otros, debían ser reevaluados pues la efectividad de estos, se veía opacada dado que no concernía a su objetivo fundamental, es decir, los controles implantados no eran los apropiados según el tipo de activo y su grado de sensibilidad.

Por otro lado no existía certeza sobre los bienes informáticos con los que contaba Casa Matriz, por tanto fue necesaria una revisión física para identificarlos y caracterizarlos.

La primera evidencia de la sensibilización por parte de la entidad, corresponde al envió de alertas de seguridad informática emitidas por la Gerencia de Infraestructura TIC´S a toda la comunidad de Casa Matriz mediante el correo corporativo.

Las alertas remitidas, conciernen a fraudes mediante correo electrónico y código malicioso circulando en la red, a través de las siguientes imágenes es posible constatar dicha información

Ilustración 33 Alerta sobre fraude No. 1

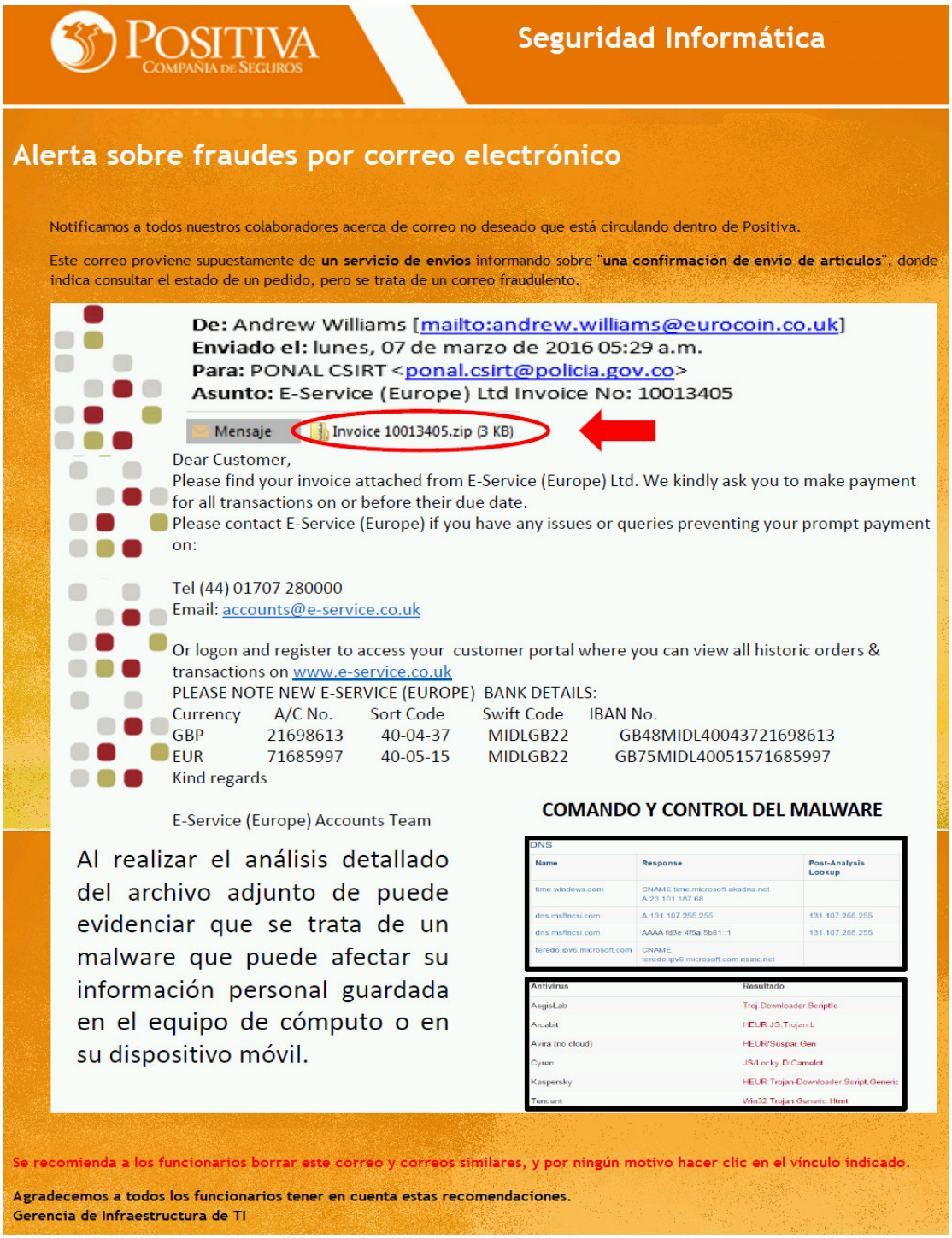


Fuente: El autor

Ilustración 34 Alerta sobre fraude No. 2

Fuente: El autor

Ilustración 35 Alerta sobre fraude No. 3



Fuente: El autor

Ilustración 36 Alerta sobre fraude No. 4

Fuente: El autor

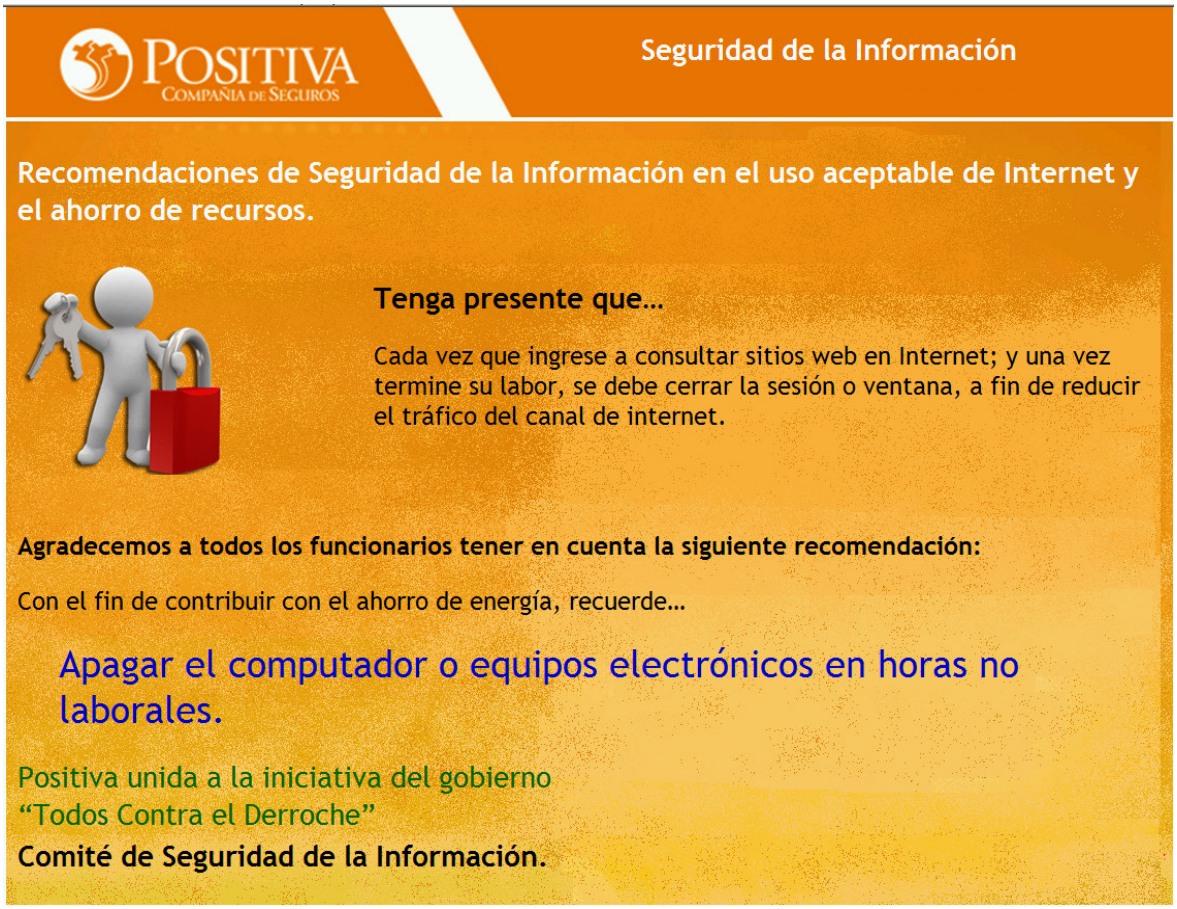
Otra de las actividades de seguridad informática incumbe a la divulgación de alertas sobre códigos maliciosos circulando en la red, aunque no es muy frecuente, si se informa a todos los usuarios sobre esta novedad, como se aprecia en la imagen adjunta:

