UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

TEMA:

"SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LAS NORMAS ISO/IEC 27001 EN EL DATACENTER DE LA EMPRESA AMBACAR-AMBATO."

Trabajo de Graduación. Modalidad: Proyecto de Investigación, presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

LÍNEA DE INVESTIGACIÓN: Normas y Estándares

AUTOR: Escobar Meléndez Jhonatan Sebastián

TUTOR: Mg. Dennis Chicaiza

Ambato – Ecuador

Enero 2020

CERTIFICACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Investigación sobre el Tema:

"SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LAS NORMAS ISO/IEC 27001 EN EL DATACENTER DE LA EMPRESA AMBACAR-AMBATO" del señor Jhonatan Sebastián Escobar Meléndez estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Art. 16 del Capítulo II, del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad técnica de Ambato

Ambato, enero de 2020

EL TUTOR

Mg. Dennis Chicaiza

AUTORÍA DEL TRABAJO

El presente trabajo de investigación titulado: "SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LAS NORMAS ISO/IEC 27001 EN EL DATACENTER DE LA EMPRESA AMBACAR-AMBATO", es absolutamente original, auténtico y personal. En tal virtud, el contenido, efectos legales y académicos que se desprendan del mismo son de exclusiva responsabilidad del autor.

Ambato, enero de 2020

Jhonatan S. Escobar Meléndez

C.I: 180413833-5

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad.

Ambato, enero de 2020

Jhonatan S. Escobar Meléndez

C.I: 180413833-5

APROBACIÓN TRIBUNAL DE GRADO

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Mg. Carlos Núñez y el Ing. PhD. Félix Fernández, revisó y aprobó el Informe Final del trabajo de graduación titulado "SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LAS NORMAS ISO/IEC 27001 EN EL DATACENTER DE LA EMPRESA AMBACAR-AMBATO", presentado por el señor Jhonatan Sebastián Escobar Meléndez de acuerdo al numeral 9.1 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ing. Elsa Pilar Urrutia Mg.

PRESIDENTA ENCARGADA DEL TRIBUNAL

Ing. Carlos Núñez

DOCENTE CALIFICADOR

Ing. Félix Fernández

DOCENTE CALIFICADOR

DEDICATORIA

Dedico este trabajo de titulación a mis abuelitos Michita y Ernesto qué me formaron desde el día que nací y aunque no pude tener la dicha de en vida poderles brindar esta alegría espero que en donde estén se sientan orgullosos de este nuevo logro alcanzado que es más de ellos que mío.

También le dedico a mis padres Amparito y Efraín que siempre sin importar todo lo sucedido siempre me guiaron y ayudaron en mi vida. Los amo y gracias por todo.

Jhonatan Sebastián Escobar Meléndez

AGRADECIMIENTO

Agradezco a Dios en primer lugar por la oportunidad de seguir creciendo día a día y especialmente a mis padres y familiares que fueron mi apoyo y sustento para sacar adelante ahora mi profesión.

De manera especial quiero agradecer a mi enamorada la Ing. Daniela Aguas por su ayuda y consejos a lo largo de la carrera y al Ing. Andrés Vasco que me ayudo, guío y colaboró en el trabajo de titulación y muy aparte me ofreció su amistad.

Muchas gracias también a mi tutor el Ing. Dennis Chicaiza por los consejos y revisiones de mi trabajo de titulación para que salga de la mejor manera.

Jhonatan Sebastián Escobar Meléndez

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

AMBACAR es una empresa automotriz en la cual deben ejecutarse procedimientos ordenados para llegar al éxito deseado. El presente proyecto busca brindar seguridad a estos procesos a través de la implantación de un modelo de Gestión de Seguridad de la Información establecido bajo la Norma ISO/IEC 27001. Esta norma se compone de diversos dominios entre los cuales resaltan las políticas de seguridad, gestión de activos, control de acceso y seguridad física, cada uno de ellos con controles definidos.

La fase de análisis y evaluación del estado de la seguridad de AMBACAR se obtienen por medio de entrevistas, encuestas, análisis de vulnerabilidad, y observación directa a través de visitas frecuentes a la empresa.

Al determinar el estado actual de la empresa, se procede a realizar el análisis de aplicabilidad y cumplimiento de los controles establecidos en la ISO/IEC 27001, para definir políticas de seguridad adecuadas para la seguridad de la información.

Palabras clave: seguridad de la información, Norma ISO/IEC 27001, gestión de seguridad, políticas de seguridad, gestión de activos, control de acceso.

ABSTRACT

AMBACAR is an automotive company in which ordered procedures must be executed to achieve the desired success. This project seeks to provide security to these processes through the implementation of an Information Security Management model established under ISO / IEC 27001. This standard consists of several domains among which security policies, management of assets, access control, physical security each with defined controls.

The phase of analysis and evaluation of the state of safety of AMBACAR is obtained through interviews, surveys, vulnerability analysis, and direct observation through frequent visits to the company.

When determining the current status of the company, the analysis of applicability and compliance with the controls established in ISO / IEC 27001 is carried out, in order to define adequate security policies for information security.

Keywords: information security, ISO / IEC 27001, security management, security policies, asset management, access control.

INTRODUCCIÓN

La prioridad de mantener la seguridad de la información en la actualidad conjuntamente con un notable incremento de arremetidas a nivel organizacional podría causar afectaciones a nivel operacional de la empresa. Esto hace requerida la búsqueda de soluciones que contrarresten el impacto que pudiese generar dichas amenazas.

Dentro de AMBACAR se maneja una cantidad considerable de información muy relevante de cada uno de sus clientes por esta razón es de suma importancia y relevancia mantener la seguridad de la información para cada uno de los departamentos presentes en la empresa AMBACAR, teniendo en cuenta los aspectos a considerar para la seguridad de la información como: confidencialidad, integridad y disponibilidad; estos aspectos de la norma ISO/IEC 27001 son los que brindan una guía específica para proporcionar diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información.

CAPITULO 1

1. EL PROBLEMA

1.1. Tema

"SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LAS NORMAS ISO/IEC 27001 EN EL DATACENTER DE LA EMPRESA AMBACAR-AMBATO."

1.2. Planteamiento del problema

Debido a los enormes cambios sufridos por el mercado en los últimos años a nivel local y mundial, la incorporación de tecnologías informáticas facilita la administración de los datos en los entes públicos y privados lo cual ha empezado a darle gran importancia a la información y a los métodos para vulnerar sistemas con el fin de proteger la información de las mismas.

Esto ha dado lugar para que se puedan utilizar normas y políticas en las organizaciones para que gestionen la información de una manera óptima y adecuada con el fin de ofrecer mejoras en la toma de decisiones gerenciales

En la actualidad todas las empresas requieren de un Sistema de Gestión de Seguridad de la Información por lo cual es necesario realizar un análisis con las principales causas que puedan ocasionar pérdida de información. Por tanto, se considera de suma importancia las normas y estándares internacionales de seguridad de la información con el fin de garantizar los mecanismos de seguridad de un departamento informático [1].

En nuestro país la gestión de riesgos y la seguridad de la información es un área poco estudiada para lo cual los entes públicos y privados contextualizan a la información como un problema tecnológico lo cual están en un gran error ya que la información es el activo más valioso que tiene la empresa [2].

Dentro de AMBACAR se maneja una cantidad considerable de información muy relevante de cada uno de sus clientes por esta razón es de suma importancia y relevancia mantener la seguridad de la información para cada uno de los departamentos presentes en la empresa AMBACAR, teniendo en cuenta los aspectos a considerar para la seguridad de la información como: confidencialidad, integridad y disponibilidad; estos aspectos de la norma ISO/IEC 27001 son los que brindan una

guía específica para proporcionar diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información.

La empresa AMBACAR por el momento no cuenta con la implementación de ningún estándar para asegurar la información que poseen, con el fin de mejorar la productividad y el rendimiento de una organización competitiva, es fundamental evaluar las técnicas actuales y la tecnología disponible para desarrollar sistemas que brinden eficiencia y eficacia de la gestión de la información relevante.

1.3. Delimitación

1.3.1. Delimitación de contenidos

Área Académica: Administrativas Informáticas

Línea de Investigación: Administración de Recursos

Sublímela de Investigación: Desarrollo de Planes Informáticos

1.3.2. Delimitación espacial

Empresa AMBACAR - Ambato.

La investigación propuesta está delimitada para empresas que no posean un Sistema de Gestión de Seguridad de la Información, el objetivo de la investigación es mostrar las ventajas de tener un Sistema de Gestión de Seguridad de la Información en la empresa para poder ofrecer un servicio de calidad a sus clientes, mejorar los procesos tecnológicos de la empresa, mejorar los servicios de los empleados y evitar la pérdida de información que tienen las empresas.

1.3.3. Delimitación Temporal

La presente investigación se desarrollará en el periodo académico febrero 2019 - agosto 2019.

1.4. Justificación

La inseguridad que existe en las empresas en la actualidad es debido a varios factores que se han presentado en la actualidad en empresas que empiezan a expandirse sin dejar de por medio la tecnología, para esto se desea realizar una propuesta de

implementación de un Sistema de Gestión de Seguridad de Información que permitirá a la empresa “AMBACAR¨ definir de una manera estructurada las responsabilidades, procedimientos a seguir, procesos y métodos necesarios para evitar la pérdida de información y mejorar la eficiencia de la empresa.

El objetivo del proyecto es implementar un Sistema de Gestión de Seguridad de la Información adecuada que permita concebir y formalizar los métodos necesarios para lograr la seguridad informática óptima en esta organización, así como su seguimiento y establecimiento permanentes con la finalidad de aportar con la seguridad tanto para los usuarios, empleados y parte administrativa en todas las sucursales.

1.5.Objetivos

1.5.1. Objetivo General

Implementar una Gestión de Seguridad de la Información en el DataCenter de AMBACAR basado en las normas ISO/IEC 27001.

1.5.2. Objetivos Específicos

- Analizar la información del departamento de TI de la empresa AMBACAR para conocer la situación actual respecto a la seguridad de información y evaluar amenazas, vulnerabilidades más importantes para la empresa.
- Determinar la existencia de activos de información y equipos utilizados en la empresa AMBACAR.
- Seleccionar los objetivos de control considerados más importantes de la norma ISO/IEC 27001 con el fin de garantizar la seguridad de la información para la empresa AMBACAR.
- Planificar y crear el Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001.

CAPITULO 2

2. MARCO TEÓRICO

2.1. Antecedentes Investigativos

Como antecedentes se puede mencionar.

Según el trabajo de Terán Valenzuela Karina Maribel denominado "GUÍA PARA LA IMPLANTACIÓN DEL SGSI CON BASE EN LA NTE ISO/IEC 27000 PARA EL SERVICIO DE AGENDAMIENTO DE CITAS DEL CONTACT CENTER DEL MINISTERIO DE SALUD PÚBLICA DEL ECUADOR" menciona:

¨La implementación de un sistema de seguridad de la información constituye un objetivo estratégico en las organizaciones, consiguiendo una ventaja competitiva y beneficios como la mejora de la imagen corporativa y el cumplimiento del marco regulatorio y legal¨ [3].

Según el trabajo realizado por Casadiegos Santana Aura Lucia, Quintero Jiménez Lucero y Toro Rueda Mileidy denominado ¨SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL ÁREA DE CONTABILIDAD DE LA E.S.E. HOSPITAL LOCAL DE RIO DE ORO CESAR¨ menciona:

¨Un SGSI – Sistema de Gestión de Seguridad de la Información, el Área de Contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar conseguirá minimizar considerablemente el riesgo de que su productividad se vea afectada debido a la ocurrencia de un evento que comprometa la confidencialidad, disponibilidad e integridad de la información o de alguno de los sistemas informáticos. Este sistema permite identificar, gestionar y minimizar los riesgos reales y potenciales de la seguridad de la información, de una forma documentada, sistemática, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías¨ [4].

Según el trabajo realizado por Vallejo Cáceres Álvaro Alejandro denominado ¨PROPUESTA DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL CENTRO DE DATOS DE LA EMPRESA LETERAGO DEL ECUADOR S.A ¨ menciona:

¨El proyecto se basa en la elaboración de una propuesta de un Sistema de Gestión de Seguridad de la información para el Centro de Datos de la empresa Leterago del Ecuador S.A, utilizando las Normas ISO 27001 e ISO 27005 que permitieron identificar los riesgos existentes en los activos de información y la forma de mitigarlos, controles que utilizan en la organización para evitar riesgos con esta información se logró realizar las políticas de seguridad de la información y la propuesta de SGSI que permitirá a la organización disminuir los riegos a un nivel aceptable por lo tanto poder proteger las actividades que son esenciales en el giro del negocio¨ [5].

Según el trabajo realizado León León Luis Adrián por denominado¨ "PLANIFICACIÓN DE UN SGSI BASADO EN LA NORMA ISO 27001:2013 EN LA EMPRESA MAFELESA. ¨ menciona:

¨Se pudo realizar un análisis de la utilidad e importancia de contar con una planificación de un sistema de gestión de seguridad de la información en la Empresa Mafelesa, con el objetivo principal de contar con una empresa mejor preparada en el manejo, protección y seguridad de los activos utilizados dentro y fuera de la organización garantizando confiabilidad en el mercado¨ [6].

2.2. Fundamentación Teórica

En el desarrollo de este proyecto se han considerado fundamentalmente los siguientes aspectos conceptuales:

2.2.1. Seguridad de la Información

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones que permiten resguardar y proteger la información buscando mantener las dimensiones (confidencialidad, disponibilidad e integridad) de la misma.

Abarca todo tipo de información

- Impresa o escrita a mano
- Grabada con asistencia técnica
- Transmitida por correo electrónico o electrónicamente
- Incluida en un sitio web
- Mostrada en videos corporativos
- Mencionada durante las conversaciones [10]

2.2.2. Seguridad de la información vs seguridad informática

Antes de abordar un enfoque metodológico para implementar un SGSI es necesario aclarar la diferencia entre seguridad informática y seguridad de la información, la cual radica en el tipo de recursos sobre los que actúa cada una. Mientras que la primera se enfoca en la tecnología propiamente dicha, i.e. en las infraestructuras tecnológicas que sirven para la gestión de la información en una organización, la segunda está relacionada con la información en sí misma, como activo estratégico de la organización. En este sentido las TIC son herramientas que permiten optimizar los procesos de gestión de la información en las organizaciones. El concepto de seguridad es el mismo, pero mientras la seguridad informática desarrolla su función sobre todos los elementos técnicos que hacen parte de las TIC, la seguridad de la información actúa sobre la información como activo estratégico para la adecuada toma de decisiones empresariales en las organizaciones modernas.

Hasta antes que surgieran de forma masiva las TIC, el concepto predominante era el de seguridad de la información; sin embargo, con el advenimiento de las TIC y su nivel de dependencia por parte de las organizaciones y más aún, su nivel de dependencia para un adecuado tratamiento de la información, se ha pasado de pensar tan solo en la seguridad informática como fin, a pensar en su adecuada implementación como medio para obtener un SGSI que permita garantizar niveles adecuados de protección de la información empresarial como recurso vital para la función decisional, y el diseño de estrategias competitivas que diferencien una organización de otra. Desde esta perspectiva lo que persigue un SGSI es proteger la información como recurso valioso, para lo cual debe proteger de igual forma los diferentes medios a través de los cuales se genera, almacena, procesa, transmite, circula y transforma en un recurso útil para los negocios. Estos medios son las TIC en su conjunto [8].

2.2.3. Sistema de gestión de seguridad de la información (sgsi)

El SGSI consiste básicamente en un conjunto de políticas para definir, construir, desarrollar y mantener la seguridad del equipo basado en hardware y recursos de software (ISO/IEC 27001, 2005); estas políticas, muestran la manera en que los recursos del computador pueden ser utilizados.

Adicionalmente, el proceso de implantación de un SGSI opera a través de proceso de cinco etapas, establecimiento de políticas de seguridad de la información, alcance del Sistema de Gestión, control de riesgos, realización de medidas y control de seguimiento, bajo un modelo PHVA (Planear-Hacer-Verificar-Actuar). Es importante definir el enfoque que se tiene para la evaluación del estado de seguridad de información en una organización, de ahí la razón de definir un marco jerárquico para priorizar lo que se tiene. Además, que los procesos de los SGSI conllevan a dificultades tales como: falta de documentación, administración y organización de la misma, ausencia de roles y responsabilidades, para llevar a cabo las actividades pertinentes para dar cumplimiento a objetivos y alcances del SGSI.

En este orden de ideas, abordar el proceso de forma tradicional y, las dificultades evidenciadas en cuanto a la documentación que se genera durante este proceso, sugieren la necesidad de buscar una pronta solución, lo cual se constituye en el objetivo principal de este trabajo. Para alcanzar el objetivo mencionado anteriormente, se desarrolló un software que enmarca la consecución de los requerimientos y actividades que conforman la debida documentación del SGSI. Como principal resultado, se obtiene un módulo de gestión documental que permite ejercer un control de documentos y asignación de actividades para miembros del grupo de implantación del SGSI, que facilita la recepción, administración, mantenimiento y estado de la documentación obtenida en el desarrollo del mismo.

Los Sistemas de Gestión de la Seguridad de la Información bajo los requerimientos que exige la norma ISO 27001, constituyen la base para la gestión de la seguridad de la información; dicha norma, define un SGSI que garantiza el conocimiento, apropiación, gestión y disminución de riesgos de seguridad de la información para la organización, de forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a cambios que se produzcan en los riesgos, entorno y tecnologías. La implantación de un SGSI implica adaptarse a un nuevo paradigma definido como enfoque de gestión, desde la implementación de controles que figuran en la norma hasta incluir productos certificados, manteniendo la combinación inteligente de aspectos tales como las políticas, normas, directrices, códigos de la práctica, la tecnología, asuntos humanos, asuntos legales y éticos hacen parte de este nuevo enfoque. Para habilitar dicho enfoque, el proceso de seguridad comprende la seguridad

lógica y física de la organización, de esta forma establecer una estructura de seguridad a partir de canales de comunicación entre áreas de la organización, facilitando el cumplimiento de las políticas o normas de seguridad aplicables [7].

2.2.4. Estándares de seguridad de la información

Uno de los requisitos para implementar un SGSI en una organización es conocer los estándares, su estructura y la relación existente entre cada uno de ellos.

Las normas para implementar un SGSI corresponden a la serie ISO/IEC 27000 publicadas por la ISO y la Comisión Electrotécnica Internacional (IEC), compuesta por aproximadamente 17 normas, clasificadas en cuatro categorías: *i*) La norma que contiene el vocabulario, contenido en la norma ISO/IEC 27000; *ii*) las normas de requerimientos, contenidos en la norma ISO/IEC 27001 y la norma ISO/IEC 27006; *iii*) las normas guía desarrolladas a través de 10 normas: ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27007, TR 27008, ISO/IEC 27013, ISO/IEC 27014, TR 27016, ISO/IEC 27032 y *iv*) las normas para sectores específicos, contenidas en las normas ISO/IEC 27010, ISO/IEC 27011, TR 27015 y TS 27017.

A pesar de la cantidad de normas de la serie ISO/IEC 27000, aquéllas que sirven de referente para la implementación de un SGSI en una organización se enmarcan en cuatro de ellas, como se puede observar en la Figura: [8].

Fig. 1.- *Referente de las Principales Normas para Implementación de un SGSI basado en los estándares de la familia de normas ISO/IEC 27000 [8]*

Fuente: *RISTI - Revista Ibérica de Sistemas e Tecnologías de Información*

2.2.5. Norma ISO/IEC 27001:2017

Norma denominada formalmente Tecnología de información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requerimientos, la cual especifica los requerimientos para el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora de un SGSI debidamente formalizado. El cumplimiento de los requerimientos de esta norma, permite que una organización pueda obtener la certificación internacional en ISO/IEC 27001 [8].

Esta norma internacional se ha preparado para proporcionar los requisitos para el establecimiento, implementación mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información. La adopción de un sistema de gestión de la seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación de un sistema de gestión de la seguridad de la información por una organización está condicionado por sus necesidades y objetivos, sus requisitos de seguridad, los procesos organizativos utilizados y su tamaño y estructura. Lo previsible es que todos estos factores condicionantes cambien con el tiempo.

El sistema de gestión de la seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y otorga a las partes interesadas confianza sobre la adecuada gestión de los riesgos.

Es importante que el sistema de gestión de la seguridad de la información forme parte y esté integrado con los procesos de la organización y con la estructura de gestión global, y que la seguridad de la información se considere durante el diseño de procesos, de los sistemas de información y de los controles. Es de esperar que la implementación del sistema de gestión de la seguridad de la información se ajuste a las necesidades de la organización.

Esta norma internacional puede ser utilizada por partes internas y externas para evaluar la capacidad de la organización para cumplir con sus propios requisitos de seguridad.

El orden en que esta norma internacional presenta los requisitos no es reflejo de su importancia ni implica el orden en el cual deben implementarse [9].

CAPITULO 3

3. METODOLOGÍA

3.1. Modalidad de Investigación

Para la recolección, procesamiento y análisis de la información para el presente trabajo se realizará un trabajo conjunto con el personal y el departamento de TI (Tecnologías de la Información) de AMBACAR en donde se conocerá cada uno de los requerimientos e información adecuada para considerar las necesidades por parte de la empresa para la seguridad de la información.

Además, para extraer información precisa y adecuada se tomará en cuenta información relacionada con revistas científicas, libros, documentos e internet que sea relacionado con el tema.

3.2. Población y Muestra

Se detallan a continuación las definiciones de población y muestra, en la intervención de la investigación planteada.

3.2.1. Población

Debido a las características del proyecto de investigación se presenta población al personal de la empresa AMBACAR - Ambato en donde se va trabajar en el presente proyecto de investigación.

3.2.2. Muestra

La muestra para la investigación en sí se lo tomará directamente de los empleados del departamento de sistemas en donde se maneja la información existente de la empresa y en donde se encuentra el DataCenter al que se va a realizar el estudio.

3.3. Recolección de la Información

Para la recolección, procesamiento y análisis de la información para el presente trabajo se realizará un trabajo conjunto con el personal y el departamento de TI (Tecnologías de la Información) de AMBACAR en donde se conocerá cada uno de los requerimientos e información adecuada para considerar las necesidades por parte de la empresa para la seguridad de la información.

Además, para extraer información precisa y adecuada se tomará en cuenta información relacionada con revistas científicas, libros, documentos e internet que sea relacionado con el tema.

3.4. Procesamiento y análisis de datos

Para el procesamiento y análisis se recolectó y recopiló información del tema planteado para validar la información, esto se lo realizó mediante documentos y normas presentes en la empresa AMBACAR Ambato.

Otra de las tareas realizadas fue la obtención de información tomada a través de la norma ISO/IEC 27001 con el fin de realizar el plan estratégico para el proyecto a desarrollar.

3.5. Desarrollo del Proyecto

Analizar la información del departamento de TI de la empresa AMBACAR para conocer la situación actual respecto a la seguridad de información y evaluar amenazas, vulnerabilidades más importantes para la empresa.

- Recolección de información a través de encuestas o entrevistas al personal de la empresa.
- Analizar de la información recolectada.
- Analizar el estado actual de seguridad de la empresa.
- Determinar políticas de seguridad para la empresa.

Determinar la existencia de activos de información y equipos utilizados en la empresa AMBACAR.

- Identificar las áreas y departamentos de la empresa.

Seleccionar los objetivos de control considerados más importantes de la norma ISO/IEC 27001 con el fin de garantizar la seguridad de la información para la empresa AMBACAR.

- Investigar acerca del estándar ISO/IEC 27001 para su uso adecuado.

Planificar y crear el Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001.

- Elaborar el Sistema de Gestión de Seguridad Informática para la identificación y localización de datos importantes para la empresa y así como la verificación de las amenazas a las que pueden ser víctimas.

- Implementar el Sistema de Gestión de Seguridad Informática para el control y seguridad de la información de la empresa.

CAPITULO 4

4. DESARROLLO DE LA PROPUESTA

Una vez realizado el estudio de acuerdo a los objetivos, para alcanzar la implementación del sistema de gestión de riesgos (SGSI) hay que tener en claro que al mencionar la palabra ¨SISTEMA¨ según el diccionario académico de la real academia de la lengua no se hace referencia solo a un conjunto de aplicaciones o programas informáticos, la palabra ¨SISTEMA¨ también se la hace referencia a un conjunto ordenado de normas y procedimientos qué regulan el funcionamiento de un grupo o colectividad, dicho conjunto de reglas, principios o medidas que tienen relación entre sí con el fin de llegar a un objetivo en específico.

Esclarecida esta definición, se acogerá el ciclo de mejora continua (PDCA) debido a sus fases:

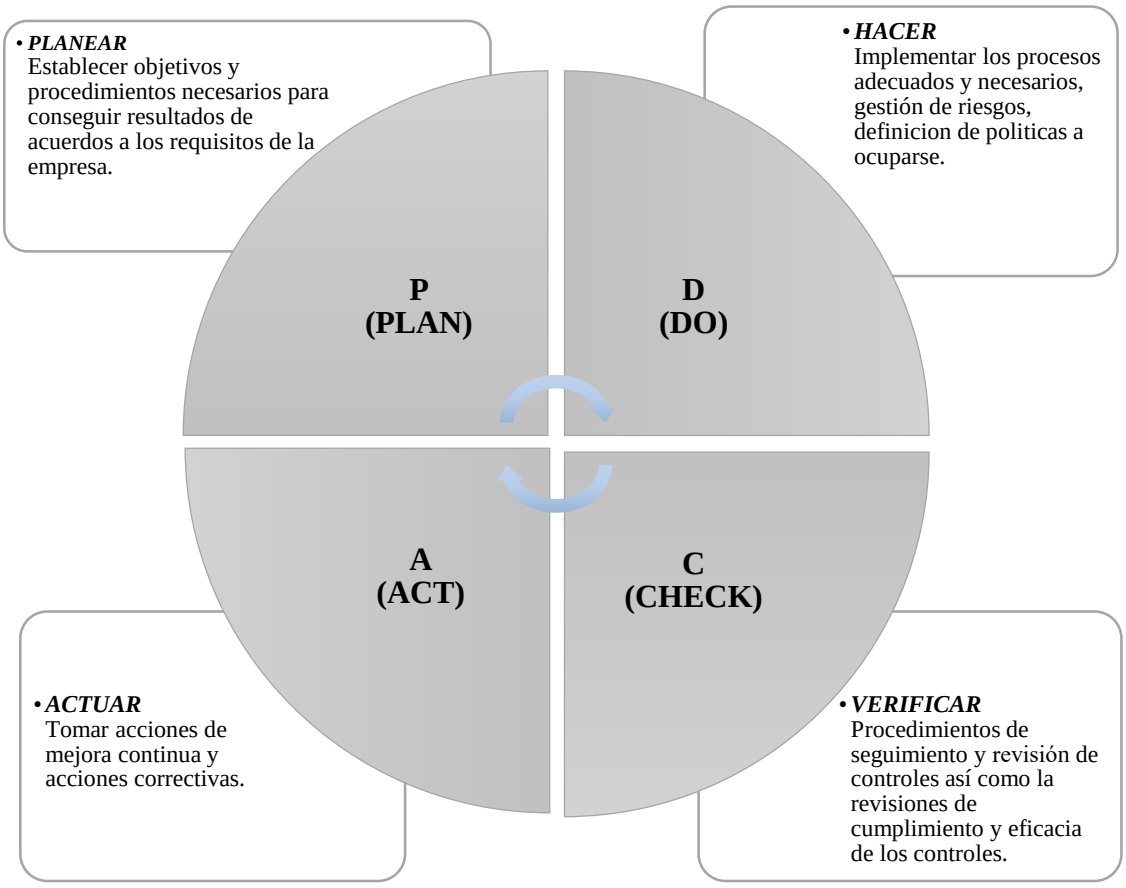


Fig. 2.- *Metodología de aplicación – ciclo de Deming*

Elaborado por: Investigador

4.1. Planeación

La planeación aplicada en el desarrollo de la propuesta del presente proyecto consta de los siguientes aspectos:

4.1.1. Análisis de la situación actual

Para el desarrollo de la investigación se inició con una entrevista en el departamento de Sistemas al Ing. Byron Jiménez encargado del manejo y control del DataCenter, esta entrevista fue con el fin de recolectar datos para tener en claro un punto de partida para la investigación.

Esta entrevista no solo tuvo el objetivo de tener un punto de partida de la investigación, también ayudó para redactar de manera concisa y entendible una encuesta que se realizó a los miembros del departamento de sistemas los cuales son los responsables de mantener los sistemas adecuadamente de toda la empresa. Mediante esta entrevista y encuesta se recolectó los datos pertinentes comprobando que la empresa no se rige a un plan de gestión de riesgos de seguridad para el manejo y uso de la información.

Tabla de Preguntas de la Entrevista

Tabla 1.- *Tabla de preguntas de la entrevista*

Elaborado por: *Investigador*

Preguntas	**Respuesta**
1.- ¿Posee la empresa, políticas de seguridad de la información?	Sí, si poseemos políticas de seguridad, pero no son políticas actualizadas.
2.- ¿Qué tipos de políticas de seguridad tienen implementadas? (Detalle mediante una lista)	La empresa tiene políticas de: • Seguridad Perimetral • Bloqueo de puertos USB
3. ¿Se ha realizado un monitoreo de las políticas de seguridad informática que tienen en la actualidad? (En caso de hacer el monitoreo explique cómo se lo realiza.)	No, no hemos realizado ningún tipo de monitoreo de las políticas que tenemos actualmente.
4. ¿Las políticas de seguridad que poseen, creen que son adecuadas y suficientes para la seguridad de la información?	Adecuadas sí, pero suficientes no.
5.- ¿Existen definidas las responsabilidades para el manejo de recursos de seguridad informática?	No, no tenemos definidas responsabilidades para el manejo de recursos de seguridad informática.

6.- ¿Se realizan simulacros de caídas de los sistemas que manejan? (En Caso de sí realizar los simulacros explique cómo los realizan.)	Sí, se realizan simulacros de caídas de seguridad perimetral.
7.- ¿Los simulacros que se realizan han ayudado al mejoramiento de la seguridad y control ante perdida de información? (Explique de qué manera ayudaron a mejorar la seguridad)	Permite alta disponibilidad en el equipo de seguridad perimetral. Tomando en cuenta que la seguridad perimetral es la integración de elementos y sistemas para la protección física, detección de intrusos en instalaciones específicas.
8. ¿Cuentan con un inventario de activos informáticos actualizados para la empresa?	Sí

4.1.2. Evaluación de la entrevista referente a la seguridad de la información

La entrevista realizada al encargado del uso y manejo de la gestión de la información Ing. Byron Jiménez afirma lo siguiente:

- La empresa sí posee políticas de seguridad, pero no son políticas actualizadas, es decir que no se ha cambiado ya en algunos años y siguen siendo las mismas lo cual no garantiza que la información está segura.
- Las políticas de seguridad que más se manejan es por medio de seguridad perimetral y bloqueo de puertos que hasta cierto punto es una seguridad básica y limitada para asegurar la información que se maneja.
- Las políticas de seguridad que poseen son adecuadas, pero no son suficientes para abarcar todo el procedimiento de seguridad de la información. Por tanto, se realizan simulacros de caídas de seguridad perimetral.
- No se tienen definidas responsabilidad para el manejo de recursos de seguridad de la información.

Tabla de Preguntas, Encuesta departamento de Sistemas

Tabla 2.- *Tabla de preguntas, encueta departamento de sistemas*

Elaborado por: *Investigador*

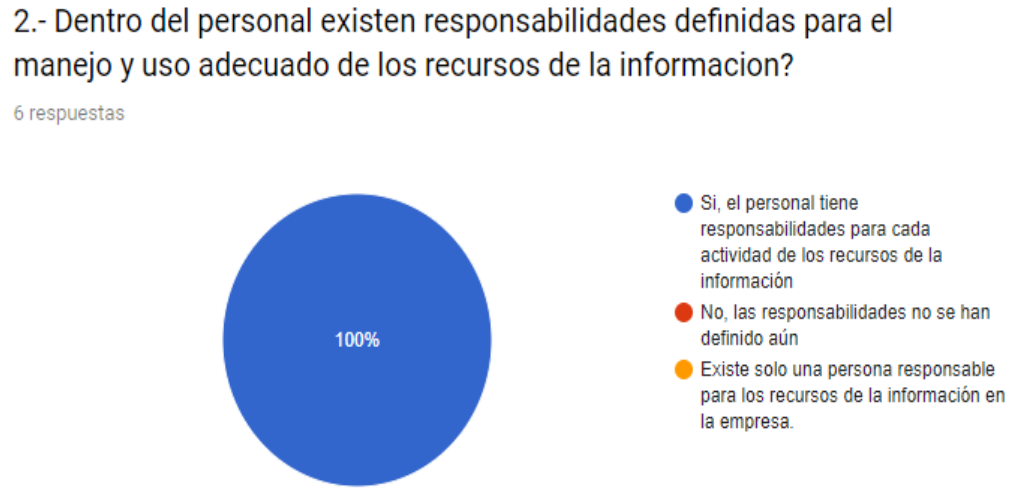
Preguntas	**Respuestas**
1.- ¿La empresa en la actualidad cuenta con políticas de seguridad para gestionar la información?	• Si • No
2.- ¿Dentro del personal existen responsabilidades definidas para el manejo y uso adecuado de los recursos de la información?	• Si, el personal tiene responsabilidades para cada actividad de los recursos de la información • No, las responsabilidades no se han definido aún • Existe solo una persona responsable para los recursos de la información en la empresa.
3.- ¿Periódicamente cada qué tiempo se realiza un mantenimiento de los instrumentos tecnológicos de la empresa?	• 1 vez al mes • De 2 a 4 veces cada 6 meses • Anualmente • No se ha realizado un mantenimiento
4.- ¿En los sistemas de información manejados por la empresa se los mantiene en constante monitoreo para un respectivo control?	• Si, si se los monitorea frecuentemente (Al menos una vez al mes) • No, no tienen un monitoreo • El monitoreo se lo realiza rara vez al año (1 a 3 veces)
5.- ¿Existe control para el personal no autorizado para el manejo de información que posee la empresa?	• Si, solo el personal autorizado tiene acceso a equipos o programas predeterminados • No, cualquier persona del departamento de tecnología tiene acceso autorizado • Tiene acceso solo personal administrativo de la empresa.
6.- ¿En la actualidad la empresa posee mecanismos de gestión de riesgos para la seguridad de la información?	• Si posee mecanismos de gestión de riesgos • No posee con ningún mecanismo de gestión de riesgos

7.- ¿Qué técnica de seguridad se aplica para el cuidado y uso de la información?	• Control de usuario • Firewall • NAT • Otros
8.- ¿Se realiza simulacros en los sistemas de información en los departamentos de la empresa?	• Sí • Rara vez • No, no existe un plan de contingencia para estos casos
9.- ¿La empresa posee un inventario de activos informáticos existentes y en uso?	• Si, si posee con un inventario actualizado • No, no posee un inventario actualizado • Nunca se a realizado un inventario de ese tipo
10.- ¿El personal o responsable de la información del departamento de Tecnología se encuentra capacitado ante una pérdida o caída de los sistemas de información?	• Si, si se encuentra capacitado • No, no se encuentra capacitado • No se tiene un responsable para estos casos
11.- ¿Se ha dado a conocer a los usuarios de los distintos departamentos alguna política de seguridad de la información, incluyendo beneficios y riesgos que puede ocurrir?	• Si conocen de las políticas • No saben la existencia de las políticas que maneja la empresa
12.- ¿La gerencia está seguro de que los departamentos comprenden de la importancia de la seguridad de la información?	• Si • No • Nunca se ha tratado de este tema en los departamentos.
13.- ¿El personal de los distintos departamentos se aseguran de proteger los equipos desatendidos? (¿Ej. bloqueando o cerrando la sesión?	• Si • No
14.- ¿Las copias se seguridad se realizan regularmente de acuerdo con una política de backup establecida?	• Si, se realizan backups según políticas • No, no se realizan bakups de ningún tipo • No, solo se realizan backups sin políticas establecidas

15.- ¿Existe un proceso formal para la gestión de las vulnerabilidades técnicas de los sistemas en uso?	• Si, si se realiza procesos de vulnerabilidades técnicas • No, no se realiza ningún proceso de este tipo.

4.1.3. Tabulación y análisis de la encuesta

Según el cuestionamiento planteado, la empresa AMBACAR no cuenta con políticas de seguridad de la información con un 83.3 % de confirmación de este resultado.



Según el cuestionamiento planteado al personal del departamento de sistemas se manifiesta una confirmación del 100 % de existencia de responsabilidades definidas para el manejo y uso de los recursos de la información; sin embargo,

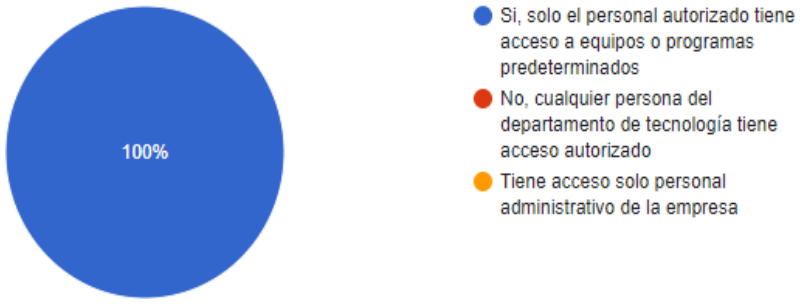
con la respuesta anterior existe una contradicción, por tanto, al analizar los procesos se evidencia la carencia de responsabilidades definidas.

Según el cuestionamiento planteado al personal del departamento de sistemas se evidencia un mantenimiento en periodos de tiempo muy lejanos, ya sea de forma semestral o anual.

Según el cuestionamiento planteado al personal del departamento de sistemas se evidencia que en la empresa AMBACAR se realiza un proceso de monitoreo periódico mensual de los sistemas de información.

5.- Existe control para el personal no autorizado para el manejo de información que posee la empresa?

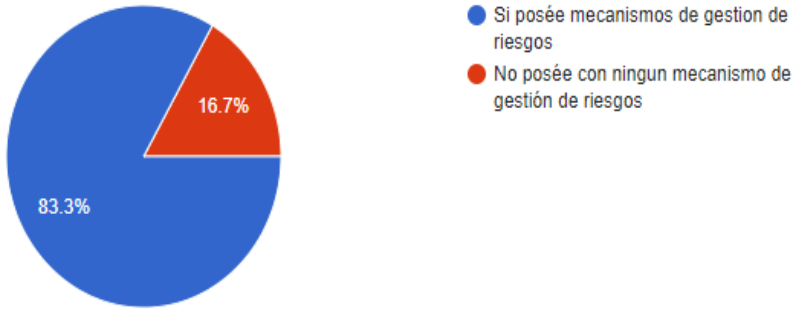
6 respuestas



Según el cuestionamiento planteado al personal del departamento de sistemas se evidencia que en la empresa AMBACAR se realiza un proceso de control de acceso a equipos o programas predeterminados; sin embargo, al no contar con políticas de gestión de seguridad de la información, se puede visualizar que los procesos de control de acceso son mínimos en comparación a las respuestas obtenidas en la encuesta.