Ilustración 37 Alerta Código malicioso circulando en la red

Fuente: El autor

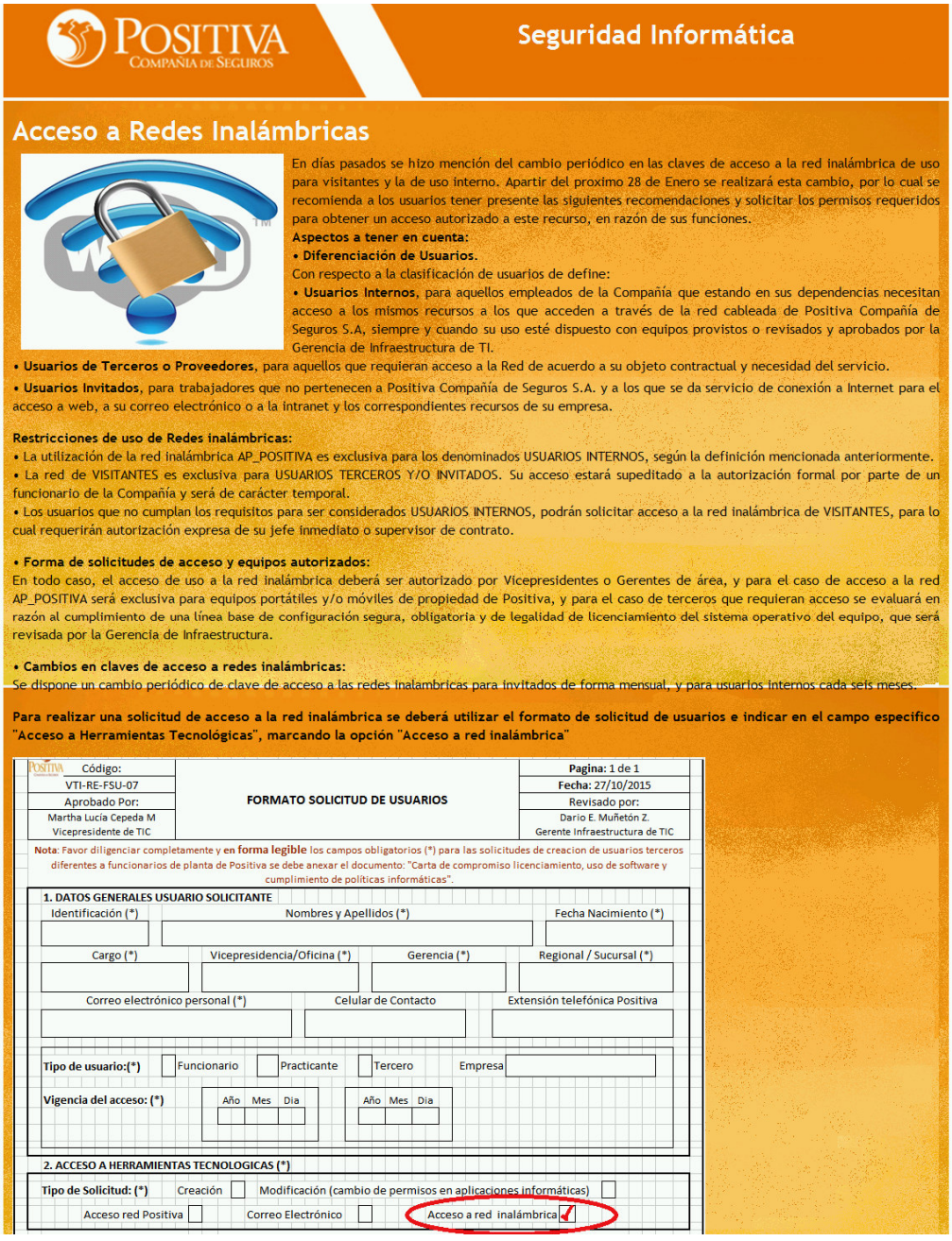
A través de este medio, no solo se informa de novedades en materia de seguridad informática, también sobre seguridad de la información, se hace recomendaciones sobre el uso racional de internet y la red inalámbrica, como se observa en las imágenes:

Ilustración 38 Recomendaciones sobre el uso de internet



Fuente: El autor

Ilustración 39 Acceso a redes inalámbricas



POSITIVA COMPAÑÍA DE SEGUROS

Seguridad Informática

Acceso a Redes Inalámbricas

En días pasados se hizo mención del cambio periódico en las claves de acceso a la red inalámbrica de uso para visitantes y la de uso interno. Apartir del proximo 28 de Enero se realizará esta cambio, por lo cual se recomienda a los usuarios tener presente las siguientes recomendaciones y solicitar los permisos requeridos para obtener un acceso autorizado a este recurso, en razón de sus funciones.

Aspectos a tener en cuenta:

• **Diferenciación de Usuarios.**

Con respecto a la clasificación de usuarios de define:

• **Usuarios Internos**, para aquellos empleados de la Compañía que estando en sus dependencias necesitan acceso a los mismos recursos a los que acceden a través de la red cableada de Positiva Compañía de Seguros S.A, siempre y cuando su uso esté dispuesto con equipos provistos o revisados y aprobados por la Gerencia de Infraestructura de TI.

• **Usuarios de Terceros o Proveedores**, para aquellos que requieran acceso a la Red de acuerdo a su objeto contractual y necesidad del servicio.

• **Usuarios Invitados**, para trabajadores que no pertenecen a Positiva Compañía de Seguros S.A. y a los que se da servicio de conexión a Internet para el acceso a web, a su correo electrónico o a la intranet y los correspondientes recursos de su empresa.

Restricciones de uso de Redes inalámbricas:

• La utilización de la red inalámbrica AP_POSITIVA es exclusiva para los denominados USUARIOS INTERNOS, según la definición mencionada anteriormente.

• La red de VISITANTES es exclusiva para USUARIOS TERCEROS Y/O INVITADOS. Su acceso estará supeditado a la autorización formal por parte de un funcionario de la Compañía y será de carácter temporal.

• Los usuarios que no cumplan los requisitos para ser considerados USUARIOS INTERNOS, podrán solicitar acceso a la red inalámbrica de VISITANTES, para lo cual requerirán autorización expresa de su jefe inmediato o supervisor de contrato.

• **Forma de solicitudes de acceso y equipos autorizados:**

En todo caso, el acceso de uso a la red inalámbrica deberá ser autorizado por Vicepresidentes o Gerentes de área, y para el caso de acceso a la red AP_POSITIVA será exclusiva para equipos portátiles y/o móviles de propiedad de Positiva, y para el caso de terceros que requieran acceso se evaluará en razón al cumplimiento de una línea base de configuración segura, obligatoria y de legalidad de licenciamiento del sistema operativo del equipo, que será revisada por la Gerencia de Infraestructura.

• **Cambios en claves de acceso a redes inalámbricas:**

Se dispone un cambio periódico de clave de acceso a las redes inalambricas para invitados de forma mensual, y para usuarios internos cada seis meses.

Para realizar una solicitud de acceso a la red inalámbrica se deberá utilizar el formato de solicitud de usuarios e indicar en el campo especifico "Acceso a Herramientas Tecnológicas", marcando la opción "Acceso a red inalámbrica"

Código: VTI-RE-FSU-07	FORMATO SOLICITUD DE USUARIOS	Pagina: 1 de 1
Aprobado Por: Martha Lucia Cepeda M Vicepresidente de TIC		Fecha: 27/10/2015 Revisado por: Dario E. Muñetón Z. Gerente Infraestructura de TIC

Nota: Favor diligenciar completamente y **en forma legible** los campos obligatorios (*) para las solicitudes de creacion de usuarios terceros diferentes a funcionarios de planta de Positiva se debe anexar el documento: "Carta de compromiso licenciamiento, uso de software y cumplimiento de políticas informáticas".