6.- En la actualidad la empresa posée mecanismos de gestión de riesgos para la seguridad de la información?

6 respuestas



Según el cuestionamiento planteado al personal del departamento de sistemas se evidencia que en la empresa AMBACAR posee mecanismos de gestión de riesgos; frente a esto, la realidad arroja muestras de que el mecanismo de gestión de riesgos es mínimo comparado a las respuestas obtenidas.

7.- Qué tecnica de seguridad se aplica para el cuidado y uso de la información?

6 respuestas

Según el cuestionamiento planteado al personal del departamento de sistemas y luego del análisis realizado se evidencia que en la empresa AMBACAR cumple con la técnica de seguridad para el cuidado y uso de la información.

8.- Se realíza simulacros en los sistemas de información en los departamentos de la empresa?

6 respuestas

Según el cuestionamiento planteado al personal del departamento de sistemas se evidencia la carencia de simulacros en los sistemas de información de la empresa.

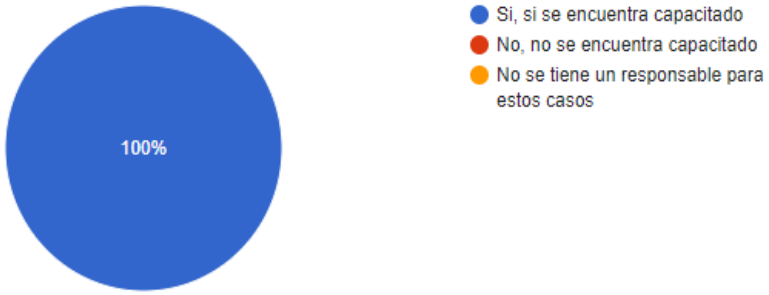
9.- La empresa posée un inventario de activos informáticos existentes y en uso?

6 respuestas

Según el cuestionamiento planteado al personal del departamento de sistemas se evidencia que en la empresa AMBACAR posee un inventario de activos informáticos existentes y en uso de los mismos, Se pone a consideración que el inventario de activos informáticos se encuentra en constante actualización.

10.- El personal o responsable de la información del departamento de Tecnologia se encuentra capacitado ante una perdida o caida de los sistemas de información?

6 respuestas



Según el cuestionamiento planteado al personal del departamento de sistemas se evidencia que en la empresa AMBACAR posee personal capacitado ante una pérdida o caída de los sistemas de información; sin embargo, se debe tener en cuenta que no se puede cubrir en su totalidad la mitigación de amenazas y vulnerabilidades de la información.

11.- Se ha dado a conocer a los usuarios de los distintos departamentos alguna política de seguridad de la información, incluyendo beneficios y riesgos que puede ocurrir?

6 respuestas

Según el cuestionamiento planteado al personal del departamento de sistemas se evidencia que en la empresa AMBACAR ha socializado las políticas de seguridad de la información al personal de los distintos departamentos. Pese a ello, se contrasta negativamente ya que la empresa no posee políticas de seguridad de la información

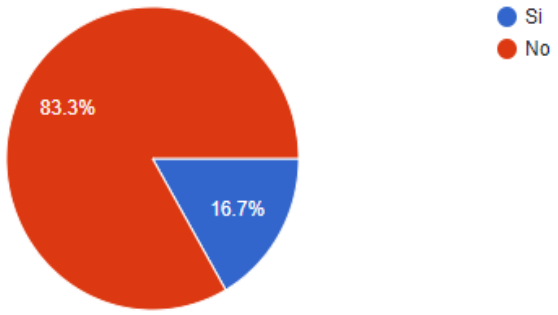
12.- La gerencia está seguro que los departamentos comprenden de la importancia de la seguridad de la información ?

6 respuestas

Según el cuestionamiento planteado se evidencia que la gerencia de la empresa AMBACAR comprende la importancia de la seguridad de la información, sin embargo, la mitad del personal del departamento de sistemas manifiesta desconocimiento de este tema dentro del departamento.

13.- El personal de los distintos departamentos se aseguran de proteger los equipos desatendidos? (Ej. bloqueando o cerrando la sesión?

6 respuestas



Según el cuestionamiento planteado se evidencia que el personal de los distintos departamentos no se asegura de la protección de los equipos desatendidos en la empresa. Por ello, luego del análisis del proyecto de investigación se debería realizar socializaciones e inducciones sobre los protocolos de protección para dichos equipos.

14.- Las copias se seguridad se realizan regularmente de acuerdo con una política de backup establecida?

6 respuestas

Según el cuestionamiento planteado se evidencia la realización de backups únicamente por proteger la información, proceso que se lleva a cabo sin el seguimiento de las políticas de seguridad de la información debido a que la empresa no dispone de las mismas.

Según el cuestionamiento planteado se evidencia la existencia de un proceso formal de gestión de la vulnerabilidad técnica de los sistemas de uso en un 66.7%: Luego del análisis realizado se puede establecer la carencia de este proceso formal, por tanto, se debería realizar lo antes mencionado una vez establecidas las políticas de seguridad de la información.

4.1.4. Evaluación de la encuesta referente a la seguridad de la información

La encuesta realizada a empleados del departamento de sistemas afirma lo siguiente:

- No se maneja un documento formal donde especifique las funciones y responsabilidades para el manejo y recursos de la seguridad de la información en el departamento de tecnología lo cual no es aconsejable debido a que se puede filtrar información o datos importantes para la empresa.
- Se realiza cada cierto tiempo simulacros de caídas de seguridad de la información teniendo en cuanta las políticas que manejan donde son simulacros adecuados, pero no suficientes debido a que falta un plan de contingencia ante este tipo de eventualidades.
- Contar con un inventario de activos permite mantener una alta seguridad de los equipos.

4.1.5. Áreas y departamentos de la empresa

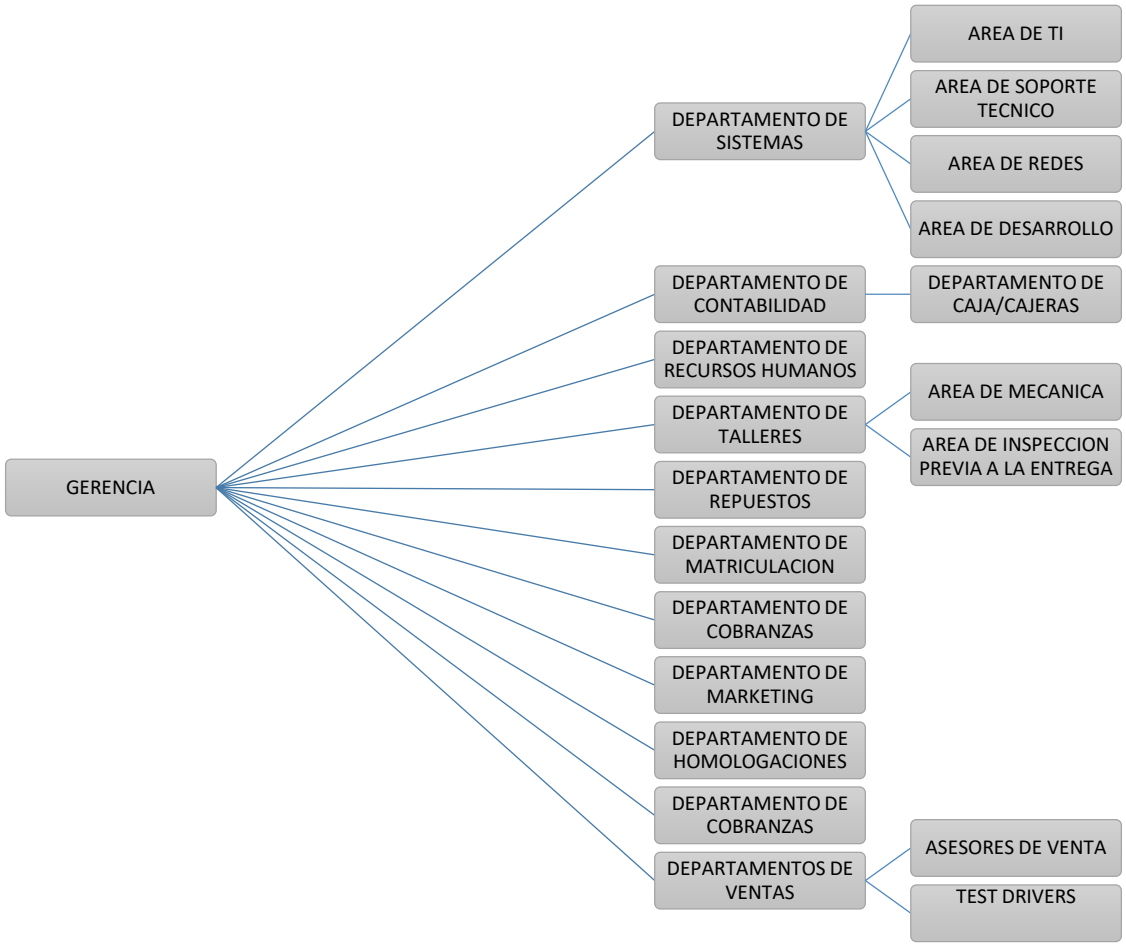


Fig. 3.- *Departamentos de la empresa*

Elaborado por: *Investigador*

4.1.6. Activos del DataCenter

Tabla 3.- *Activos del DataCenter*

Elaborado por: *investigador*

AMBACAR							
SERVIDOR	**CANTIDAD**	**UBICACIÓN**	**ACTIVO**	**USABILIDAD**	**PAIS DE USO**	**CARACTERISTICAS**	**TAMAÑO/CAPACIDAD**
1	1	MATRIZ	SERVIDOR	BASE DE DATOS SISTEMAS	ECUADOR	INTEL DL380P GEN-8 SN: 2M221901KJ INTEL XEON 6 CORE E5-2630 (2.3 GHZ) SN:	16 GB
2	1	MATRIZ	SERVIDOR	APLICACIÓN SISTEMAS	ECUADOR	SERVIDOR HP PROLIANT DL320e Gen8v2 32 GB RAM HP PCL3-12800E DDR3 SN: FM17A3005DZ-DV-E5-E4	32 GB
3	1	MATRIZ	SERVIDOR	BASE DE DATOS SISTEMAS	PERU	HP PROLIANT DL180 GEN9V3 +DISCO 3TB 6G SATA+FUENTE PODER 900W INTEL XEON E5-2609 6 CORE 1.90GHZ 15MB/85W sN: 2M262804JR 24 RAM HP 1X8GB SINGLE RANK X4 PC4 SN: KVR62201Y5-R7-YK	24 GB
4	1	MATRIZ	SERVIDOR	APLICACIÓN SISTEMAS	PERU	SERVIDOR HP PROLIANT DL160 GEN9V4 + FUENTE PODER 900W +DISCO 3TB 6G SATA INTEL XEON E5-2609V4 8-CORE, 1,70GHZ 20MB,8GB SN: 2M262105C9 24 RAM HPE PC4-2400T-R KIT SN: 2CV628049V,8J-6X	24 GB
5	1	MATRIZ	SERVIDOR	ANTIVIRUS	TODOS	LG MONITOR LCD 18,5"	

						INTEL DH61WW INTEL CORE I3 2100 3.1GHZ KINGSTON 2GB RAM DDR3	
6	1	UNAMUNCHO	SERVIDOR	BASE DE DATOS SISTEMAS	COLOMBIA	5 HPE 600 GB SAS DICO DURO (3 TB) HPE PROLIANT DL380 GEN10 2X INTEL XEON-G 5118 2X HPE 12 CORE 2.30 GHZ 16.5MB 64 GB (2X32GB) 2666MHZ RDIMM	64 GB
7	1	UNAMUNCHO	SERVIDOR	APLICACIÓN SISTEMAS	COLOMBIA	HP PROLIANT DL360 G10MATROX G200eH2 / XEON -S4114 10-CORE 2.20GHZ 13.75MB L3 CACHÉ HPE 2RX4 PC4-2666V-R 96GB RAM	96 GB

4.2. Identificación de vulnerabilidades

Por medio de la herramienta Maltego y tras la exploración del dominio **ambacar.com y ambacar.ec** se determinaron las relaciones existentes con las que cuenta este dominio.

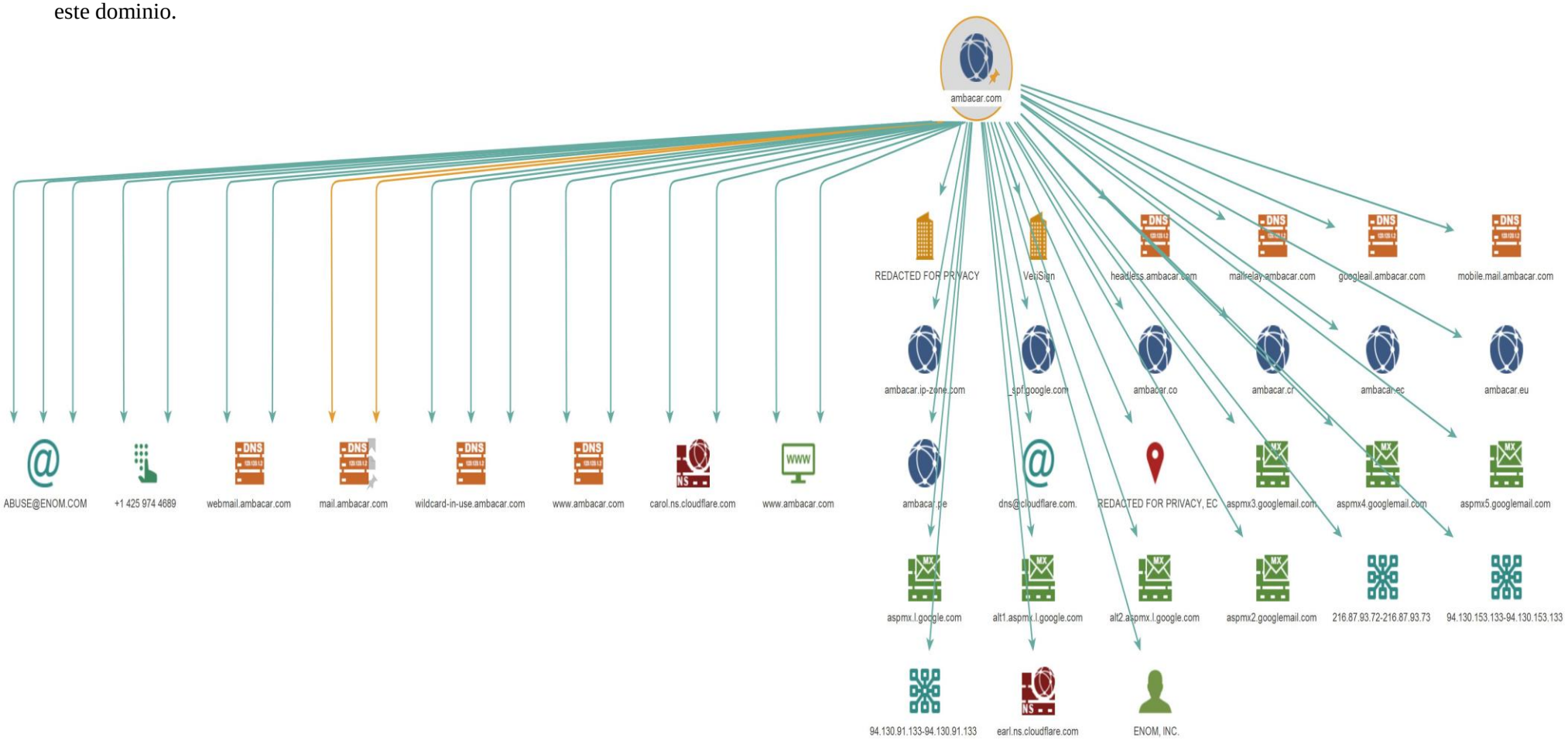


Fig. 4.- *Maltego, transformación en torno al dominio ambacar.com*

Elaborado por: *Investigador*

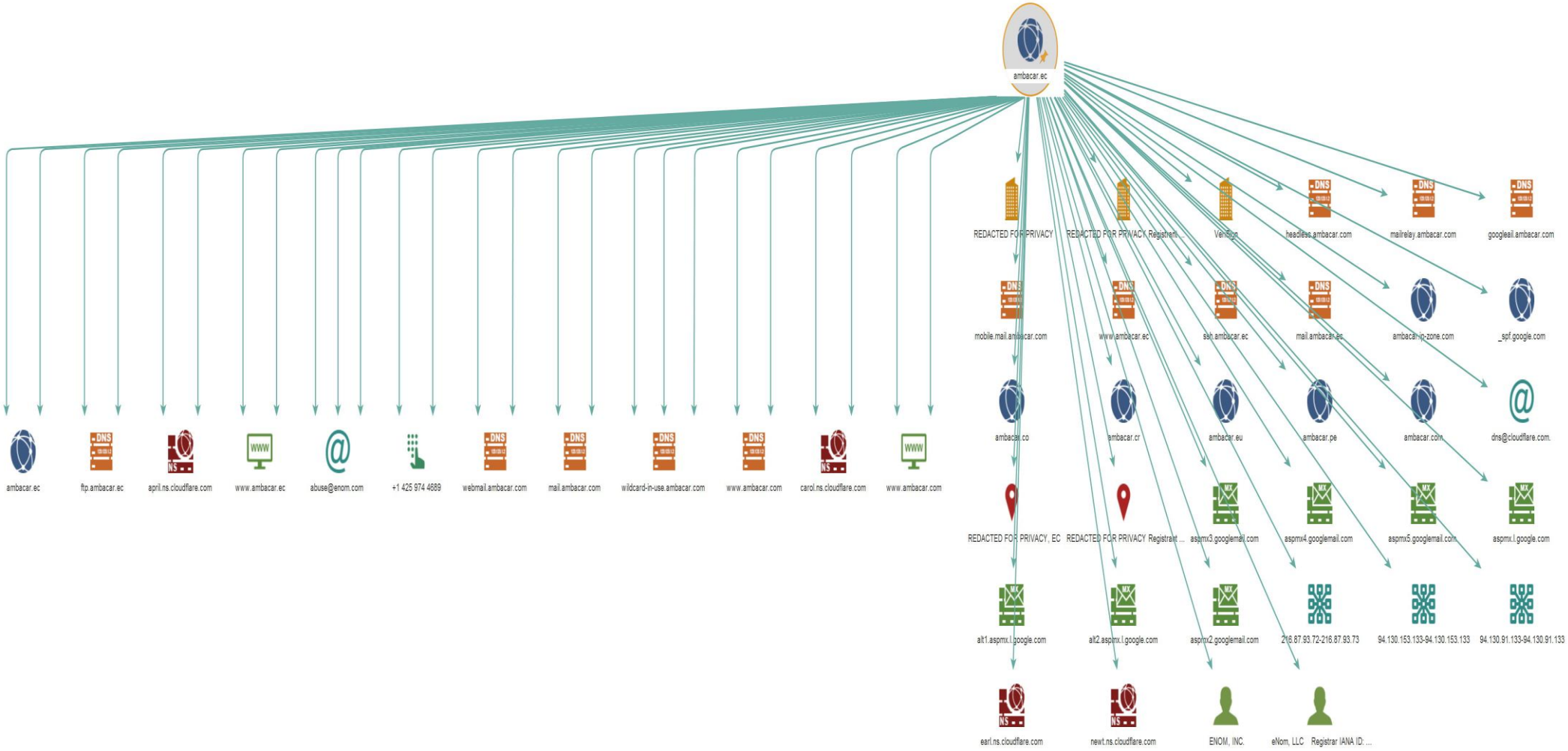


Fig. 5.- *Maltego, transformación en torno al dominio ambacar.ec*

Elaborado por: *Investigador*

Como se puede observar en las figuras 4 y 5, mediante la herramienta Maltego se aprecia NS RECORD, MX RECORD, DNS FROM DOMAIN, así también como se muestra varios dominios en común aplicado a un objeto de tipo DOMAIN (ambacar.com y ambacar.ec). Los resultados muestran servidores de correo, servidores DNS y servidores relacionados, así como una IP que se procede a analizar. También podemos visualizar el cloudfire el encargado de la protección de dominios de internet contra ataques de denegación de servicios.

El análisis se lo realizó con la herramienta TheHarvester, esta procederá a extraer información relacionada a los dominios en cuestión.

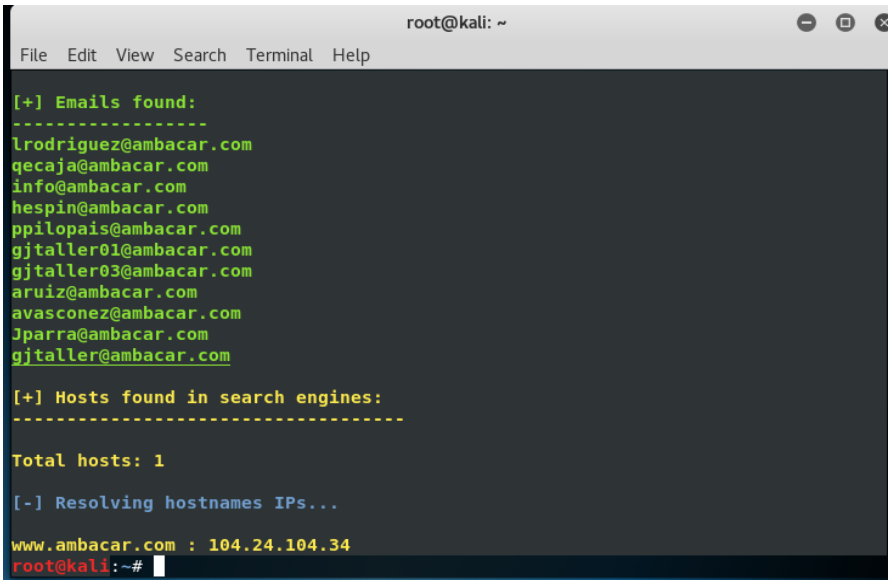


Fig. 6.- *The Harvester a dominio Ambacar.com*

Elaborado por: *Investigador*

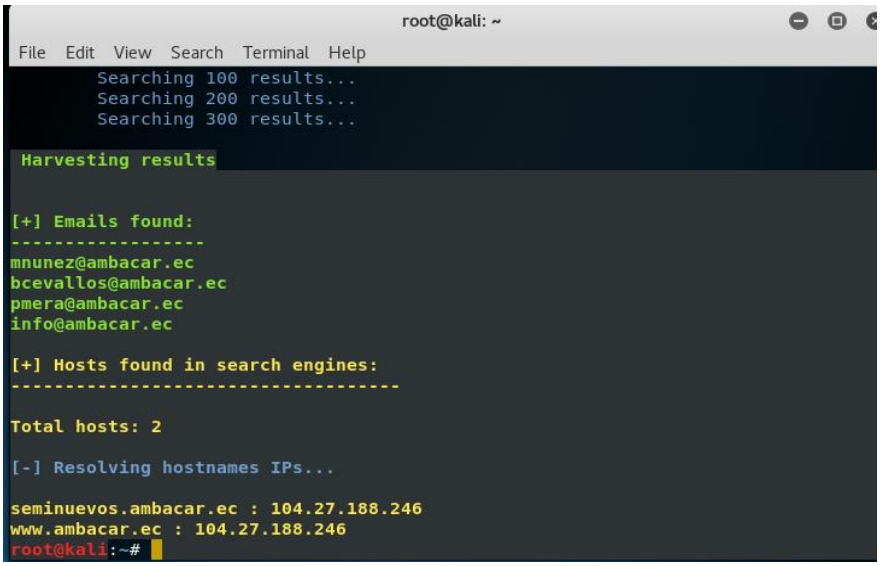


Fig. 7.- *The Harvester a dominio ambacar.ec*

Elaborado por: *Investigador*

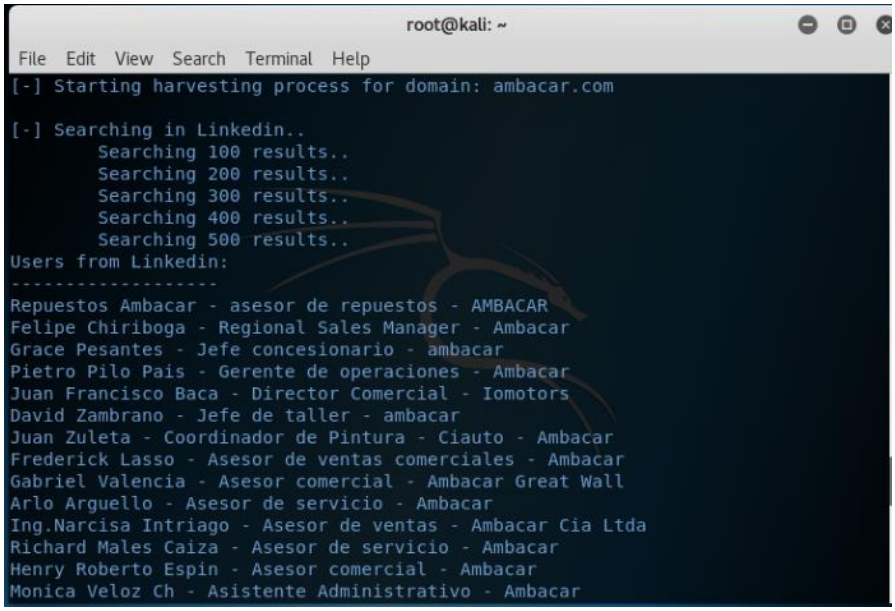


Fig. 8.- *The Harvester a dominio ambacar.com con linkedin*

Elaborado por: *Investigador*

Una vez realizado el análisis con la herramienta The Harvester se obtuvo varios correos electrónicos y algunos hosts relacionados a los dominios como se muestra en las figuras 6 y 7, además de las IPs que maneja ese dominio; así también se recolectó información de empleados y parte administrativa de la empresa como se muestra en la figura 8, teniendo en cuenta que no se visualizan todos los datos extraídos por la herramienta debido a la seguridad que desea mantener la empresa, con lo que se firmó una carta de confidencialidad para el uso de la información.

Resultados obtenidos con Maltego:

Tabla 4.- *Listado de servidores relacionados a los dominios*

Elaborado por: *Investigador*

DNS Name	
Nombre	**IP**
www.ambacar.com	104.24.104.34
googleail.ambacar.com	144.217.184.198
headless.ambacar.com	94.130.120.125
mail.ambacar.com	172.217.3.83
mailrelay.ambacar.com	93.159.210.2
webmail.ambacar.com	144.217.184.198
wildcard-in-use.ambacar.com	144.217.184.198
ftp.ambacar.ec	94.130.91.133
ssh.ambacar.ec	94.130.91.133

Domain	
Nombre	**IP**
seminuevos.ambacar.ec	104.27.108.246
ambacar.ec	104.27.189.246
ambacar.co	104.27.142.242
ambacar.cr	104.31.94.167
ambacar.ip-zone.com	93.159.210.2
ambacar.pe	104.27.180.193
ambacar.com	104.24.104.34
Mx Records	
Nombre	**IP**
alt1.aspmx.l.google.com	209.85.202.27
alt2.aspmx.l.google.com	64.233.184.26
aspmx.l.google.com	172.217.204.26
aspmx2.googlemail.com	209.85.202.27
aspmx3.googlemail.com	64.233.184.26
aspmx4.googlemail.com	172.217.218.27
aspmx5.googlemail.com	209.85.233.27
NS Records	
Nombre	**IP**
carol.ns.cloudflare.com	173.245.58.80
earl.ns.cloudflare.com	173.245.59.161
april.ns.cloudflare.com	173.245.58.66
newt.ns.cloudflare.com	173.245.59.212

Sondeo de Red

El sondeo de la red se la realizó mediante las IP proporcionadas directamente por la persona encargada el Ing. Byron Jiménez con el fin de detallar cada aspecto relevante de la auditoría. Hay que aclarar que para realizar el proceso de auditoría no se tuvo acceso a toda la información relevante de la empresa.

Por lo cual la auditoría solo se centralizó en los dominios (AMBACAR.com y AMBACAR.ec), y en los servidores mencionados en la Tabla 5. Se debe tomar en consideración que los servicios PHP del sistema principal no puede ser vulnerado de acuerdo al documento de confidencialidad para el manejo de información firmado con la empresa. Debido también, a que el sistema principal de la empresa es contratado a un agente externo que no permite realizar este tipo de actividades.

Listado de Servidores de AMBACAR

Tabla 5.- *Listado de Servidores a auditar*

Elaborado por: *Investigador*

N°	Dirección	Nombre	Sistema Operativo
1	192.168.3.16	Servidor base de datos	Oracle Linux 7.3
2	192.168.3.17	Servidor base de datos	Oracle Linux 7.3
3	192.168.3.15	Servidor de aplicaciones	Windows Server 2008
4	192.168.3.95	Servidor inventario Vehiculos	Windows Server 2008
5	192.168.3.46	Servidor de antivirus	Windows Server 2012 r2
6	192.168.35.10	Servidor de archivos	Windows Server 2012 r2
7	192.168.3.18	Servidor de aplicaciones	Windows Server 2008

4.2.3. Identificación de Servicios y Sistemas

Se realizó un sondeo en los puertos para encontrar los servicios que se estén ejecutando.

Para el análisis y sondeo de puertos la opción escogida es Nmap en Kali Linux dando los siguientes resultados.

Servidor BASE DE DATOS ORACLE LINUX 7.3

Tabla 6.- *NMAP a servidor base de datos oracle linux 7.3*

Elaborado por: *Investigador*

Puerto	Protocolo	Estado	Servicio	Detalle
22	tcp	abierto	ssh	OpenSSH 6.6.1 (Protocol 2.0)
1521	tcp	abierto	Oracle-tns	Oracle TNS listener 12.1.0.2.0 (unauthorizer)
5500	tcp	abierto	Ssl/http	Oracle XML DB Enterprise Edition httpd

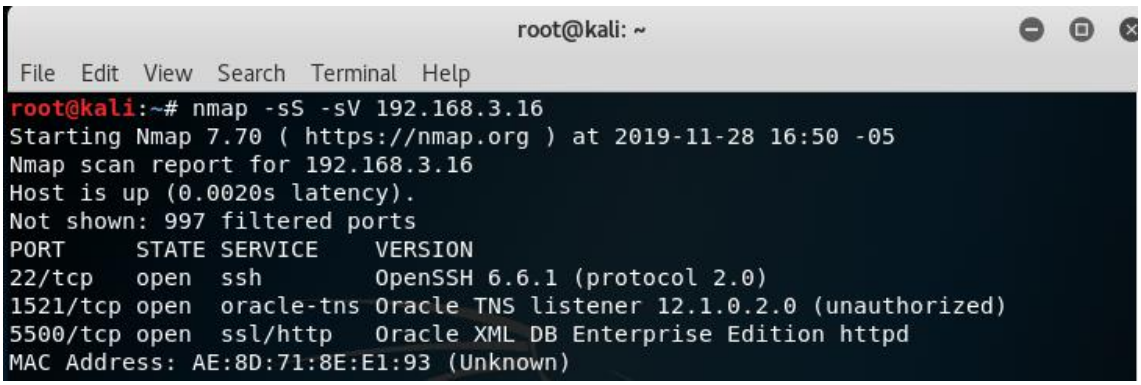


Fig. 9.- *Sondeo de puertos con NMAP Ip 192.168.3.16*

Elaborado por: *Investigador*

Servidor BASE DE DATOS ORACLE LINUX 7.3

Tabla 7.- *NMAP a servidor base de datos oracle linux 7.3*

Elaborado por: *Investigador*

Puerto	Protocolo	Estado	Servicio	Detalle
22	Tcp	abierto	ssh	OpenSSH 6.6.1 (Protocol 2.0)
1521	Tcp	abierto	Oracle-tns	Oracle TNS listener 12.1.0.2.0 (unauthorizer)
5500	tcp	abierto	Ssl/http	Oracle XML DB Enterprise Edition httpd

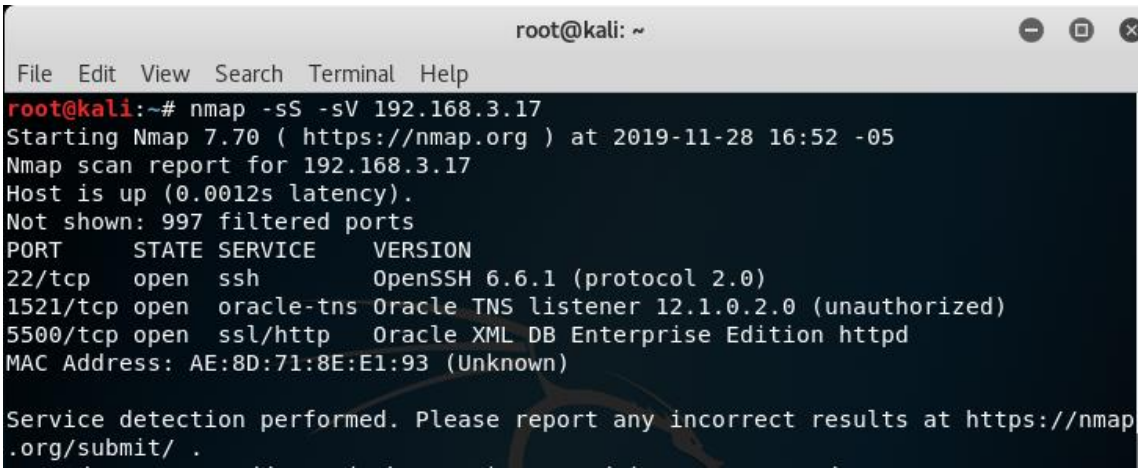


Fig. 10.- *Sondeo de puertos con NMAP Ip 192.168.3.17*

Elaborado por: *Investigador*

Servidor DE APLICACIONES WINDOWS SERVER 2008

Tabla 8.- *NMAP a servidor aplicaciones Windows server 2008*

Elaborado por: *Investigador*

Puerto	Protocolo	Estado	Servicio	Detalle
22	tcp	abierto	ssh	OpenSSH 6.6.1 (Protocol 2.0)
80	tcp	abierto	http	
443	tcp	abierto	Ssl/http	

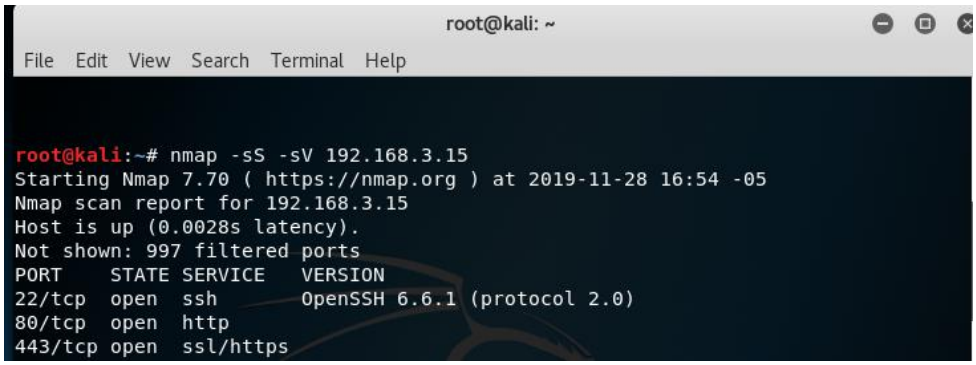


Fig. 11.- *Sondeo de puertos con NMAP ip 192.168.3.15*

Elaborado por: *Investigador*

Servidor INVENTARIO VEHICULOS WINDOWS SERVER 2008

Tabla 9.- *NMAP a servidor inventario vehículos Windows server 2008*

Elaborado por: *Investigador*

Puerto	Protocolo	Estado	Servicio	Detalle
80	tcp	Abierto	http	Microsoft IIS httpd 10.0
135	tcp	Abierto	msrpc	Microsoft Windows RPC
139	tcp	Abierto	netbios-scan	Microsoft Windows netbios-ssn
443	tcp	Abierto	ssl/http	VMware VirtualCenter Web service
445	tcp	Abierto	microsoft-ds	Microsoft Windows 7-10 microsoft-ds
902	tcp	Abierto	nagios-nsca	Nagios NSCA
912	tcp	Abierto	vmware-auth	VMware Authentication Daemon 1.0
1433	tcp	Abierto	ms-sql-s	Microsoft SQl Server 2012
2030	tcp	Abierto	device2?	
7070	tcp	Abierto	ssl/realserver?	
8040	tcp	Abierto	http	Microsoft IIS httpd 10.0

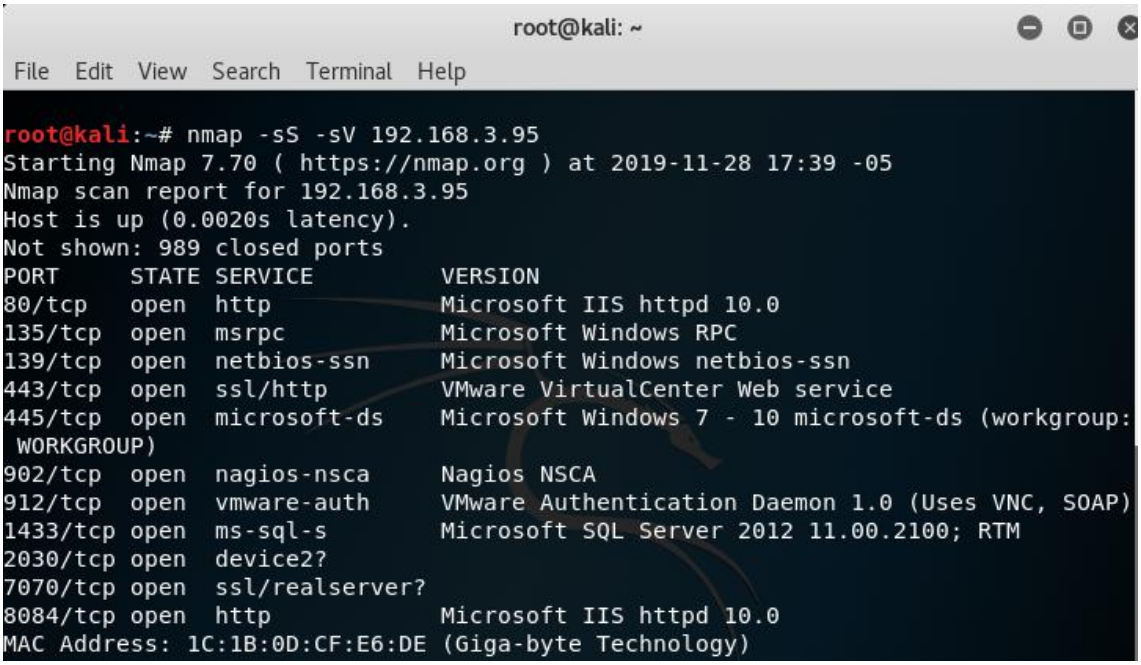


Fig. 12.- *Sondeo de puertos con NMAP Ip 192.168.3.95*

Elaborado por: *Investigador*

Servidor ANTIVIRUS WINDOWS SERVER 2012 r2

Tabla 10.- *NMAP a servidor de antivirus Windows server 2012 r2*

Elaborado por: *Investigador*

Puerto	Protocolo	Estado	Servicio	Detalle
80	Tcp	Abierto	http	Nginx 1.2.3
135	Tcp	Abierto	msrpc	Microsoft Windows RPC
139	Tcp	Abierto	netbios-ssn	Microsoft Windows netbios-ssn
443	Tcp	Abierto	ssl/http	VMware VirtualCenter web service
445	Tcp	Abierto	microsoft-ds	Microsoft Windows 7-10 microsoft-ds
902	Tcp	Abierto	ssl/vmware-auth	VMware Authentication Daemon 1.10
912	Tcp	Abierto	vmware-auth	VMware Authentication Daemon 1.0
1801	Tcp	Abierto	msmq?	
2103	Tcp	Abierto	msrpc	Microsoft Windows RPC
2105	Tcp	Abierto	msrpc	Microsoft Windows RPC
2107	Tcp	Abierto	msrpc	Microsoft Windows RPC
2968	tcp	Abierto	enpp?	
3306	tcp	Abierto	mysql	MySQL
4899	tcp	Abierto	radmin	Famatech Radmin 3.0

5357	tcp	Abierto	http	Microsoft HTTPAPI httpd 2.0
7070	tcp	Abierto	ssl/realserver?	
11111	tcp	Abierto	vce?	
14000	tcp	Abierto	scotty-ft?	
20000	tcp	Abierto	dnp?	