1. DATOS GENERALES USUARIO SOLICITANTE

Identificación (*)	Nombres y Apellidos (*)	Fecha Nacimiento (*)

Cargo (*)	Vicepresidencia/Oficina (*)	Gerencia (*)	Regional / Sucursal (*)

Correo electrónico personal (*)	Celular de Contacto	Extensión telefónica Positiva

Tipo de usuario:(*) ☐ Funcionario ☐ Practicante ☐ Tercero Empresa

Vigencia del acceso: (*) Año Mes Dia | Año Mes Dia

2. ACCESO A HERRAMIENTAS TECNOLOGICAS (*)

Tipo de Solicitud: (*) Creación ☐ Modificación (cambio de permisos en aplicaciones informáticas) ☐

Acceso red Positiva ☐ Correo Electrónico ☐ Acceso a red inalámbrica ☑

Fuente: El autor

Ilustración 40 Recomendación uso de correo electrónico

POSITIVA COMPAÑIA DE SEGUROS

Seguridad Informática

Recomendaciones de Seguridad Informática en la utilización del correo electrónico y la navegación a internet

Informamos que desde hace un par de semanas se han reportado amenazas en donde una nueva variante de **ransomware** está comprometiendo la información de personas en internet, a lo que el fabricantes de Antimalware, han prestado completa atención y están trabajando para neutralizar la amenaza y sus múltiples variantes.

A continuación, acercamos algunos síntomas que evidencian que el equipo puede estar siendo atacado:

* La amenaza tipo **ransomware** secuestra la información de los usuarios usando técnicas de cifrado y luego solicita un rescate (dinero). Una vez se realiza el pago, se podrán recuperar los archivos, aunque se aclara, que el pago no garantiza siempre la recuperación total de la información.

*Los archivos cifrados se reconocen porque al final presenta la extensión **.LOCKY**, por ejemplo: **264685148D063E24A1EDAADE509544BB.LOCKY**

* La amenaza se propaga a través de correo electrónico y solicita al usuario descargar un archivo de Excel o Word, el cual al ser ejecutado, indica que se deben habilitar las macros y una vez habilitadas, se comienza el proceso de cifrado. Dichos archivos pueden presentarse como archivos adjuntos o como enlace, en el cuerpo del correo.

Preste atención a las siguientes recomendaciones para evitar ser víctima de esta amenaza y compártalas con los usuarios para que también se protejan:

* Informe a los usuarios de las compañías que no abran ni ejecuten archivos de correos electrónicos, páginas web o medios extraíbles, que provengan de sitios no oficiales.

* Actualice bases de datos de firmas de virus de nuestras soluciones Endpoint, que hasta este momento es la base con identificador 13116 (20160302).

* Si cuenta con equipos infectados, desconéctelos de la red de organización, con el fin de aislarlos de los demás equipos no infectados y servidores.

* Tenga en cuenta que la mejor práctica siempre será (y siempre fue) protegerse del ransomware y de la pérdida de datos mediante backups de rutina. Así, pase lo que pase, el usuario que ha sido atacado, será capaz de reiniciar su vida digital rápidamente.

Agradecemos a todos los funcionarios tener en cuenta estas recomendaciones.
Gerencia de Infraestructura de TI

Fuente: El autor

Por otro lado, durante la semana del 25 al 29 de abril en Casa Matriz, se realizó la primer Feria SGSI, esta actividad se concibió con el objetivo de capacitar a todos los colaboradores sobre conceptos básicos de la seguridad informática y de la información, como parte de integral del diseño y puesta en marcha de un sistema de seguridad que garantice la confidencialidad, disponibilidad, integridad y trazabilidad de la información tratada por esta sede.

Ilustración 41 Comunicado Feria SGSI

Fuente: El autor

La Feria SGSI consiste en un concurso a nivel Casa Matriz y Regional Bogotá, en la cual se solicita a todos los colaboradores de estas sucursales, conformar un equipo de máximo 8 integrantes, dentro de los cuales era importante vincular a un directivo o aliado estratégico para poder participar. La inscripción a este evento se llevó a cabo mediante el diligenciamiento de una plantilla la cual era remitida a una de las funcionarias de la Gerencia de Infraestructura TI, quienes son los

encargados de esta actividad. El equipo conformado debía tener un nombre, lema y vestuario alusivo a los colores de la entidad.

La Feria SGSI se estructuro por estaciones de tal forma que los conceptos básicos sobre seguridad informática y de la información se abarcaran de forma clara y precisa. La actividad conto con los profesionales del aliado estratégico ADA y de la Gerencia de Infraestructura. La Feria se agendo de forma tal, que durante las dos jornadas realizadas en el día, se contara con la participación de 6 grupos.

Cada estación contaba con una atracción didáctica que le permitía al colaborador aprender de forma divertida, una vez se brindaba la charla sobre los temas mencionados, se realizaba una serie de preguntas por las cuales se otorga un puntaje de 5 puntos si contestaba correctamente y de 2 si realizaba más de un intento en resolver la pregunta. El puntaje en juego durante la jornada, equivalía a 100 puntos, el grupo que obtuviera dicho puntaje se declaraba el ganador de la actividad y posteriormente era premiado.

Ilustración 42 Agenda para la Feria SGSI

Fuente: El autor

Ilustración 43 Ganadores primer jornada Feria SGSI

Fuente: El autor

Ilustración 44 Ganadores segunda jornada Feria SGSI

Fuente: El autor

Otro de los resultados relevantes de este ejercicio, se relaciona con la definición del alcance, objetivos y política del Sistema de Gestión de Seguridad de la Información y la definición de la política de seguridad de la información la cual se contempló en el numeral 9.3 Alcance SGSI y 9.5 Alcance de la política de seguridad y en la numeración subsiguiente se encuentra la política propuesta para ser aprobada por las directivas de la entidad.

Por otro lado, también se cuenta con la revisión y actualización que se lleva a cabo en la entidad a fin de validar y verificar la pertinencia de los documentos soporte de algunos lineamientos y controles puestos en marcha años atrás y que deben ser analizados a fin de implementar el SGSI propuesta en este proyecto.

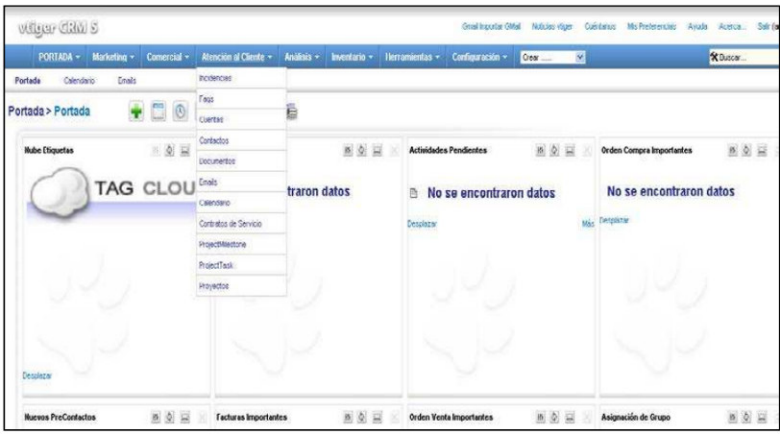
Finalmente se cuenta con el avance en materia de reporte de incidentes de seguridad informática, el objetivo de esta actividad es promover el canal de comunicación para que los funcionarios de Casa Matriz puedan reportar de forma oportuna incidentes o eventos y así asegurar el tratamiento de los mismos por parte de los profesionales de Informática.