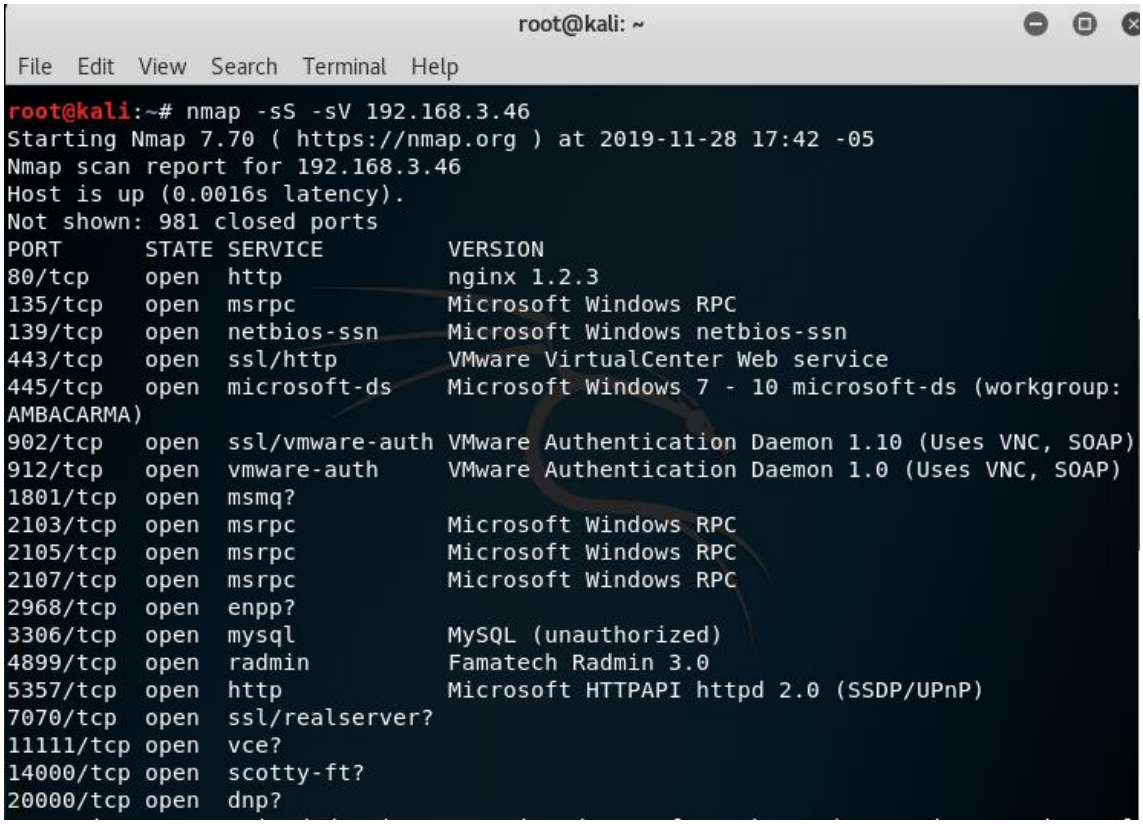


Fig. 13.- *Sondeo de puertos con NMAP Ip 192.168.3.46*

Elaborado por: *Investigador*

Servidor DE ARCHIVOS SERVER 2012 r2

Tabla 11.- *NMAP a servidor de archivos server 2012 r2*

Elaborado por: *Investigador*

Puerto	Protocolo	Estado	Servicio	Detalle
21	tcp	Abierto	ftp	
22	tcp	Abierto	ssh	OpenSSH 7.4
25	tcp	Abierto	smtp	Postfix smtpd
80	tcp	Abierto	http	nginx
110	Tcp	Abierto	pop3	Dovecot pop3d
111	Tcp	Abierto	rpcbind	2-4 RPC
139	Tcp	Abierto	netbios-ssn	Samba smdb 3.X-4.X
143	Tcp	Abierto	imap	Dovecot imap
443	Tcp	Abierto	ssl/http	nginx
445	Tcp	Abierto	netbios-ssn	Samba smbd 3.X-4.X

465	Tcp	Abierto	ssl/smtp	Postfix smtpd
548	Tcp	Abierto	afp	Netatalk 3.1.8
587	Tcp	Abierto	smtp	Postfix smtpd
993	Tcp	Abierto	ssl/imap	Dovecot imap
995	Tcp	Abierto	ssl/pop3	Dovecot imap
2049	Tcp	Abierto	nfs	2-3 RCP
3260	Tcp	Abierto	iscsi	Synology DSM ISCSI
3261	Tcp	Abierto	iscsi	Synology DSM Snapshot Replication Iscsi lun
8500	Tcp	Filtered	fmtp	
10025	Tcp	Filtered	Unknown	

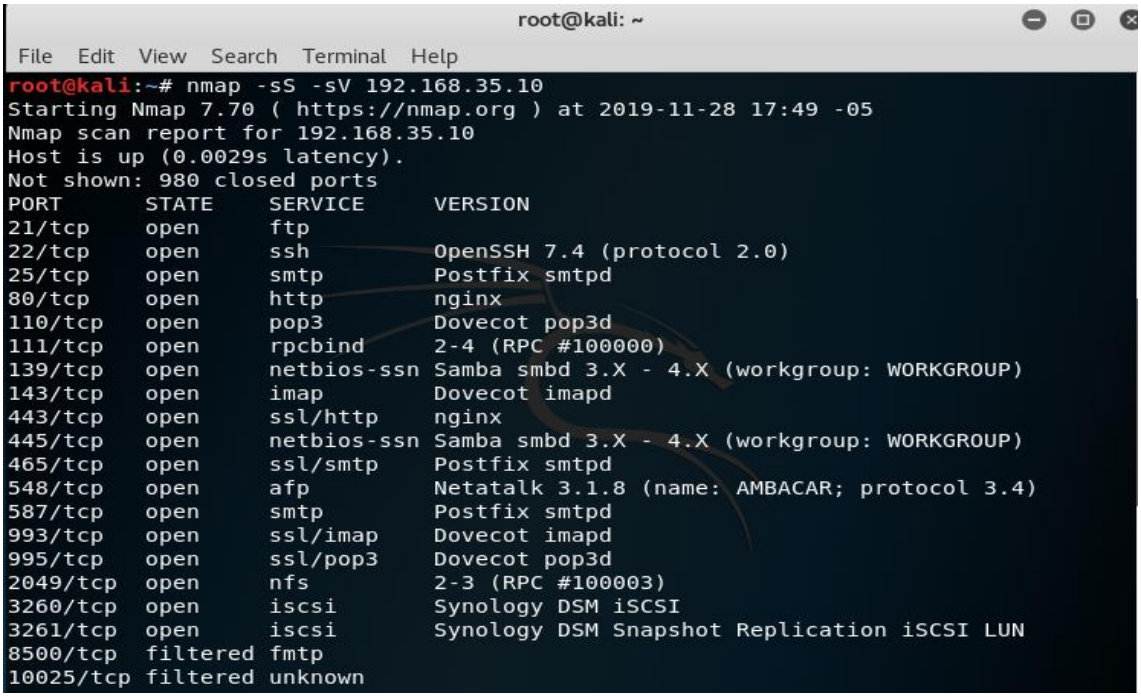


Fig. 14.- *Sondeo de puertos con NMAP Ip 192.168.35.10*

Elaborado por: *Investigador*

Servidor DE APLICACIONES SERVER 2008

Tabla 12.- *NMAP a servidor de aplicaciones server 2008*

Elaborado por: *Investigador*

Puerto	Protocolo	Estado	Servicio	Detalle
22	tcp	Abierto	ssh	OpenSSH 7.4
1521	tcp	Abierto	oracle-tns	Oracle TNS listener 12.1.0.2.0
5500	tcp	Abierto	ssl/http	Oracle XML BD Enterprise Edition httpd

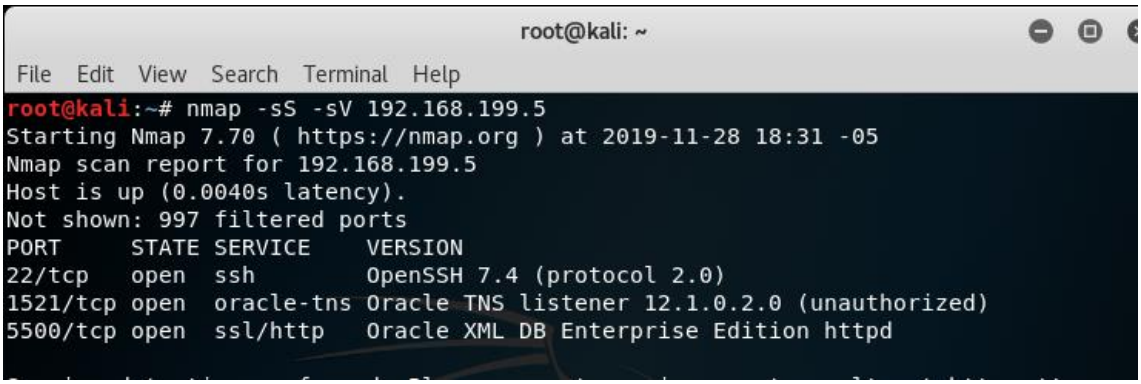


Fig. 15.- *Sondeo de puertos con NMAP Ip 192.168.3.18*

Elaborado por: *Investigador*

4.2.4. Búsqueda y verificación de vulnerabilidades

Mediante la herramienta NESSUS se procedió al escaneo de vulnerabilidades a los servidores de la empresa Ambacar, esta herramienta realiza un escaneo masivo donde muestra el nivel del riesgo que tiene a un posible ataque o ser vulnerado.

Análisis de vulnerabilidades con NESSUS

NESSUS es una herramienta que se la pueda encontrar tanto en Windows, Linux, entre otros.

Para la realización del escaneo simplemente se crea en la página principal un Nuevo Escaneo (New Scan), posterior a esto se debe escoger escaneo recomendado (Basic Network Scan), dentro del mismo se procede a colocar el nombre del proceso, la descripción, se escoge la carpeta contenedora para el proceso, se coloca la dirección IP y finalmente se guarda esta información.

Hay que tener en cuenta que algunas de las pruebas de vulnerabilidades de Nessus pueden causar que los servicios o sistemas operativos se corrompan, se dañen o caigan, para esto se procedió a desactivar "unsafe test" (pruebas no seguras) antes de escanear para evitar cualquier inconveniente con los servidores.

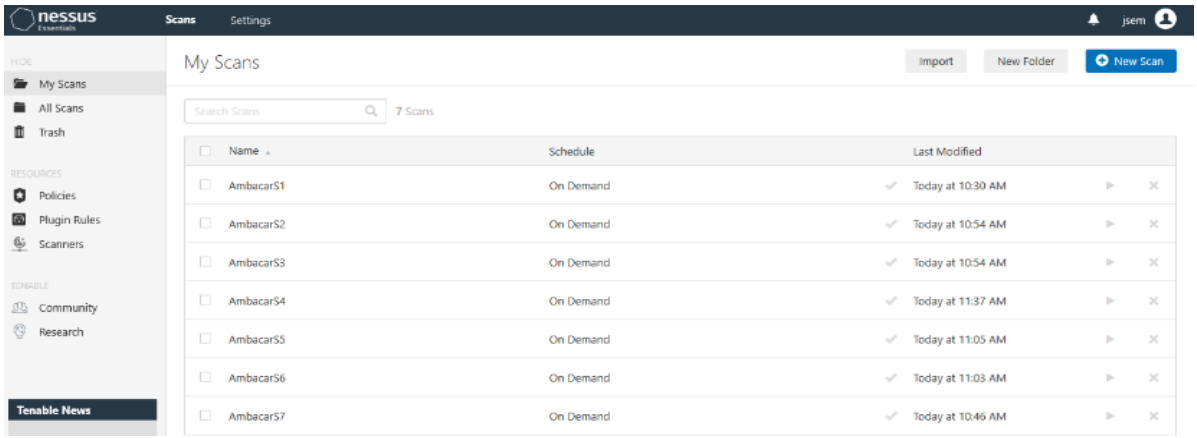


Fig. 16.- *Vista de escaneo a los servidores con NESSUS*

Elaborado por: *Investigador*

Se detallará como muestra en la figura cada vulnerabilidad encontrada con su respectiva imagen.

Servidor 1

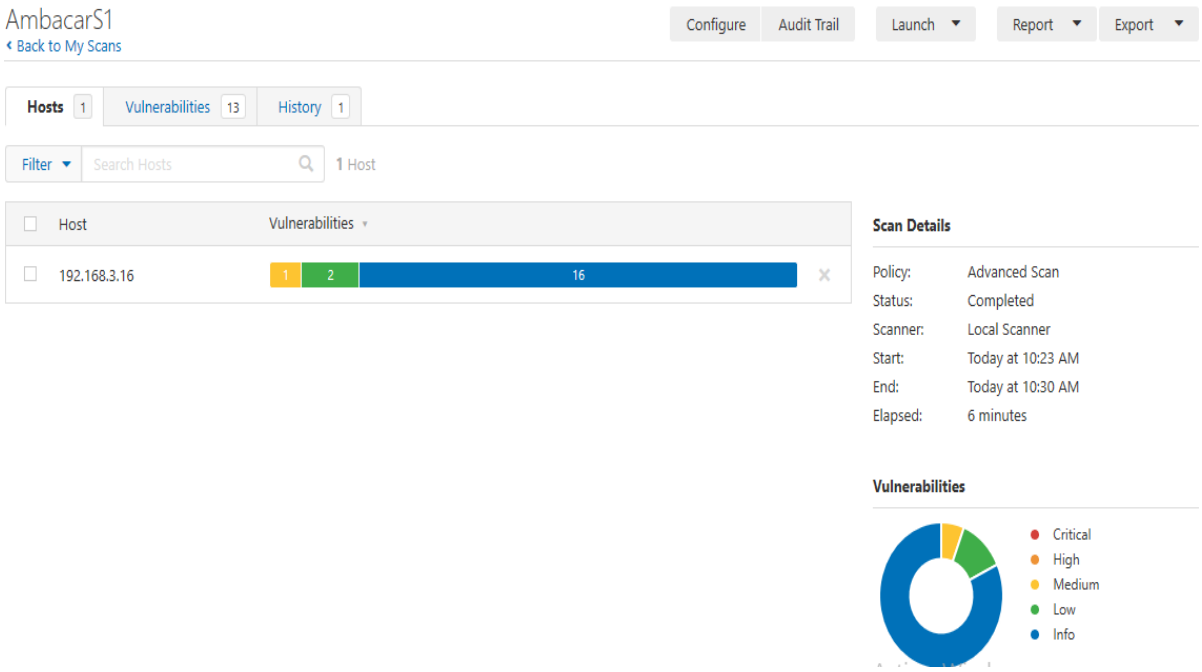


Fig. 17.- *Escaneo de vulnerabilidades con NESSUS Servidor 1*

Elaborado por: *Investigador*

Servidor BASE DE DATOS ORACLE LINUX 7.3

Tabla 13.- *Vulnerabilidades detectadas en servidor de BASE DE DATOS ORACLE LINUX 7.3 con Nessus*

Elaborado por: *Investigador*

Servicio	Vulnerabilidad	Riesgo	Observación
Remote SSH serve	Nessus ha detectado que el servidor SSH remoto está configurado para usar el	Medio	El servidor SSH remoto está configurado para permitir

	cifrado de flujo Arcfour o ningún cifrado. RFC 4253 desaconseja el uso de Arcfour debido a un problema con claves débiles.		algoritmos de cifrado débiles o ningún algoritmo.
SSH server -Cipher Block Chaining	El servidor SSH está configurado para admitir el cifrado Cipher Block Chaining (CBC) lo que esto puede permitir que un atacante recupere el mensaje de texto sin formato del texto cifrado.	Bajo	El servidor SSH está configurado para usar Cipher Block Chaining. Tenga en cuenta que este complemento solo busca las opciones del servidor SSH y no busca versiones de software vulnerables.
Remote SSH server	El servidor SSH remoto está configurado para permitir algoritmos MAC MD5 o de 96 bits, los cuales se consideran débiles. .	Bajo	El servidor SSH remoto está configurado para permitir algoritmos de MD5 y MAC de 96 bits. Tenga en cuenta que este complemento solo busca las opciones del servidor SSH y no busca versiones de software vulnerables