La herramienta piloto dispuesta para esto es Vtiger CRM 5.0, de acuerdo a imagen adjunta:

Ilustración 45 Aplicación Vtiger CRM

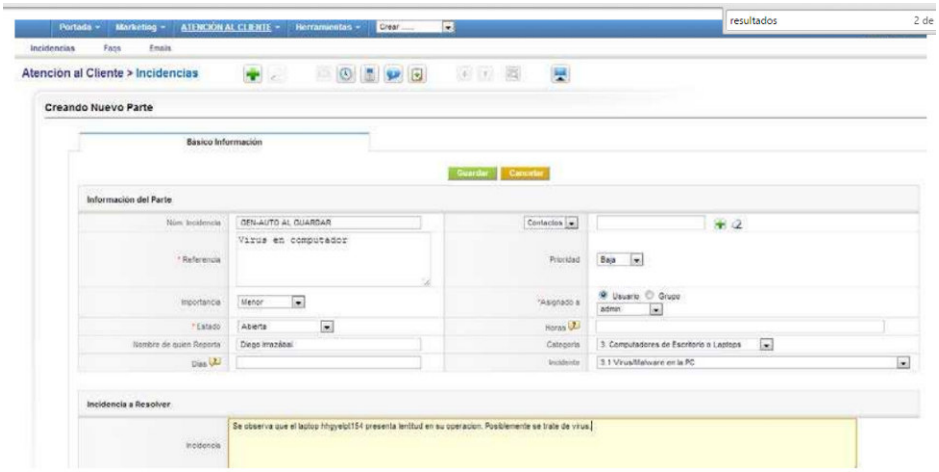
Fuente: El Autor

Ilustración 46 Reporte de incidentes informáticos



Fuente: El autor

Ilustración 47 Reporte de eventos



Fuente: El autor

12. DIVULGACIÓN

Con el fin de socializar el desarrollo y los resultados obtenidos del presente proyecto de grado, se determinó los siguientes medios de divulgación:

- Publicación en el espacio denominado UNIVERSITAS XXI ubicado en la página web de la UNAD, pues allí es posible publicar el contenido del proyecto de grado y sus avances.
- Plegables diseñados de forma sencilla y ágil para facilitar la comprensión del proyecto. El objetivo es llegar a un público puntual para garantizar la socialización del tema tratado en el proyecto de grado.
- Campañas informativas mediante afiches y carteleras dirigidas a la comunidad estudiantil de la UNAD y las organizaciones del sector asegurador.
- Utilización de la emisora Radio UNAD Virtual para distribuir información sobre el proyecto de grado.

BIBLIOGRAFÍA E INFOGRAFÌA

AGUILERA, Purificación. Seguridad Informática: Ciclos Formativos. México: Editex, 2010. 9 p.

MARTOS, Fernando. Centros Hospitalarios de Alta Resolución de Andalucía-Auxiliares Administrativos. 1 ed. España: Mad-eduforma, 2006. 195 p.

Lanzan pólizas de seguros para amparar ataques informáticos. En: PORTAFOLIO. Bogotá, D.C.23, Agosto, 2015, 2. Sec. p.5

SEGUNDA COHORTE DEL DOCTORADO EN SEGURIDAD ESTRATÉGICA. Seguridad de la Información. En: Marzo, 2014, No. 1, p 15-16

INSTITUTO COLOMBIANO DE NORMALIZACIÒN Y CERTIFICACIÒN. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. NTC-ISO-IEC 27001. Bogotá, D.C.: El Instituto, 2013. 37 p.

INSTITUTO COLOMBIANO DE NORMALIZACIÒN Y CERTIFICACIÒN. Tecnología de la información. Técnicas de seguridad. Código de Práctica para la gestión de la Seguridad de la Información. Requisitos. NTC-ISO-IEC 27002. Bogotá, D.C..: El Instituto, 2013. 37 p.

MINISTERIO DEL INTERIOR Y DE JUSTICIA. Dirección nacional de derecho de autor. Unidad administrativa especial. Manual de Derecho de Autor. Bogotá, D.C.: El ministerio, 2010. 9 p.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Formato e implementación de políticas de seguridad y privacidad de la información. Bogotá, D.C.: El ministerio, 2014. 19 p.

ORGANIZACIÓN INTERNACIONAL PARA LA ESTANDARIZACIÓN. Sistema de Gestión de la Seguridad de la Información. ISO/IEC 27001. España.: El instituto, 2013. 14 p.

AGUIRRE, Juan David y ARISTIZABAL, Catalina. Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la ofrenda. Trabajo de grado. Pereira.: Universidad Tecnológica de Pereira. Facultad de Ingenierías. Programa de Ingeniería de Sistemas y Computación, 2013. 23 p.

AREVALO, Oscar William. Metodología de Análisis de Riesgo de la Empresa la Casa de las Baterías S.A de C.V Trabajo de Grado. El Salvador: Universidad Tecnológica del Salvador. Facultad de Ingeniería. Desarrollo de Redes, 2009. 27 p.

DE FREITAS, Vidalina. Análisis y Evaluación del Riesgo de la información. Caso de Estudio Venezuela. Universidad Simón Bolívar. Revista Venezolana de Información, Tecnología y Conocimiento, 2009. 55 p.

DIAZ, Flor Nancy. Principales Estándares para la Seguridad de la Información IT. Investigación. España.: Universidad Pontificia de Salamanca, 2015. 83 p.

GAONA, Karina. Aplicación de la metodología Magerit para el análisis y gestión de Riesgos de la Seguridad de la Información aplicado a la Empresa Pesquera e Industrial Bravito S.A. en la ciudad de Machala. Trabajo de Grado. México: Facultad de Ingeniería de Sistemas, 2013. 76 p

GONZALEZ, Frank. Diagnóstico y Actualización del Sistema de Gestión de Seguridad de la Información (SGSI) para Ventas y Servicios S.A. Trabajo de grado. Bogotá D.C.: Universidad Católica de Colombia. Programa de Ingeniería de Sistema, 2013. 63 p

GUZMAN, Carlos. Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad financiera de segundo piso. Trabajo de grado. Bogotá, D.C.: Institución Universitaria Politécnico GranColombiano. Facultad de Ingeniería y Ciencias Básicas. 2015. 173 p.

COLOMBIA. SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Decreto ley 19 de 2012, artículo 160 (10, enero, 2012). Por el cual se dictan normas

para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública. Bogotá: La superintendencia, 2012. 5 p.
COLOMBIA. ALCALDÍA MAYOR DE BOGOTÁ. Resolución 26930 de 2000 (26, octubre, 2000) Por la cual se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores. Bogotá, D.C.: La alcaldía, 2000.

COLOMBIA. OFICINA JURIDICA NACIONAL. Concepto No. 5 (2, febrero, 2009) Concepto sobre suministro de bases de datos con propósitos académicos. Bogotá, D.C.: La oficina, 2009. 3 p.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (5, enero, 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 preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras. Diario oficial. Bogotá, D.C., 2009. No. 47223. p 1.

COLOMBIA. PRESIDENCIA DE LA REPUBLICA. Decreto 1377 (27, junio, 2013). Por medio del cual se reglamenta la Ley 1581 de 2012. Diario oficial. Bogotá, D.C., 2013. No. 48834. p 3.

COLOMBIA. CONGRESO SE LA REPUBLICA. Ley 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario oficial. Bogotá, D.C., 2012. No. 48587. p 2.

CUERVO, Diego. Aspectos Jurídicos de Internet y el comercio electrónico. En: http://www.informaticajuridica.com/trabajos/Aspectos_juridicos_de_Internet_y_el_comercio_electronico.a. Octubre, 2012. Vol. 1, no. 2, 5 p.

EVERIS. Estudio de Gestión de Riesgos en el Sector Asegurador. Informe unidad de servicios de seguros. Bogotá, D.C.: 2009, MFC artes gráficas. 111 p. En:http://www.everis.com/COLOMBIA/WCRepositoryFiles/GESTION%20RIESGOS%20EN%20EL%20SECTOR%20ASEGURADOR.pdf

FIDUAGRARIA. Amenazas y riesgos en el manejo de la información. Informe defensor del consumidor financiero. Bogotá, D.C. 2012. 5 p En: http://www.fiduagraria.gov.co/wp-content/uploads/2014/12/Amenazas-y-riesgos-en-el-manejo-de-la-informacion.pdf

CONSEJO SUPERIOR DE ADMINISTRACIÓN ELECTRÓNICA. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. MAGERIT versión 3.0. Libro I- Método. En: //http: www.ccn.-cert.cni.es /publico/herramientas/pilar5/magerit.
CONSEJO SUPERIOR DE ADMINISTRACIÓN ELECTRÓNICA. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. MAGERIT versión 3.0. Libro II- Catálogo. En: http://www.ccn.-cert.cni.es /publico/herramientas/pilar5/magerit.

CONSEJO SUPERIOR DE ADMINISTRACIÓN ELECTRÓNICA. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. MAGERIT versión 3.0., Libro III- Guía Técnica. En: http://www.ccn.-cert.cni.es /publico/herramientas/pilar5/magerit.

POSITIVA COMPAÑÍA DE SEGUROS S.A. Caracterización Proceso Vicepresidencia TIC´S.: La entidad, 2012. 48 p. En: https://www.positiva.gov.co/positiva/ViceTIC´S/Documents/caracterización%20de%20proceso%202012.pdf

POSITIVA COMPAÑÍA DE SEGUROS S.A. Informe de Gestión 2014.: La entidad, 2014. 31 p. En: https://www.positiva.gov.co/positiva/PlaneacionGestion/Documents/INFORME%20DE%20GESTION%202014.pdf

POVEDA, José. Análisis y valoración de los riesgos-Metodologías. Artículo. Bogotá D.C.: Universidad Católica de Colombia. Programa de Ingeniería de Sistema, 2013. 63 p. En: https://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-8.pdf

PRANDINI, Patricia y PALLERO, Marcela. Vulnerabilidades, amenazas y riesgo. (25, agosto, 2015). En: http://www.magazcitum.com.mx/?p=2193.

¿Seguridad informática o seguridad de la información? (25, septiembre, 2015) En: http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html

WORDPRESS. Gestión de Riesgos en la Seguridad. Informática. (02, marzo, 2015) En: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

Anexo B.

Formato para la aplicación de entrevista sobre generalidades de la Seguridad Informática en Casa Matriz

Entrevista a los líderes de proceso en Casa Matriz

El presente es un cuestionario sencillo que pretende evidenciar el conocimiento del concepto de seguridad informática y lo que este abarca.

Seguridad General

- ✓ ¿De cuántos ordenadores dispone su área?

  1-10 10-20 +20

- ✓ Los equipos de cómputo de su área, ¿tienen instalado antivirus?

  Sí No n/s

- ✓ El antivirus que tienen instalado (si es el caso), ¿está actualizado con las últimas definiciones?

  Sí No n/s

- ✓ ¿Se realiza un mantenimiento informático periódico sobre los ordenadores de la empresa?

  Sí No n/s

- ✓ ¿Se utilizan programas de descarga de archivos de usuario (música, películas, programas...)?

Sí No n/s

- ✓ ¿Conoce si Casa Matriz cuenta con un servidor central de datos?

  Sí No

- ✓ Sobre dicho servidor, ¿sabe si se le realiza un mantenimiento informático periódico?

  Sí No n/s

Comunicaciones

- ✓ ¿En la entidad se trabaja desde algún ordenador externo, por conexión vía Internet?

  Sí No n/s

- ✓ Si la conexión en Casa Matriz es mediante la red (WIFI), ¿conoce si se utilizan las medidas de seguridad pertinentes para proteger dicha conexión?

  Sí No n/s

Datos de la empresa

- ✓ ¿Los computadores de su área tienen datos de la empresa almacenados en el disco duro?

  Sí No n/s

- ✓ ¿Se realiza copia de seguridad de la información que maneja su área?

  Sí No n/s

Con qué frecuencia

Diaria semanal otro

¿Usted o sus colaboradores a cargo poseen alguna copia de seguridad (USB / DVD / ..Otro) fuera de la empresa?

Sí No n/s

¿Se realiza un mantenimiento de las copias de seguridad de Casa Matriz?

Sí No n/s

Programas y Aplicaciones Informáticas

¿Los programas y aplicaciones usadas en Casa Matriz, cumplen con las características de seguridad informática propuestas por Positiva?

Sí No n/s

¿Hay algún encargado de instalar/desinstalar los programas y aplicaciones informáticas en Casa Matriz?

Sí No n/s

Seguridad Informática

¿Conoce usted algo referente a la seguridad informática?

Sí No algo

Dígame que sabe al respecto

¿La compañía ha dispuesto políticas de seguridad para el manejo de las herramientas informáticas de las que disponen para la gestión de su proceso?

Sí No n/s

¿Cuáles?

¿Qué medidas de seguridad toma para proteger la información que trata su área?

Anexo C.

<table>
<tr><td>  </td><td colspan="2">Positiva Compañía de Seguros S. A.</td></tr>
<tr><td>Código:
VA-OD-CCLUS-03</td><td rowspan="2">CARTA DE COMPROMISO DE LICENCIAMIENTO, USO DE SOFTWARE Y CUMPLIMIENTO DE POLÍTICAS INFORMÁTICAS</td><td>Pagina:1de 1
Fecha actualización: 30/06/2012</td></tr>
<tr><td>Aprobado Por:
Gerente de Informática</td><td>Revisado por:
Profesional Informática</td></tr>
</table>

Los programas de computador instalados en **Positiva Compañía de Seguros S. A.** están protegidos por la ley de Derechos de Autor (ley 23 de 1982, ley 44 de 1993, Decisión 351 de 1993, ley 603 del 2000). La empresa y/o persona que no cumpla con lo estipulado en la licencia correspondiente está violando la ley de derechos de autor vigente y se expone a enfrentar juicios civiles y penales, pagar cuantiosas indemnizaciones y enfrentar publicidad adversa.

Todo software de índole gratuito, Demos o Freeware no se deberá instalar sin la previa autorización de la Gerencia de Informática,

En consecuencia no deberá estar instalado software no licenciado, juegos, software de ataques a las redes, así como material con contenido erótico.

La utilización de este tipo de software hará responsable al empleado y/o tercero por los eventuales perjuicios que lleguen a causarse al computador y a la Red de la Compañía.

Ningún funcionario y/o tercero de la Compañía podrá instalar, ejecutar, copiar ni hacer uso de Software que no haya sido licenciado, adquirido e instalado por la Gerencia de informática o por las entidades externas autorizadas.

Así mismo me comprometo a consultar y aplicar las políticas informáticas, establecidas en el manual de Calidad de la Compañía y publicadas en la Intranet.

De acuerdo con lo anterior yo _____**,**

Identificado con cédula de ciudadanía número _____ aseguro que he entendido esta información, estoy de acuerdo con ella y me comprometo a abstenerme de instalar software que no esté debidamente licenciado y autorizado por la empresa para desempeñar mis funciones.

_____

FIRMA

NOMBRE:

C.C

Anexo D.

Lineamiento Básico de Seguridad

No.	ACTIVIDAD	RESPONSABLE
1	En el proceso de alistamiento de una estación de trabajo (Windows 7) se debe hacer una instalación nueva con la herramienta utilizada en el área.	Soporte Técnico
2	Realizar la verificación de instalación de sysprep para las estaciones de trabajo.	
3	Se deben crear dos particiones lógicas C: \, D: \, en la cual C deben ir el S.O y los programas de instalación y actualizaciones, en la unidad D se debe configurar el perfil del usuario (Datos, Pst).	
4	Sin excepción, toda instalación del sistema Operativo se debe realizar personalizado, nunca por defecto; teniendo presente las actividades, 5, 6.	
5	Según el caso, valide las siguientes opciones y proceda según corresponda, así: a. Desinstale los juegos. b. Desinstale el papel tapiz que viene por defecto y las imágenes. c. Desinstale los punteros del Mouse. e. Deshabilite la opción de otros servicios de impresión y archivo de red. f. Desinstale Media Player. g. Deshabilite el servicio de fax. h. No debe tener instalado IIS. i. Desinstale el servicio de mensajería instantánea Windows Messenger. j. El firewall local del Sistema Operativo debe quedar habilitado con las excepciones necesarias para su funcionamiento. k. Se deben revisar los servicios y puertos que publica la estación, los cuales deben ser solo los estrictamente los necesarios; esto va integrado con las excepciones del firewall local de la estación de trabajo. l. Verifique si es necesario, que en la opción de directivas de seguridad local /directivas locales /opciones de seguridad / nivel de autenticidad de Lan Manager /	Soporte Técnico