Servidor 2

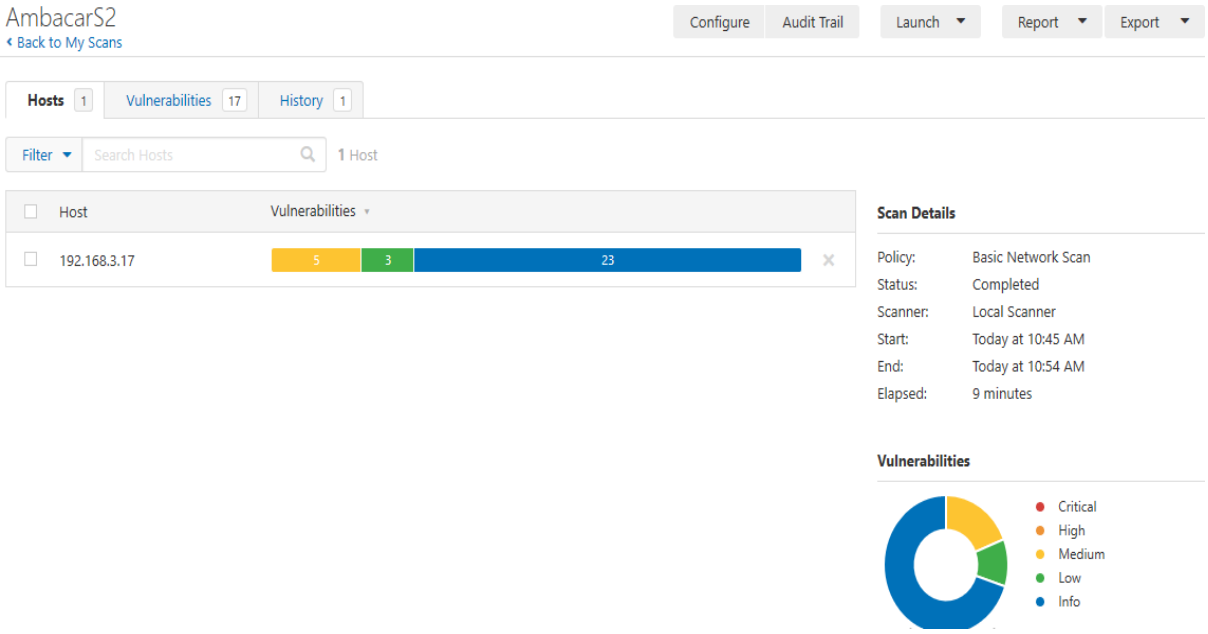


Fig. 18.- *Escaneo de vulnerabilidades con NESSUS Servidor 2*

Elaborado por: *Investigador*

Servidor BASE DE DATOS ORACLE LINUX 7.3

Tabla 14.- *Vulnerabilidades detectadas en servidor de BASE DE DATOS ORACLE LINUX 7.3 con Nessus*

Elaborado por: *Investigador*

Servicio	Vulnerabilidad	Riesgo	Observación
SSL Certificate	No se puede confiar en el certificado X.509 del servidor. Esta situación puede ocurrir debido a que se puede romper la cadena de confianza. Si el host remoto es un host público en producción, cualquier interrupción en la cadena hace que sea más difícil para los usuarios verificar la autenticidad e identidad del servidor web.	Medio	No se puede confiar en el certificado SSL para este servicio. Esto podría facilitar la realización de ataques man-in-the-middle contra el host remoto.
SSL Self-Signed Certificate	La cadena de certificados X.509 para este servicio no está firmada por una	Medio	La cadena de certificados SSL para este servicio termina en un certificado autofirmado no reconocido.

	autoridad de certificación reconocida.		Si el host remoto es un host público en producción, esto anula el uso de SSL ya que cualquiera podría establecer un ataque man-in-the-middle contra el host remoto.
SSL Certificate - Hashing Algorithm	El servicio remoto utiliza una cadena de certificados SSL que se ha firmado utilizando un algoritmo de hash criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a los ataques de colisión.	Medio	Un atacante puede explotar esto para generar otro certificado con la misma firma digital, permitiendo que un atacante se haga pasar por el servicio afectado.
SSL Cipher (SWEET32)	El host remoto admite el uso de cifrados SSL que ofrecen cifrado de fuerza media	Medio	Nessus considera la fuerza media como cualquier encriptación que usa longitudes de clave de al menos 64 bits y menos de 112 bits, o que usa la suite de encriptación 3DES.
SSH - Algorithms Supported	Nessus ha detectado que el servidor SSH remoto está configurado para usar el cifrado de flujo Arcfour o ningún cifrado.	Medio	Nessus y su servicio RFC 4253 desaconseja el uso de Arcfour debido a un problema con claves débiles.
SSH Server CBC Ciphers	El servidor SSH está configurado para admitir el cifrado Cipher Block Chaining (CBC).	Bajo	Esto puede permitir que un atacante recupere el mensaje de texto sin formato del texto cifrado. Tenga en cuenta que este complemento solo busca las opciones del servidor SSH y no busca versiones de software vulnerables.
SSH MAC Algorithms	El servidor SSH remoto está configurado para permitir algoritmos MAC MD5 o de 96 bits	Bajo	Los algoritmos MAC MD5 o de 96 bits se consideran débiles. Tenga en cuenta que este complemento solo busca las opciones del servidor SSH y no busca versiones de software vulnerables.

SSL RC4 Cipher	El host remoto admite el uso de RC4 en uno o más conjuntos de cifrado. El cifrado RC4 tiene fallas en su generación de una secuencia de bytes pseudoaleatoria, de modo que se introduce una amplia variedad de pequeños sesgos en la secuencia, disminuyendo su aleatoriedad.	Bajo	En el cifrado RC4 si el texto sin formato se encripta repetidamente (por ejemplo, cookies HTTP), y un atacante puede obtener muchos (por ejemplo, decenas de millones) de textos cifrados, el atacante puede derivar el texto sin formato.

Servidor 3

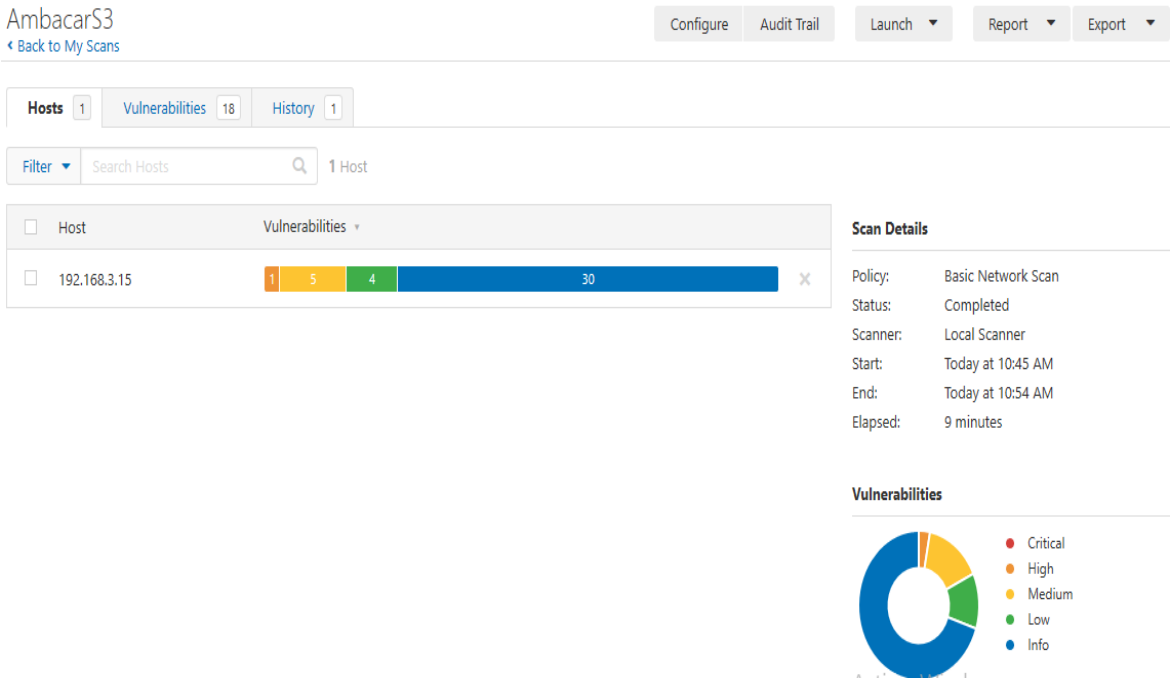


Fig. 19.- *Escaneo de vulnerabilidades con NESSUS Servidor 3*

Elaborado por: *Investigador*

Servidor DE APLICACIONES WINDOWS SERVER 2008

Tabla 15.- *Vulnerabilidades detectadas en Servidor de APLICACIONES WINDOWS SERVER 2008 con Nessus*

Elaborado por: *Investigador*

Servicio	Vulnerabilidad	Riesgo	Observación
SSL Version 2 and 3 Protocol	El servicio remoto acepta conexiones encriptadas usando SSL 2.0 y / o SSL 3.0. Estas versiones de SSL se ven afectadas por	Alto	Aunque SSL / TLS tiene un medio seguro para elegir la versión más compatible del protocolo muchos navegadores web

	varios defectos criptográficos, que incluyen: - Un esquema de relleno inseguro con cifrados CBC. - Renegociación de sesiones inseguras y esquemas de reanudación.		implementan esto de una manera insegura que permite a un atacante degradar una conexión. Por lo tanto, se recomienda que estos protocolos se deshabiliten por completo.
SSL Certificate	No se puede confiar en el certificado X.509 del servidor. Esta situación puede ocurrir debido a que se puede romper la cadena de confianza. Si el host remoto es un host público en producción, cualquier interrupción en la cadena hace que sea más difícil para los usuarios verificar la autenticidad e identidad del servidor web.	Medio	No se puede confiar en el certificado SSL para este servicio. Esto podría facilitar la realización de ataques man-in-the-middle contra el host remoto.
SSL Self-Signed Certificate	La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida.	Medio	Si el host remoto es un host público en producción, esto anula el uso de SSL ya que cualquiera podría establecer un ataque man-in-the-middle contra el host remoto.
SSL Cipher (SWEET32)	El host remoto admite el uso de cifrados SSL que ofrecen cifrado de fuerza media. Nessus considera la fuerza media como cualquier encriptación que usa longitudes de clave de al menos 64 bits y menos de 112 bits, o que usa la suite de encriptación 3DES. .	Medio	Tener en cuenta que es considerablemente más fácil eludir el cifrado de fuerza media si el atacante está en la misma red física

SSH Algorithms Supported	Nessus ha detectado que el servidor SSH remoto está configurado para usar el cifrado de flujo Arcfour o ningún cifrado.	Medio	Nessus desaconseja el uso de Arcfour debido a un problema con claves débiles.
Transport Layer Security (TLS) Protocol	El servicio remoto tiene una de dos configuraciones que se sabe que son necesarias para el ataque CRIME: - La compresión SSL / TLS está habilitada. - TLS anuncia el protocolo SPDY anterior a la versión 4.	Medio	Deshabilite la compresión y / o el servicio SPDY para evitar esos ataques.
SSH Server CBC Ciphers	El servidor SSH está configurado para admitir el cifrado Cipher Block Chaining (CBC).	Bajo	Esto puede permitir que un atacante recupere el mensaje de texto sin formato del texto cifrado por lo que es mejor deshabilitar el cifrado de modo CBC y habilitar el cifrado en modo de cifrado CTR o GCM.
SSH MAC Algorithms	El servidor SSH remoto está configurado para permitir algoritmos MAC MD5 o de 96 bits, los cuales se consideran débiles	Bajo	Como recomendación es mejor desactivar los algoritmos MD5 y MAC de 96 bits.
SSL RC4 Cipher	El host remoto admite el uso de RC4 en uno o más conjuntos de cifrado. El cifrado RC4 tiene fallas en su generación de una secuencia de bytes pseudoaleatoria, de modo que se introduce una amplia variedad de pequeños sesgos en la secuencia, disminuyendo su aleatoriedad.	Bajo	En el cifrado RC4 si el texto sin formato se encripta repetidamente (por ejemplo, cookies HTTP), y un atacante puede obtener muchos (por ejemplo, decenas de millones) de textos cifrados, el atacante puede derivar el texto sin formato.
SSL Certificate Chain	No se puede confiar en el certificado X.509 del servidor. Esta situación	Bajo	Para evitar estos problemas reemplace el certificado en la cadena con la clave RSA

	puede ocurrir debido a que se puede romper la cadena de confianza. Si el host remoto es un host público en producción, cualquier interrupción en la cadena hace que sea más difícil para los usuarios verificar la autenticidad e identidad del servidor web.		de menos de 2048 bits de longitud con una clave más larga

Servidor 4

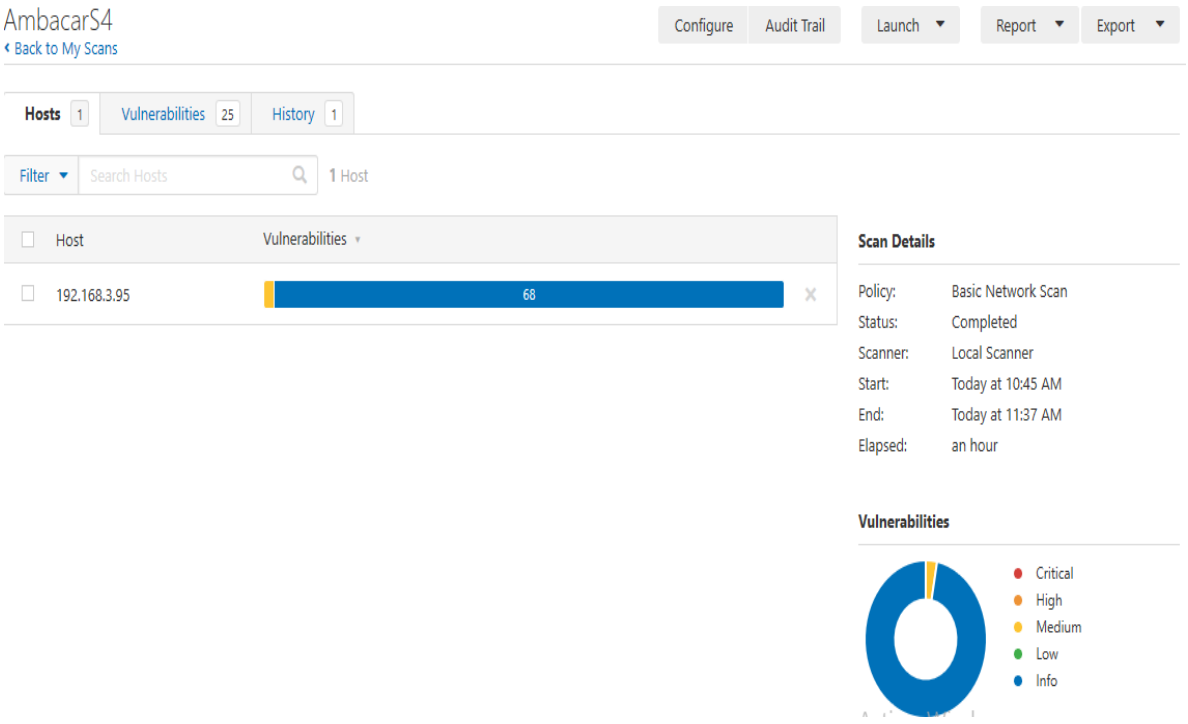


Fig. 20.- *Escaneo de vulnerabilidades con NESSUS Servidor 4*

Elaborado por: *Investigador*

Servidor INVENTARIO VEHICULOS WINDOWS SERVER 2008

Tabla 16.- *Vulnerabilidades detectadas en servidor INVENTARIO VEHICULOS WINDOWS SERVER 2008 con Nessus*

Elaborado por: *Investigador*

Servicio	Vulnerabilidad	Riesgo	Observación
SMB server	No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede explotar esto para realizar ataques	Medio	Aplicar la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de

	man-in-the-middle contra el servidor SMB.		directiva 'Servidor de red de Microsoft: firmar digitalmente las comunicaciones (siempre)'.

Servidor 5

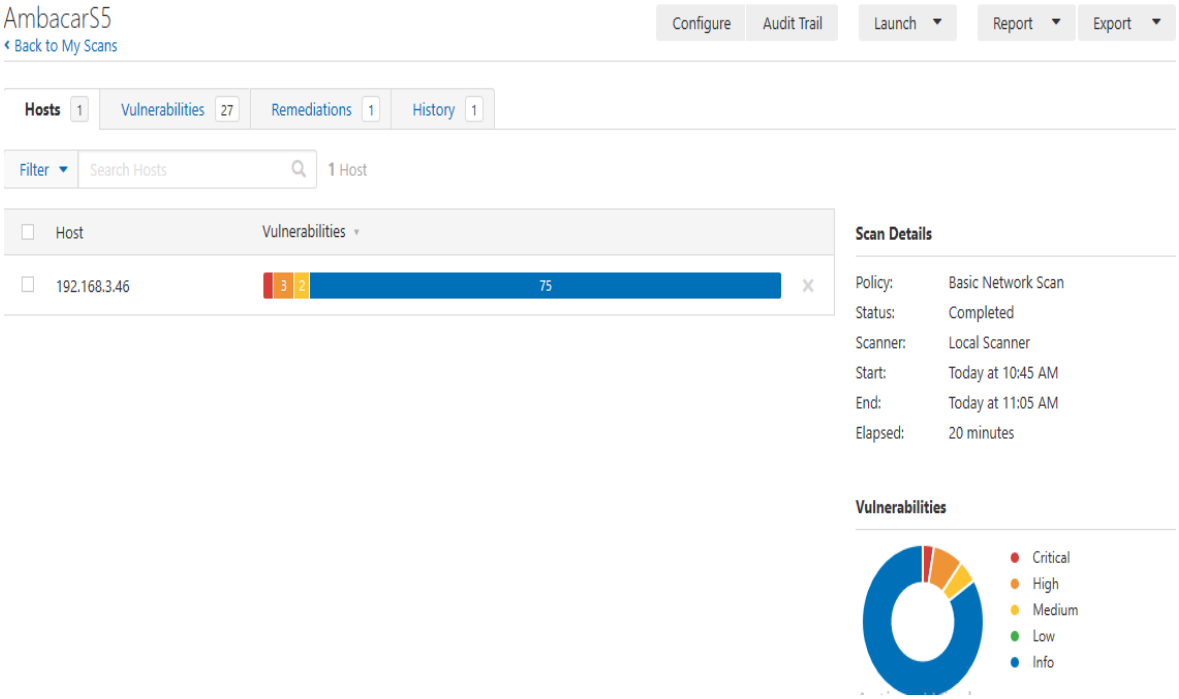


Fig. 21.- *Escaneo de vulnerabilidades con NESSUS Servidor 5*

Elaborado por: *Investigador*

Servidor DE ANTIVIRUS WINDOWS SERVER 2012 r2

Tabla 17.- *Vulnerabilidades detectadas en servidor DE ANTIVIRUS WINDOWS SERVER 2012 r2 con Nessus*

Elaborado por: *Investigador*

Servicio	Vulnerabilidad	Riesgo	Observación
PHP Unsupported Version	Según su versión, la instalación de PHP en el host remoto ya no es compatible.	Critico	Según su versión, la instalación de PHP en el host remoto ya no es compatible.
PHP < 5.3.11	La versión de PHP instalada en el host remoto es anterior a 5.3.11 y, como tal, se ve potencialmente afectada por múltiples vulnerabilidades:	Alto	Actualice a PHP versión 5.3.11 o posterio

PHP < 5.3.12 / 5.4.2 CGI Query String	La versión de PHP instalada en el host remoto es anterior a 5.3.12 / 5.4.2, y como tal se ve potencialmente afectada por una vulnerabilidad de ejecución remota de código y divulgación de información.	Alto	Actualizar PHP versión 5.3.12 / 5.4.2 o posterior. También está disponible una solución alternativa 'mod_rewrite'.
PHP < 5.3.9	La versión de PHP instalada en el host remoto es anterior a 5.3.9.	Alto	Actualice a PHP versión 5.3.9 o posterior.
PHP_ RSHUTDOWN_ FUNCTION	El servidor web remoto utiliza una versión de PHP que se ve potencialmente afectada por una vulnerabilidad de omisión de seguridad.	Medio	Actualice a PHP versión 5.3.11 / 5.4.1 o posterior.
SMB server	Un atacante remoto no autenticado puede explotar esto para realizar ataques man-in-the-middle contra el servidor	Medio	Aplicar la firma de mensajes en la configuración del host en Windows, esto se encuentra en la configuración de directiva 'Servidor de red de Microsoft: firmar digitalmente las comunicaciones (siempre)'.