	debe estar la opción enviar respuesta LM y NTLM. n. Configurar en la opción Propiedades de conexión de área local /Protocolo Internet TCP/IP /Propiedades /Opciones Avanzadas / DNS/Sufijo DNS para esta conexión debe estar ¿	
6	Verifique la versión del software antivirus de la máquina y compárela con la última versión Corporativa (ESET), si no es la última versión, actualícela, Verificar con el Administrador, que estas se reportan con la consola de la aplicación (IP). Verifique la restricción de puertos USB.	Soporte Técnico
7	Verifique con el administrador del Antivirus, que la estación de trabajo se reporta en la consola ESET y cada uno de sus componentes se encuentre actualizados.	
8	Ingrese la estación al dominio Positiva.col, la cual debe cumplir con el estándar de nombres; esta debe ser autorizada y/o reportada al profesional de seguridad Informática.	
9	Revise que en la estación (Sistema Operativo) tenga instalado las actualizaciones críticas, office y de seguridad como ServicePack y hotfix. Las cuáles serán descargadas del WSUS.	
10	Solo las máquinas autorizadas tienen configurado el servicio de escritorio remoto y las cuentas autorizadas para ello.	
11	La cuenta de administración local queda bajo custodia Del profesional de infraestructura asignado para su control y la cual se debe renombrar por ESTATEC.	
12	Instale los agentes de Aranda	Soporte Técnico
13	Verificar que en las opciones del explorador de Internet, en configuración de LAN, no quede activa ninguna de las opciones de configuración automática y proxy.	

Guía Base de Seguridad para Usuarios Locales

No.	ACTIVIDAD	RESPONSABLE
1	Se deben revisar los permisos asignados a los discos duros de la estación de trabajo, los cuales deben estar así: ➔ Administrador local. WRX ➔ Administradores locales. WRX ➔ System. WRX ➔ Creator Owner. WRX	Profesional de seguridad informática

	➔ Grupo usuarios RX	
2	Las carpetas compartidas deben ser estrictamente autorizadas, parametrizadas a través de las pestañas de compartir y seguridad, y delimitada por cantidad de usuarios que se conectan; las cuales deben estar documentadas; con permisos de sólo lectura o escritura de acuerdo con su función, pero nunca de control total.	Profesional de seguridad informática
3	Verifique que en (administración de equipos,) en la opción (usuarios locales y grupos), en la opción (Administradores), deben estar las cuentas del administrador local, Domain Admin y el grupo soportepc únicamente. Para los casos en que los usuarios requieren ser administradores del equipo previa autorización de seguridad informática deben ser ingresados al grupo administradores	
4	En el grupo (usuarios) deben estar las cuentas de Dominio\Domain Users, NT Authority\interactive y NT Authority\Usuarios autentificados únicamente; los cuales son creados en la instalación del Sistema Operativo y al agregar la estación de trabajo al dominio.	
5	En ningún de los grupos, debe existir cuentas de usuario, excepto en los grupos administradores y usuarios, las cuales contienen las cuentas mencionadas previamente.	
6	La cuenta de administrador local queda bajo custodia del profesional de infraestructura; la cuenta de invitado debe quedar eliminada.	
7	Sistema de archivos: En los discos duros (raíz) deben quedar configurada la pestaña de seguridad, con los siguientes atributos: a. Administrador: control total. b. Administradores: Control total. c. Creator Owner: Sólo debe estar habilitado el campo de Permitir “permisos especiales” para Windows 7 debe tener control total. d. El usuario system, permitir “control total”. e. El grupo de Usuarios (Nombre de Maquina\Usuarios), que contiene el grupo (Dominio \Domain Users), debe tener habilitado permitir “lectura y ejecución” y “Mostrar el contenido o listar”.	Profesional de seguridad informática
8	Se debe configurar las auditorias locales de seguridad, de los eventos fallidos y realizar la respectiva excepción en el firewall de Windows → Configuración Avanzada En Reglas de entrada Todas las opciones de Administración remota de registro de eventos Se debe definir el tamaño de los log´s de Sistema, Seguridad y Aplicación en; Sistema y aplicación 40 Mb ; Seguridad en 120 MB	Profesional de seguridad informática

ANEXO D.

Formato para la aplicación de entrevista sobre objetivos de control y controles establecidos por la Norma ISO/IEC 27002: 2013

Entrevista al Gerente de infraestructura y Soporte de TIC´S

El presente es un cuestionario sencillo que pretende evidenciar el grado de cumplimiento de los objetivos de control y controles establecidos en el Estándar ISO/IEC 27002:2013.

Política de Seguridad de la información

- ✓ Positiva, en especial Casa Matriz ¿cuenta con una política de Seguridad de la información establecida y socializada con todo el personal?

  Sí No (x) n/s

- ✓ ¿Se tienen implementados controles para validar el cumplimiento de la política de seguridad?

  Sí No (x) n/s

- ✓ ¿Las políticas de seguridad de la información son conocidas por todos los colaboradores de Casa Matriz?

  Sí No (x) n/s

Aspectos organizacionales para la seguridad de la información

- ✓ ¿Tiene Casa Matriz un lugar específico para actividades relacionadas con la seguridad de la información?

  Sí No n/s

- ✓ ¿Positiva cuenta o a contado con algún tipo de asesoramiento en materia de seguridad de la información?

  Sí No n/s

- ✓ ¿La entidad en el momento de gestionar contratos con terceros, contratistas u otros, exige algún tipo de cláusulas de seguridad de la información?

  Sí No n/s

Con relación a la clasificación y control de activos

- ✓ ¿Se tiene un inventario de activos de información actualizado o se actualiza periódicamente?

  Sí No n/s

- ✓ ¿Dicho inventario esta automatizado?

  Sí No n/s

Políticas del personal con relación a la seguridad informática

- ✓ ¿Los incidentes de seguridad de los sistemas de información son reportados por los usuarios?

  Sí No n/s

- ✓ ¿Positiva cuenta con acuerdos de confidencialidad de la información?

  Sí No n/s

Seguridad física y ambiental de los sistemas de información

- ✓ ¿Las áreas o dependencias están debidamente identificadas en Casa Matriz?

  Sí No n/s

- ✓ ¿Se cuenta con controles de ingreso de personal para las áreas seguras?

  Sí No n/s

- ✓ En el evento en que ocurra una falla en el cableado de datos, ¿está preparada Casa Matriz para corregir el daño y continuar con la operación?

Sí No n/s

- ✓ ¿En las instalaciones de Casa Matriz se realiza periódicamente mantenimiento al hardware y software?

Sí No n/s

Gestión de las comunicaciones de datos y operaciones en los sistemas informáticos

- ✓ La Casa Matriz de Positiva cuenta con controles que contrarresten el software malicioso (antivirus, antispyware)?

Sí No n/s

- ✓ ¿Se cuenta con registros de acceso, uso de los aplicativos y servicios de la red por parte de los funcionarios?

Sí No n/s

- ✓ ¿Existen controles para regular los medios de almacenamiento?

Sí No n/s

- ✓ ¿Casa Matriz cuenta con compromisos sobre el uso de los recursos informáticos?

Sí No n/s

Control de acceso

- ✓ ¿Para el ingreso a las aplicaciones y sistemas de información hay establecidos controles de acceso?

Sí No n/s

- ✓ ¿Hay un registro de todos los usuarios, perfiles y privilegios otorgados?

Sí No n/s

- ✓ ¿Todas las aplicaciones utilizadas en Casa Matriz requieren de una contraseña para ingresar?

  Sí No n/s

- ✓ Para las conexiones remotas ¿se tienen establecidos mecanismos de autenticación de usuarios a la red interna de Positiva?

  Sí No n/s

- ✓ ¿Hay implementados controles para el monitoreo de los recurso informáticos en Casa Matriz?

  Sí No n/s

Desarrollo y mantenimiento de sistemas informáticos

- ✓ En cuanto al desarrollo de aplicaciones ¿se tienen controles de validación de datos de entrada y de salida?

  Sí No n/s

- ✓ ¿La entidad cuenta con controles criptográficos para el cifrado de datos?

  Sí No n/s

- ✓ ¿Se tienen controles que eviten el acceso no autorizado a los códigos fuente de las aplicaciones?

  Sí No n/s

- ✓ ¿Está establecido el procedimiento de control de cambios para las aplicaciones, software y sistema operativo?

  Sí No n/s
- ✓ ¿Son validados y verificados los códigos fuente desarrollados por personal externo antes de su puesta en producción?

  Sí No n/s

Gestión de incidentes

- ✓ ¿Cuenta Casa Matriz con un procedimiento formal para el reporte de incidentes?

  Sí No n/s

- ✓ ¿Posee Casa Matriz una herramienta para el registro de incidentes?

  Sí No n/s

- ✓ Una vez reportado un incidente, ¿posee Casa Matriz equipos de respuesta?

  Sí No n/s

- ✓ Dado el incidente de seguridad, la información relacionada es recolecta, investigada y analizada

  Sí No n/s

Plan de continuidad

- ✓ ¿Se tiene establecido un plan de contingencia en Casa Matriz?

  Sí No n/s

- ✓ ¿El plan de continuidad del negocio es probado, evaluado y se le realiza mantenimiento?

  Sí No n/s

Cumplimiento legal

- ✓ ¿Está debidamente identificada la normatividad vigente aplicable y que regula las aplicaciones usadas en Casa Matriz?

  Sí No n/s

- ✓ Casa Matriz se pone en práctica la normatividad regulatoria de la protección de datos y privacidad de la información de sus grupos de interés

  Sí No n/s

ANEXO E

	FORMATO
	RESUMEN ANALÍTICO EN EDUCACIÓN - RAE
Código:	**Versión: 01**
Fecha de Aprobación:	**Página 247 de 257**

1. Información General	
Tipo de documento	Proyecto de Aplicado
Acceso al documento	Universidad Nacional Abierta y a Distancia
Título del documento	Diseño de un Sistema de Gestión de seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 para Positiva Compañía de Seguros S.A. en la ciudad de Bogotá
Autor(es)	ARDILA, Julián
Director	GONZALEZ, Salomón
Publicación	Bogotá. Universidad Nacional Abierta y a Distancia, 2016. P. 143.
Unidad Patrocinante	Positiva Compañía de Seguros S.A.
Palabras Claves	Seguridad informática y de la información, Sistema de seguridad informática, vulnerabilidades, amenazas, riesgos, análisis de riesgos, metodología de evaluación y gestión del riesgo MAGERIT 3.0,ISO/IEC 27001 e ISO/IEC 27002.

2. Descripción
El proyecto de grado, detalla el diseño de un Sistema de Gestión de la Seguridad de la información- SGSI basado en la norma ISO/IEC 27001 para la entidad Positiva Compañía de Seguros S.A. El objetivo es identificar cómo el proyecto proveerá a dicha organización, los elementos, mecanismo y lineamientos adecuados para garantizar la integridad, disponibilidad y confiabilidad de la información tratada por esta aseguradora; además, pretende evidenciar la medida en que la implementación de este sistema, mejorará la seguridad de la información disminuyendo el impacto reputacional y operacional, la probabilidad de ocurrencia de las

vulnerabilidades, amenazas y riesgos.

3. Fuentes

AGUILERA, Purificación. Seguridad Informática: Ciclos Formativos. México: Editex, 2010. 9 p.

MARTOS, Fernando. Centros Hospitalarios de Alta Resolución de Andalucía-Auxiliares Administrativos. 1 ed. España: Mad-eduforma, 2006. 195 p.

Lanzan pólizas de seguros para amparar ataques informáticos. En: PORTAFOLIO. Bogotá, D.C.23, Agosto, 2015, 2. Sec. p.5

SEGUNDA COHORTE DEL DOCTORADO EN SEGURIDAD ESTRATÉGICA. Seguridad de la Información. En: Marzo, 2014, No. 1, p 15-16

INSTITUTO COLOMBIANO DE NORMALIZACIÒN Y CERTIFICACIÒN. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. NTC-ISO-IEC 27001. Bogotá, D.C.: El Instituto, 2013. 37 p.

INSTITUTO COLOMBIANO DE NORMALIZACIÒN Y CERTIFICACIÒN. Tecnología de la información. Técnicas de seguridad. Código de Práctica para la gestión de la Seguridad de la Información. Requisitos. NTC-ISO-IEC 27002. Bogotá, D.C..: El Instituto, 2013. 37 p.

MINISTERIO DEL INTERIOR Y DE JUSTICIA. Dirección nacional de derecho de autor. Unidad administrativa especial. Manual de Derecho de Autor. Bogotá, D.C.: El ministerio, 2010. 9 p.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Formato e implementación de políticas de seguridad y privacidad de la información. Bogotá, D.C.: El ministerio, 2014. 19 p.

ORGANIZACIÓN INTERNACIONAL PARA LA ESTANDARIZACIÓN. Sistema de Gestión de la Seguridad de la Información. ISO/IEC 27001. España.: El instituto, 2013. 14 p.

AGUIRRE, Juan David y ARISTIZABAL, Catalina. Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la ofrenda. Trabajo de grado. Pereira.: Universidad Tecnológica de Pereira. Facultad de Ingenierías. Programa de Ingeniería de Sistemas y Computación, 2013. 23 p.

AREVALO, Oscar William. Metodología de Análisis de Riesgo de la Empresa la Casa de las Baterías S.A de C.V Trabajo de Grado. El Salvador: Universidad Tecnológica del Salvador. Facultad de Ingeniería. Desarrollo de Redes, 2009. 27 p.

DE FREITAS, Vidalina. Análisis y Evaluación del Riesgo de la información. Caso de Estudio Venezuela. Universidad Simón Bolívar. Revista Venezolana de Información, Tecnología y Conocimiento, 2009. 55 p.

DIAZ, Flor Nancy. Principales Estándares para la Seguridad de la Información IT. Investigación. España.: Universidad Pontificia de Salamanca, 2015. 83 p.

GAONA, Karina. Aplicación de la metodología Magerit para el análisis y gestión de Riesgos de la Seguridad de la Información aplicado a la Empresa Pesquera e Industrial Bravito S.A. en la ciudad de Machala. Trabajo de Grado. México: Facultad de Ingeniería de Sistemas, 2013. 76 p

GONZALEZ, Frank. Diagnóstico y Actualización del Sistema de Gestión de Seguridad de la Información (SGSI) para Ventas y Servicios S.A. Trabajo de grado. Bogotá D.C.: Universidad Católica de Colombia. Programa de Ingeniería de Sistema, 2013. 63 p

GUZMAN, Carlos. Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad financiera de segundo piso. Trabajo de grado. Bogotá, D.C.: Institución Universitaria Politécnico GranColombiano. Facultad de Ingeniería y Ciencias Básicas. 2015. 173 p.

COLOMBIA. SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Decreto ley 19 de 2012, artículo 160 (10, enero, 2012). Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública. Bogotá: La superintendencia, 2012. 5 p.

COLOMBIA. ALCALDÍA MAYOR DE BOGOTÁ. Resolución 26930 de 2000 (26, octubre, 2000) Por la cual se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores. Bogotá, D.C.: La alcaldía, 2000.

COLOMBIA. OFICINA JURIDICA NACIONAL. Concepto No. 5 (2, febrero, 2009) Concepto sobre suministro de bases de datos con propósitos académicos. Bogotá, D.C.: La oficina, 2009. 3 p.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (5, enero, 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 preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras. Diario oficial. Bogotá, D.C., 2009. No. 47223. p 1.

COLOMBIA. PRESIDENCIA DE LA REPUBLICA. Decreto 1377 (27, junio, 2013). Por medio del cual se reglamenta la Ley 1581 de 2012. Diario oficial. Bogotá, D.C., 2013. No 48834 p 3.

COLOMBIA. CONGRESO SE LA REPUBLICA. Ley 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario oficial. Bogotá, D.C., 2012. No. 48587. p 2.

CUERVO, Diego. Aspectos Jurídicos de Internet y el comercio electrónico. En: http://www.informaticajuridica.com/trabajos/Aspectos_juridicos_de_Internet_y_el_comercio_electronico.a. Octubre, 2012. Vol. 1, no. 2, 5 p.