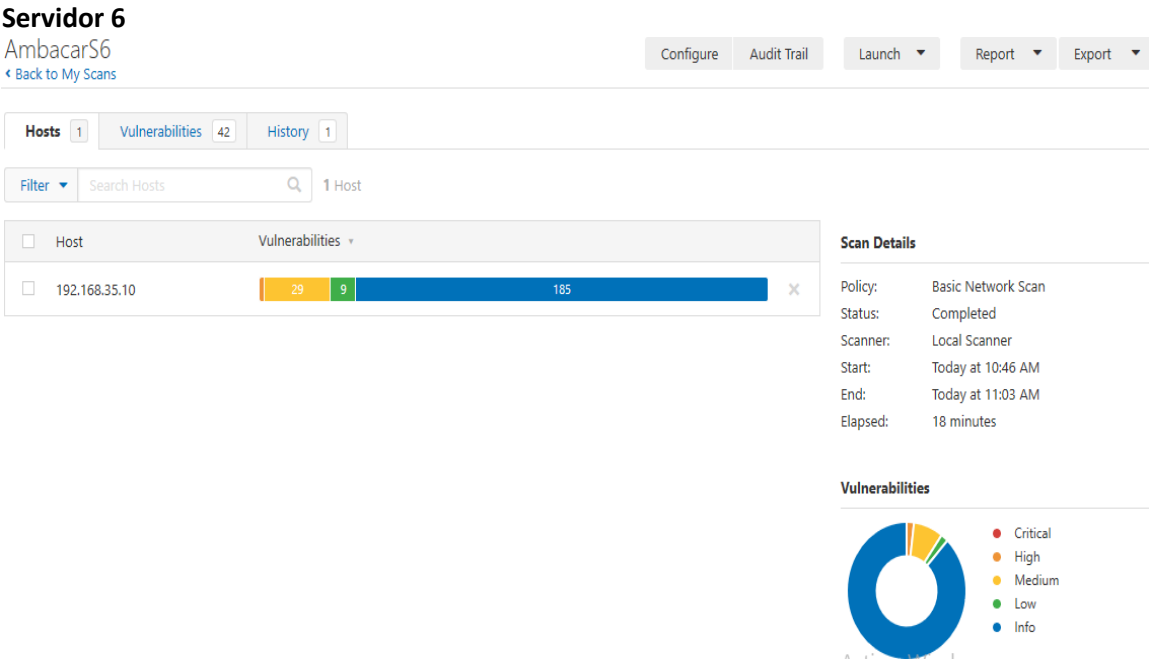


Fig. 22.- *Escaneo de vulnerabilidades con NESSUS Servidor 6*

Elaborado por: *Investigador*

Servidor DE ARCHIVOS WINDOWS SERVER 2012 r2

Tabla 18.- *Vulnerabilidades detectadas en servidor DE ARCHIVOS WINDOWS SERVER 2012 r2 con Nessus*

Elaborado por: *Investigador*

Servicio	Vulnerabilidad	Riesgo	Observación
iSCSI Target	Uno o más de los objetivos iSCSI (Interfaz de sistemas de computadoras pequeñas de Internet) en el host remoto están configurados para no usar un mecanismo de autenticación, lo que potencialmente permite el acceso no autorizado a los objetivos.	Alto	Configure la autenticación en el destino para restringir el acceso a los iniciadores autorizados.
SSL Certificate	No se puede confiar en el certificado X.509 del servidor. Esta situación puede ocurrir debido a que se puede romper la cadena de confianza. Si el host remoto es un host público en producción, cualquier interrupción en la cadena hace que sea más difícil	Medio	No se puede confiar en el certificado SSL para este servicio. Esto podría facilitar la realización de ataques man-in-the-middle contra el host remoto.

	para los usuarios verificar la autenticidad e identidad del servidor web.		
SMB server	No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede explotar esto para realizar ataques man-in-the-middle contra el servidor SMB.	Medio	Aplicar la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de directiva 'Servidor de red de Microsoft: firmar digitalmente las comunicaciones (siempre)'.
SSL Certificate	El certificado SSL para este servicio es para un host diferente.	Medio	Compre o genere un certificado adecuado para este servicio.
SSL Cipher (SWEET32)	El host remoto admite el uso de cifrados SSL que ofrecen cifrado de fuerza media. Nessus considera la fuerza media como cualquier encriptación que usa longitudes de clave de al menos 64 bits y menos de 112 bits, o que usa la suite de encriptación 3DES.	Medio	Vuelva a configurar la aplicación afectada si es posible para evitar el uso de cifrados de fuerza media.
mDNS (Remote Network)	Es posible obtener información sobre el host remoto, el servicio remoto comprende el protocolo Bonjour (también conocido como ZeroConf o mDNS), que permite a cualquier persona descubrir información del host remoto, como el tipo de sistema operativo y la versión exacta, su nombre de host , y la lista de servicios que está ejecutando.	Medio	Este complemento intenta descubrir los mDNS utilizados por los hosts que no están en el segmento de red en el que reside Nessus. Filtre el tráfico entrante al puerto UDP 5353 para resolver este problema.
SSL Certificate Chain	La cadena de certificados X.509 utilizada por este servicio contiene certificados con claves RSA de menos de 2048 bits.	Bajo	Reemplace el certificado en la cadena con la clave RSA de menos de 2048 bits de longitud con una clave más larga.

Servidor 7

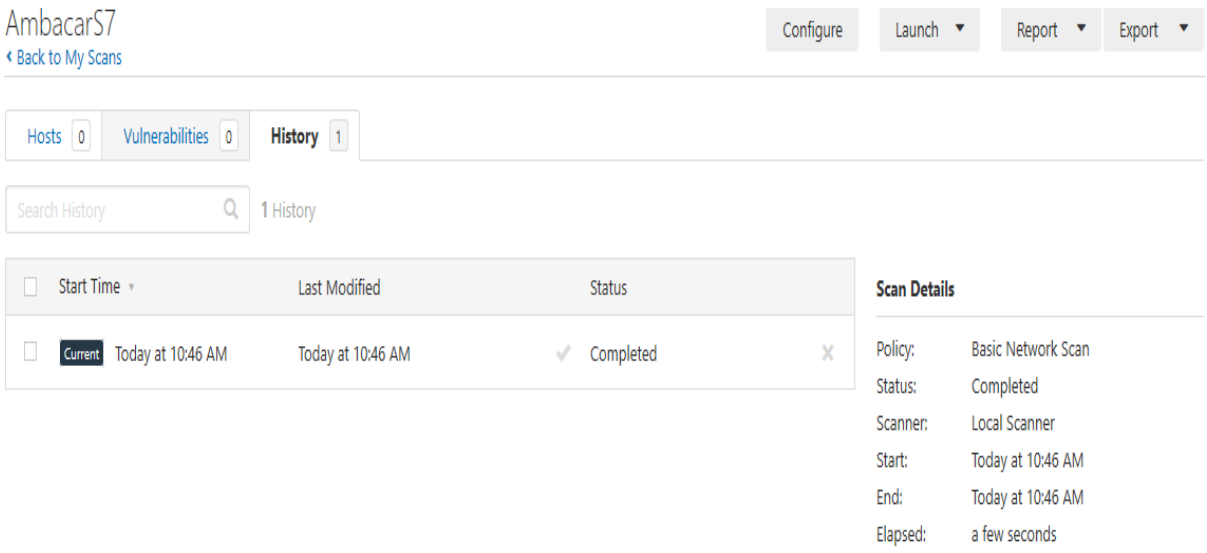


Fig. 23.- *Escaneo de vulnerabilidades con NESSUS Servidor 7*

Elaborado por: *Investigador*

- En el caso del servidor 7 no se encontró vulnerabilidades.

4.3.Implementación del SGSI

El Sistema de Gestión de Riesgos se lo realizará en base a los dominios y controles de la ISO/IEC 27001 donde su estructura es la siguiente:

- Alcance
- Definición de Políticas
- Gestión de Riesgos
- Declaración de Aplicabilidad
- Análisis de cumplimiento de controles

4.3.1. Alcance del SGSI

El alcance del proyecto se basa según los servicios a donde está orientado tomando en cuenta sus activos, departamentos, procesos etc. El alcance se definirá de la siguiente manera:

- Mantenimiento periódico a los equipos (Hardware / Software) existentes en el DataCenter, así como a los sistemas que se manejan en la empresa para su desempeño óptimo y fiable.

- Dentro del departamento de recursos humanos al personal se le definirá responsables cuyas funciones garanticen las seguridades de los recursos ya sea en el caso de laborar en la empresa o de culminación o cambio de empleo.
- Para la gestión de activos de la empresa se asignará responsables cuya función es la regulación y control de uso adecuado de los activos, estas responsabilidades serán asignadas después de un previo análisis y gestión de riesgos y vulnerabilidades existentes.
- Control y verificación de identidades a la persona que tenga acceso a activos físicos y lógicos de la empresa para mantener la integridad y confidencialidad de la información.

4.3.2. Política de Seguridad del Sistema de Gestión de Seguridad de la Información

A continuación, la política de seguridad qué cumple de manera general con las necesidades relacionadas con la seguridad de la empresa es:

¨Fomentar la continuidad de las prácticas, tareas y funciones del departamento de sistemas mediante un Sistema de Gestión de Seguridad Informática basado en la integridad, confidencialidad y disponibilidad de la información con el objetivo de prevenir, controlar y mitigar riesgos para la empresa ¨

Objetivos:

Se han definido objetivos para asegurar el cumplimiento de la política mencionada:

- Establecer períodos de control para prever vulnerabilidades referentes a la seguridad de la información.
- Elaborar una gestión de riesgos para para el control de la información.
- Implementar el sistema de gestión de seguridad de la información.
- Supervisar y controlar el sistema de gestión de la seguridad de la información para su tratamiento.

4.3.3. Gestión de Riesgos

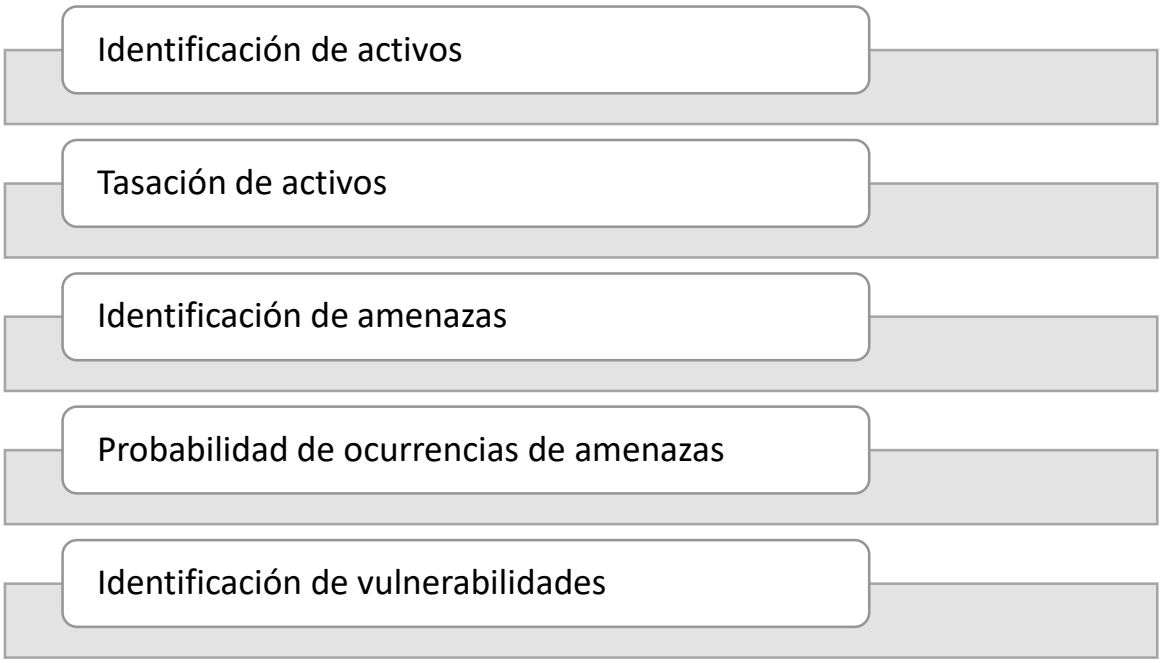
Analizar los riesgos en una empresa o institución es de suma importancia debido a que mediante este análisis y evaluación de riegos se puede definir un proceso donde estos riesgos se los considere como aceptables o mitigables aplicando un determinado tratamiento.

El objetivo esencial de la gestión de riesgos es identificar las amenazas que se susciten a los activos de la empresa para a partir de ello detallar las vulnerabilidades encontradas y así poder disminuir o mitigar estas amenazas.

El esquema metodológico a utilizar es el siguiente:

Tabla 19.- *Metodología para la gestión de riesgos*

Elaborado por: *investigador*



- **Identificación y Tasación de Activos**

La información manipulada en la empresa es de gran importancia es por esto que se va a dar un trato especial y adecuado para su protección adecuada y eficaz, esto se lo realiza mediante la identificación de los activos que tiene la empresa en la actualidad donde se procede a tasarlos con el fin de observa que activos de mayor relevancia para la empresa según los niveles de confidencialidad, integridad y disponibilidad de la información [13].

La probabilidad de ocurrencia, e impacto está compuesta por 5 niveles así:

- **Eje de Probabilidad:**

1. Casi seguro
2. Alto
3. Medio
4. Bajo
5. Raro

- **Eje de Impacto:**

1. Muy grave
2. Severo
3. Medio
4. Leve
5. Sin impacto

Con el proceso mencionado anteriormente se determina la probabilidad de incidencia de las amenazas teniendo en cuenta los riegos que implican, el valor del riesgo por último se extrae de la siguiente manera [13]:

$$Riesgo = Valoración\ total\ del\ activo\ \times\ Probabilidad\ de\ amenaza$$

Inventario de activos informáticos

Para cada criterio se deben generar áreas de impacto, es decir, condiciones de cómo la organización se verá afectada por algún incidente de seguridad. El impacto puede ser alto, medio o bajo, y esto deberá ser definido por el personal encargado de generar los criterios de medición del riesgo [13].

Los principales tipos de activos son los físicos, de sistemas de información y de software, es por esto que se los evaluará en un rango del 1 al 5, en los cuales la categoría más importante recibe el puntaje más alto y la menos importante recibe la calificación más baja, para obtener un promedio de disponibilidad, confidencialidad e integridad de la información que tiene la empresa [13].

Tabla 20.- *Identificación y tasación de riesgos*

Elaborado por: *Investigador*

ACTIVOS	Confidencialidad	Disponibilidad	Integridad	Total
Servidor de Archivos	4	3	4	4
Impresoras multifunción	3	3	3	3
Sistema Financiero	4	4	4	4
Central Telefónica IP	2	4	4	3
Correo Institucional	3	2	3	2
Router	3	3	3	3
Cuentas de usuario	3	3	3	3

Computadores de oficina y Laptops	3	3	3	3
Switch	2	3	3	3

Los activos que en el total den igual o mayor a 3 se proceden a ser una evaluación de riesgos minuciosa.

Tabla 21.- *Activos de mayor importancia*

Elaborado por: *Investigador*

Activo	***Amenaza***	***Vulnerabilidades***	***Valoración del Activo***	***Probabilidad de Amenaza***	***Total del Riesgo***
Servidor de Archivos	Robo de Información	Falta de Mantenimiento	4	4	16
	Alteración de Datos o Información	Falta de Medidas de seguridad			
Impresoras Multifunción	Atasco de Papel		3	3	9
	Falta de Limpieza de Cabezales	Falta de Mantenimiento			
	Falta de Tinta	Formato incompatible de papel			
	Cartuchos Dañados o Desgastados				
Sistema Financiero	Perdida de Documentos	Falta de Políticas de Seguridad	4	3	12
	Robo de Información	Falta de Control de acceso			
Central Telefónica IP	Perdida de Señal	Falta de Mantenimiento	3	2	6
	Trafico excesivo en la red y caída de conexión.	Inadecuada Configuración			
Router	Falta de Mantenimiento	Mala ubicación del equipo	3	3	9

	Calentamiento Excesivo	Problemas eléctricos			
	Equipo antiguo	Excesivo tráfico de Datos			
Cuentas de Usuario	Modificación de una cuenta	Control de acceso inadecuado	3	3	9
	Pérdida de password de una cuenta				
Computadoras de oficina y Laptops	Spyware	Falta de control de acceso	3	3	9
	Virus de Computadora	Falta de Mantenimiento			
	Malware	Uso indebido de internet			
	Phishing	Falta de herramientas de monitoreo			
Switch	Falta de Mantenimiento	Mala ubicación del equipo	3	2	6
	Calentamiento Excesivo	Problemas eléctricos			
	Equipo antiguo	Excesivo tráfico de Datos			

Este análisis de evaluación de riesgos de activos informáticos de la empresa AMBACAR permitió identificar de una manera clara y sencilla la tasa de activos más altas que pueden ser vulnerados, atacados o que presenten algún posible dañado.

- **Selección de objetivos de control**

Mediante la tasa de índices de riesgos estudiadas en la Tabla85 se prosigue a gestionar los controles mediante la ISO 27001

- **Dominios de la ISO27001**

Según en Anexo A Objetivos de control y controles de referencia de la ISO27001 – 2017

  - A.5 Políticas de seguridad de la información.
  - A.6 Organización de seguridad de la información.
  - A.7 Seguridad relativa a los recursos humanos.
  - A.8 Gestión de activos.
  - A.9 Control de acceso.
  - A.10 Criptografía.
  - A.11 Seguridad física y del entorno.
  - A.12 Seguridad de las operaciones.
  - A.13 Seguridad de las comunicaciones
  - A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información.
  - A.15 Relación con proveedores.
  - A.16 Gestión de incidentes de seguridad de la información.
  - A, 17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio.
  - A.18 Cumplimiento

Mediante estos dominios de la ISO 27001 podemos agregar una casilla donde se muestre la columna “Objetivo de Control” donde se escogerá el dominio pertinente que llene con las condiciones de la evaluación realizada en la Tabla 86 con el fin de detallar la amenaza en el activo informático.