EVERIS. Estudio de Gestión de Riesgos en el Sector Asegurador. Informe unidad de

servicios de seguros. Bogotá, D.C.: 2009, MFC artes gráficas. 111 p. En:http://www.everis.com/COLOMBIA/WCRepositoryFiles/GESTION%20RIESGOS%20EN%20EL%20SECTOR%20ASEGURADOR.pdf

FIDUAGRARIA. Amenazas y riesgos en el manejo de la información. Informe defensor del consumidor financiero. Bogotá, D.C. 2012. 5 p En: http://www.fiduagraria.gov.co/wp-content/uploads/2014/12/Amenazas-y-riesgos-en-el-manejo-de-la-informacion.pdf

CONSEJO SUPERIOR DE ADMINISTRACIÓN ELECTRÓNICA. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. MAGERIT versión 3.0. Libro I- Método. En: //http: www.ccn.-cert.cni.es /publico/herramientas/pilar5/magerit.

CONSEJO SUPERIOR DE ADMINISTRACIÓN ELECTRÓNICA. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. MAGERIT versión 3.0. Libro II-Catálogo. En: http://www.ccn.-cert.cni.es /publico/herramientas/pilar5/magerit

CONSEJO SUPERIOR DE ADMINISTRACIÓN ELECTRÓNICA. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. MAGERIT versión 3.0., Libro III- Guía Técnica. En: http://www.ccn.-cert.cni.es /publico/herramientas/pilar5/magerit.

POSITIVA COMPAÑÍA DE SEGUROS S.A. Caracterización Proceso Vicepresidencia TIC´S.: La entidad, 2012. 48 p. En: https://www.positiva.gov.co/positiva/ViceTIC´S/Documents/caracterización%20de%20proceso%202012.pdf

POSITIVA COMPAÑÍA DE SEGUROS S.A. Informe de Gestión 2014.: La entidad, 2014. 31 p. En: https://www.positiva.gov.co/positiva/PlaneacionGestion/Documents/INFORME%20DE%20GESTION%202014.pdf

POVEDA, José. Análisis y valoración de los riesgos-Metodologías. Artículo. Bogotá D.C.: Universidad Católica de Colombia. Programa de Ingeniería de Sistema, 2013. 63 p. En: https://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-8.pdf

PRANDINI, Patricia y PALLERO, Marcela. Vulnerabilidades, amenazas y riesgo. (25, agosto, 2015). En: http://www.magazcitum.com.mx/?p=2193.

Seguridad Informática. (25, septiembre, 2015) En: http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html.

WORDPRESS. Gestión de Riesgos en la Seguridad. Informática. (02, marzo, 2015) En: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

4. Contenidos

El Proyecto de Grado consta de:

Objetivo general

Diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) para la Casa Matriz de Positiva Compañía de Seguros S.A. en la ciudad de Bogotá; basado en la Norma NTC-ISO-IEC 27001:2013

Objetivos específicos

Analizar la situación actual de la Casa Matriz, con relación a la Gestión de Seguridad de la Información.

Realizar un análisis y evaluación del riesgo identificando los recursos a proteger con incidencia directa en la operación de la entidad mediante una metodología de evaluación sistemática.

Determinar y evaluar la aplicabilidad de los controles de seguridad de la información bajo la norma ISO/IEC 27002:2013.

Establecer la política, alcance y objetivos del Sistema de Gestión de Seguridad de la Información para la Casa Matriz de Positiva.

- **Marco Referencial,** el cual está constituido por (marco de antecedentes, contextual, teórico, conceptual y legal)

- **Diseño Metodológico:** correspondiente a los pasos a seguir para recopilar información relevante para el desarrollo del proyecto de grado, por ejemplo: línea y tipo de investigación, área de investigación, técnicos y herramientas de recolección de información.

- **Metodología de desarrollo:** Con el fin de desarrollar satisfactoriamente la propuesta se contemplaron cuatro fases vitales las cuales a su vez, permitirán el diseño de un SGSI basado en la norma ISO/IEC 27001-2013 para Positiva Compañía de Seguros S.A, a saber:

Fase 1: Diagnostico de la situación actual en materia de seguridad informática en Casa Matriz

Fase 2: Identificar los activos informáticos, definir y aplicar de la metodología de análisis y gestión del riesgo.

Fase 3: Determinar y evaluar la aplicabilidad de los controles de seguridad de la información bajo

la norma ISO/IEC 27002:2013

Fase 4: Definición de la política, alcance y objetivos del Sistema de Gestión de Seguridad de la Información para la Casa Matriz de Positiva

Cronograma de actividades

Resultados y discusiones: Corresponde al desarrollo del proyecto de grado.

Divulgación: Determinación de medios de divulgación del proyecto de grado.

Conclusiones

Bibliografía e infografía

Anexos

5. Metodología

- La investigación se encuentra enmarcada por los planteamientos de la línea de investigación en Seguridad de la Información, Diseño e implementación de Sistemas de Gestión de Seguridad de la Información, políticas de seguridad, el buen uso de los recursos informáticos que involucra los funcionarios de la entidad bajo análisis.
- El tipo de investigación es exploratoria y descriptiva
- Las técnicas e instrumentos de recolección de información definidos corresponden a la observación, entrevista estructurada y encuesta.
-

La población de esta propuesta implica la Casa Matriz de Positiva ubicada en la ciudad de Bogotá pues es donde se centraliza toda la actividad de administración.

En tanto a la muestra se estima que involucrara cerca de 345 personas dentro de las cuales 35 son profesionales del área de informática e infraestructura y 310 son funcionarios que actúan como usuarios de los sistemas informáticos.

6. Conclusiones

- El diseño de un Sistema de Gestión de Seguridad de la Información basado en el estándar ISO/IEC 27001:2013, permite identificar los aspectos relevantes a tener en cuenta a la hora de establecer un modelo de seguridad de la información sólido y sostenible.
- La puesta en marcha de un Sistema de Gestión de Seguridad de la Información, inicia con un claro compromiso por parte de los directivos de la entidad, pues desde allí se fortalece la cultura de seguridad de la información tan fundamental de cara a la protección de los datos organizacionales.

- La declaración de aplicabilidad de la norma ISO/IEC 27001 evidencio el grado de madurez de Positiva frente a la administración de seguridad de la información, el cual se ubicó en el nivel medio y el grado de cumplimiento de los requisitos del estándar corresponde al 69% de lo requerido; esto es una alerta para que la entidad adopte medidas oportunas y fortalezca la cultura de seguridad de la información, pues de esta depende el éxito del SGSI por implementar y el consecución de los resultados estimados.
- El proceso de identificación de activos informáticos evidencio activos críticos que la organización desconocía y a su vez permitió estudiar las medidas apropiadas para protegerlos oportunamente.
- La aplicación de la metodología de análisis de riesgos Magerit, permitió a la aseguradora reconocer oportunamente la probabilidad y el impacto una vez se ha materializado una amenaza sobre los activos informáticos; a su vez establecer los controles apropiados para mitigar o contrarrestar el daño según corresponda.
- El hecho de que Positiva no contara con una política de seguridad de la información correspondía a no tener un lineamiento que guiara apropiadamente la gestión de los activos de información y los datos tratados por la misma, representaba un riesgo inminente que podía comprometer seriamente la confiabilidad de los asegurados, proveedores y colaboradores al no contar con un respaldo que garantizara la protección de la información.
- La ausencia de controles en materia de intercambio de información con terceros, representa un alto riesgos para la organización pues puede afectar considerablemente la relación con sus grupos de interés y la pérdida de confianza de los mismos, igualmente puede tener un impacto significativo en la reputación de la aseguradora que le costaría su participación en el mercado asegurador.
- La implementación de controles, el rediseño de algunos y la documentación de otros le permitirá a la entidad mejorar su nivel de madurez frente a la administración de seguridad de la información, el cumplimiento de los requisitos establecidos en el estándar ISO/IEC 27002 y al acatamiento de la Estrategia de Gobierno en Línea definida por el gobierno Nacional

Elaborado por:	Ardila Navarrete Julián Andrés
Revisado por:	González García Salomón

Fecha de elaboración del Resumen:	15	05	2016