Tabla 22.- *Selección de controles*

Elaborado por: *Investigador*

Activo	***Amenaza***	***Vulnerabilidades***	***Valoración del Activo***	***Probabilidad de Amenaza***	***Total del Riesgo***	***Objetivo de Control***
Servidor de Archivos	Robo de Información	Falta de Mantenimiento	4	4	16	A.11 Seguridad física y del entorno
	Alteración de Datos o Información	Falta de Medidas de seguridad				
Impresoras Multifunción	Atasco de Papel	Formato incompatible de papel	3	3	9	A.8 Gestión de activos A.11 Seguridad física y del entorno
	Falta de Limpieza de Cabezales	Falta de Mantenimiento				
	Falta de Tinta	Falta de Mantenimiento				
	Cartuchos Dañados o Desgastados					
Sistema Financiero	Perdida de Documentos	Falta de Politicas de Seguridad	4	3	12	A.9 Control de acceso A.5 Políticas de seguridad de la información
	Robo de Información	Falta de Control de acceso				
	Perdida de Señal	Falta de Mantenimiento	3	2	6	

Central Telefónica IP	Trafico excesivo en la red y caída de conexión.	Inadecuada Configuración				A.11 Seguridad física y del entorno A.13 Seguridad de las comunicaciones
Router	Falta de Mantenimiento	Mala ubicación del equipo	3	3	9	A.11 Seguridad física y del entorno A.13 Seguridad de las comunicaciones
	Calentamiento Excesivo	Problemas eléctricos				
	Equipo antiguo	Excesivo tráfico de Datos				
Cuentas de Usuario	Modificación de una cuenta	Control de acceso inadecuado	3	3	9	A.9 Control de acceso
	Perdida de password de una cuenta					
Computadoras de oficina y Laptops	Spyware	Falta de control de acceso	3	3	9	A.9 Control de acceso
	Virus de Computadora	Falta de Mantenimiento				

	Malware	Uso indebido de internet				A.11 Seguridad física y del entorno A.12 Seguridad de las operaciones
	Phishing	Falta de herramientas de monitoreo				
Switch	Falta de Mantenimiento	Mala ubicación del equipo	3	2	6	A.11 Seguridad física y del entorno A.13 Seguridad de las comunicaciones
	Calentamiento Excesivo	Problemas eléctricos				
	Equipo antiguo	Excesivo tráfico de Datos				

4.3.4. Declaración de aplicabilidad

La Declaración de Aplicabilidad - SOA (Arquitectura Orienta a Servicios) permite la creación de sistema de información con una escalabilidad alta para la empresa lo cual se basa en las áreas y dominios de la ISO 27001.

Todo este proceso tiene la finalidad de analizar e identificar cada uno de los controles aplicables en el departamento de sistemas de la empresa AMBACAR – Ambato para su uso correcto, así como la identificación de los controles no aplicables para no usarlos con una debida justificación.

Esta declaración de aplicabilidad será revisada y aprobada previamente por el Ing. Jorge Parra, donde la declaración consiste en:

- Área o Dominio de control de la norma ISO 27001.
- Objetivos de control de cada Dominio.
- Justificación de controles de cada Objetivo de control escogido.

➢ A.5 Políticas de seguridad de la información

Tabla 23.- *Políticas de seguridad de la información*

Elaborado por: *Investigador*

Política	***Análisis***			
A.5 Políticas de seguridad de la información	***Sección***		A.5.1 Directrices de gestión de la seguridad de la información	
	Control de la ISO 27001		5.1.1	5.1.2
			Políticas para la seguridad de la información	Revisión de las políticas para la seguridad de la información
	Aplicabilidad	***Si***		
		No	X	X
	Justificación		Es de vital importancia la creación de un documento de políticas de seguridad para la empresa AMBACAR ya que el bien más preciado de la empresa es la información además ayuda a guiarse en el caso de una emergencia o catástrofe, es importante también que este documento sea revisado periódicamente.	

- A.8 Gestión de activos

Tabla 24.- *Gestión de activos – responsabilidad sobre los activos*

Elaborado por: *Investigador*

Política	***Análisis***					
A.8 Gestión de activos	***Sección***		8.1 Responsabilidad sobre los activos			
	Control de la ISO 27001		8.1.1	8.1.2	8.1.3	8.1.4
			Inventario de activos	Propiedad de los activos	Uso aceptable de los activos	Devolución de los activos
	Aplicabilidad	***Si***	X			
		No		X	X	X
	Justificación		La empresa ya cuenta con este apartado			

Tabla 25.- *Gestión de activos – clasificación de la información*

Elaborado por: *Investigador*

A.8 Gestión de activos	***Sección***		8.2 Clasificación de la información		
	Control de la ISO 27001		8.2.1 Clasificación de la información	8.2.2 Etiquetado de la información	8.2.3 Manipulado de la información
	Aplicabilidad	***Si***	X	X	X
		No			
	Justificación		Es necesario para que la información que se maneje en AMBACAR sea asegurada y para que se le dé una protección adecuada según la relevancia que tenga para la empresa.		

Tabla 26.- *Gestión de activos - manipulación de los soportes*

Elaborado por: *Investigador*

A.8 Gestión de activos	***Sección***		8.3 Manipulación de los soportes		
	Control de la ISO 27001		8.3.1	8.3.2	8.3.3
			Gestión de soportes extraíbles	Eliminación de soportes	Soportes físicos en tránsito
	Aplicabilidad	***Si***			
		No	X	X	X
	Justificación		La empresa ya cuenta con este apartado		

- A.9 Control de Acceso

Tabla 27.- *Control de Acceso- requisitos de negocio para el control de acceso*

Elaborado por: *Investigador*

<table>
<tr><td>Política</td><td colspan="3">Análisis</td></tr>
<tr><td rowspan="5">A.9 Control de acceso</td><td colspan="2">Sección</td><td colspan="2">A.9.1 Requisitos de negocio para el control de acceso</td></tr>
<tr><td colspan="2" rowspan="2">Control de la ISO 27001</td><td>9.1.1</td><td>9.1.2</td></tr>
<tr><td>Política de control de acceso</td><td>Acceso a las redes y a los servicios de red</td></tr>
<tr><td rowspan="2">Aplicabilidad</td><td>Si</td><td>X</td><td>X</td></tr>
<tr><td>No</td><td></td><td></td></tr>
<tr><td colspan="2">Justificación</td><td colspan="2">Es necesario para poder limitar el uso de las redes y servicios para un uso específico y de beneficio para la empresa</td></tr>
</table>

Tabla 28.- *Control de acceso - gestión de acceso de usuario*

Elaborado por: *Investigador*

Política	***Análisis***							
A.9 Control de acceso	***Sección***		A.9.2 Gestión de acceso de usuario					
	Control de la ISO 27001		9.2.1	9.2.2	9.2.3	9.2.4	9.2.5	9.2.6
			Registro y baja de usuario	Provisión de acceso de usuario	Gestión de privilegios de acceso	Gestión de la información secreta de autenticación de los usuarios	Revisión de los derechos de acceso de usuario	Retirada o reasignación de los derechos de acceso
	Aplicabilidad	***Si***	X	X	X	X	X	X
		No						
	Justificación		Es necesaria para evitar inconvenientes de acceso no autorizado lo cual elevará los niveles de seguridad de redes y servicios de la empresa.					

Tabla 29.- *Control de acceso - responsabilidades de usuario*

Elaborado por: *Investigador*

Política	***Análisis***		
A.9 Control de acceso	***Sección***		A.9.3 Responsabilidades del usuario
	Control de la ISO 27001		9.3.1
			Uso de la información secreta de autenticación
	Aplicabilidad	***Si***	X
		No	
	Justificación		Es necesaria esta política para salvaguardar la información de los usuarios y su autentificación y así evitar ingreso no deseado de otros usuarios.

Tabla 30.- *Control de acceso - control de acceso a sistemas y aplicaciones*

Elaborado por: *Investigador*

Política	***Análisis***						
A.9 Control de acceso	***Sección***		A.9.4 Control de acceso a sistemas y aplicaciones				
	Control de la ISO 27001		9.4.1	9.4.2	9.4.3	9.4.4	9.4.5
			Restricción del acceso a la información	Procedimientos seguros de inicio de sesión	Sistema de gestión de contraseñas	Uso de utilidades con privilegios del sistema	Control de acceso al código fuente de los programas
	Aplicabilidad	***Si***	X	X	X	X	X
		No					
	Justificación		Es necesario asiganar una o varias personas por parte del departamento de sistemas para qué pueda crear, restringir y controlar el manejo de contraseñas y accesos para la información de la empresa.				

- A.11 Seguridad física y del entorno

Tabla 31.- *Seguridad física y del entorno - áreas seguras*

Elaborado por: *Investigador*

Política	***Análisis***							
A.11 Seguridad física y del entorno	***Sección***		A.11.1 Áreas seguras					
	Control de la ISO 27001		A.11.1.1 Perímetro de seguridad física	A.11.1.2 Controles físicos de entrada	A.11.1.3 Seguridad de oficinas, despachos y recursos	A.11.1.4 Protección contra las amenazas externas y ambientales	A.11.1.5 El trabajo en áreas seguras	A.11.1.6 Áreas de carga y descarga
	Aplicabilidad	***Si***	X	X	X	X	X	X
		No						
	Justificación		Es necesario para mitigar el acceso no autorizado a la información y a los recursos que posee la empresa.					

Tabla 32.- *Seguridad física y del entorno - seguridad de los equipos*

Elaborado por: *Investigador*

Política	***Análisis***									
A.11 Seguridad física y del entorno	***Sección***		A.11.2 Seguridad de los equipos								
	Control de la ISO 27001		A.11.2.1 Emplazamiento y protección de equipos	A.11.2.2 Instalaciones de suministro	A.11.2.3 Seguridad del cableado	A.11.2.4 Mantenimiento de los equipos	A.11.2.5 Retirada de materiales propiedad de la empresa	A.11.2.6 Seguridad de los equipos fuera de las instalaciones	A.11.2.7 Reutilización o eliminación segura de equipos	A.11.2.8 Equipo de usuario desatendido	A.11.2.9 Política de puesto de trabajo despejado y pantalla limpia
	Aplicabilidad	***Si***	X	X	X	X	X	X	X	X	X
		No									
	Justificación		Es necesario para evitar que los activos de la empresa se vean comprometidos en perdias, daños o robos, asi tambien es necesario para la desactivación o interrupción de operaciones que la empresa este realizando.								

- A.12 Seguridad de las operaciones

Tabla 33.- *Seguridad de las operaciones - procedimientos y responsabilidades operacionales*

Elaborado por: *Investigador*

Política	***Análisis***					
A.12 Seguridad de las operaciones	***Sección***		A.12.1 Procedimientos y responsabilidades operacionales			
	Control de la ISO 27001		12.1.1	12.1.2	12.1.3	12.1.4
			Documentación de procedimientos operacionales	Gestión de cambios	Gestión de capacidades	Separación de los recursos de desarrollo, prueba y operación
	Aplicabilidad	***Si***				
		No	X	X	X	X
	Justificación		La empresa ya cuenta con este apartado			

Tabla 34.- *Seguridad de las operaciones - protección contra el software malicioso (malware)*

Elaborado por: *Investigador*

Política	***Análisis***		
A.12 Seguridad de las operaciones	***Sección***		A.12.2 Protección contra el software malicioso (malware)
	Control de la ISO 27001		12.2.1
			Controles contra el código malicioso
	Aplicabilidad	***Si***	X
		No	
	Justificación		Es necesaria esta política para la prevención y aseguramiento contra recursos protegidos contra malware

Tabla 35.- *Seguridad de las operaciones - copias de seguridad*

Elaborado por: *Investigador*

Política	***Análisis***		
A.12 Seguridad de las operaciones	***Sección***		A.12.3 Copias de seguridad
	Control de la ISO 27001		12.3.1 Copias de seguridad de la información
	Aplicabilidad	***Si***	X
		No	
	Justificación		Es necesaria para asegurar la información y evitar la pérdida de datos de la empresa.

Tabla 36.- *Seguridad de las operaciones - registros y supervisión*

Elaborado por: *Investigador*

Política	***Análisis***					
A.12 Seguridad de las operaciones	***Sección***		A.12.4 Registros y supervisión			
	Control de la ISO 27001		12.4.1 Registro de eventos	12.4.2 Protección de la información del registro	12.4.3 Registros de administración y operación	12.4.4 Sincronización del reloj
	Aplicabilidad	***Si***				
		No	X	X	X	X
	Justificación		La empresa ya cuenta con este apartado			

Tabla 37.- *Seguridad de las operaciones - control de software en explotación*

Elaborado por: *Investigador*

Política	***Análisis***		
A.12 Seguridad de las operaciones	***Sección***		A.12.5 Control del software en explotación
	Control de la ISO 27001		12.5.1
			Instalación del software en explotación
	Aplicabilidad	***Si***	
		No	X
	Justificación		La empresa ya cuenta con este apartado

Tabla 38.- *Seguridad de las operaciones - gestión de la vulnerabilidad técnica*

Elaborado por: *Investigador*

Política	***Análisis***			
A.12 Seguridad de las operaciones	***Sección***		A.12.6 Gestión de la vulnerabilidad técnica	
	Control de la ISO 27001		12.6.1	12.6.2
			Gestión de las vulnerabilidades técnicas	Restricción en la instalación de software
	Aplicabilidad	***Si***	X	X
		No		
	Justificación		Es necesaria para reducir y mitigar en su totalidad riesgos de vulnerabilidades de explotación técnicas.	

Tabla 39.- *Seguridad de las operaciones - consideraciones sobre la auditoría de sistemas de la información*

Elaborado por: *Investigador*

Política	***Análisis***		
A.12 Seguridad de las operaciones	***Sección***		A.12.7 Consideraciones sobre la auditoria de sistemas de información
	Control de la ISO 27001		12.7.1
			Controles de auditoria de sistemas de información
	Aplicabilidad	***Si***	
		No	X
	Justificación		La empresa ya cuenta con este apartado

- A.13 Seguridad de las comunicaciones

Tabla 40.- *Seguridad de las comunicaciones - gestión de la seguridad de las redes*

Elaborado por: *Investigador*

Política	***Análisis***				
A.13 Seguridad de las comunicaciones	***Sección***		A.13.1 Gestión de la seguridad de las redes		
	Control de la ISO 27001		13.1.1 Controles de red	13.1.2 Seguridad de los servicios de red	13.1.3 Segregación en redes
	Aplicabilidad	***Si***	X	X	X
		No			
	Justificación		Es necesaria para que los activos, recursos y redes tenga un tratamiento adecuado y la información sea asegurada.		

Tabla 41.- *Seguridad de las comunicaciones - intercambio de la información*

Elaborado por: *Investigador*

Política	***Análisis***					
A.13 Seguridad de las comunicaciones	***Sección***		A.13.2 Intercambio de información			
	Control de la ISO 27001		13.2.1	13.2.2	13.2.3	13.2.4
			Políticas y procedimientos de intercambio de información	Acuerdos de intercambio de información	Mensajería electrónica	Acuerdos de confidencialidad o no revelación
	Aplicabilidad	***Si***				
		No	X	X	X	X
	Justificación		La empresa ya cuenta con este apartado			

Analizado y justificado cada uno de los controles de la empresa AMBACAR se procese a porcentualizar el cumplimiento de estos controles con el objetivo de visualizar el cumplimiento de los mismo y así poder realizar la propuesta de mejora para mencionados controles que se manejan.

4.3.5. Análisis de cumplimiento de controles

La valoración de los controles se lo realizó de manera porcentual conjuntamente con el Ing. Byron Jiménez encargado del departamento de redes y seguridad de la información de la empresa AMBACAR.

Se elaboró la gráfica de cumplimiento para cada área en la que se detalla los porcentajes obtenidos, además se detalla los controles y como se encuentra al momento de la revisión, esto se lo realizó con cada una de las áreas relevantes para AMBACAR.

A.5 Políticas de seguridad de la información

A.5.1 Directrices de gestión de la seguridad de la información

- ***A.5.1.1 Políticas para la seguridad de la información***

AMBACAR carece de la documentación de políticas de seguridad de la información, sin embargo, así se lleven a cabo los diferentes procesos para salvaguardar información, únicamente se aplican ciertas normativas básicas, por lo tanto, no se garantiza una total seguridad de información.

Es primordial establecer políticas de seguridad, las cuales deberán ser documentas y socializadas con el personal de la empresa, además se debe analizar el establecimiento de sanciones al personal que incumpla con las políticas establecidas, dicho documento deberá realizarse en conjunto por el departamento de Tecnologías de la Información y la Gerencia.

- ***A.5.1.2 Revisión de las políticas para la seguridad de la información***

AMBACAR al carecer de un documento de políticas de seguridad como se mencionó en el control anterior, por esta razón no se puede tener una revisión de las políticas de seguridad.

Una vez definidas y documentadas las políticas de seguridad, el departamento de tecnologías conjuntamente con la gerencia debe comprometerse a realizar un monitoreo periódico con el fin de avalar la efectividad y de igual manera hacer un proceso de examinación de las políticas definidas para que se cumplan sin objeción alguna.

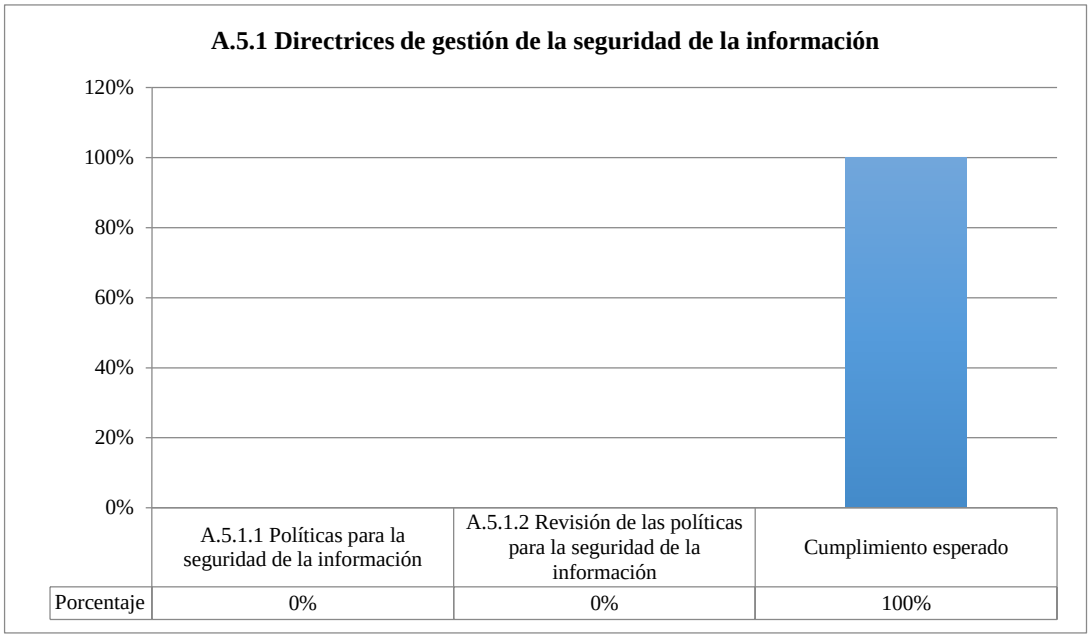


Fig. 24.- *Análisis porcentual - directrices de gestión de la seguridad de la información*

Elaborado por: *Investigador*

A.8 Gestión de activos

A.8.2 Clasificación de la información

- ***A.8.2.1 Clasificación de la información***

TECNOLOGÍA DE LA INFORMACIÓN - AMBACAR es el encargado de llevar la clasificación y gestión de activos de la empresa, dicho departamento es el encargado de asignar el nivel de importancia para la organización de la información, así como también el nivel adecuado de protección de acuerdo al rol y usuario asignados.

- ***A.8.2.2 Etiquetado de la información***

TECNOLOGÍA DE LA INFORMACIÓN - AMBACAR es el encargado de realizar el etiquetado adecuado para la clasificación y gestión de activos de la empresa, dicho departamento es el encargado de asignar la etiqueta de acuerdo al esquema de clasificación adoptado por le empresa.

- ***A.8.2.3 Manipulación de la información***

TECNOLOGÍA DE LA INFORMACIÓN - AMBACAR es el encargado de realizar los procedimientos de control para el manejo y manipulación de la información, de acuerdo a la clasificación adoptada por la empresa.

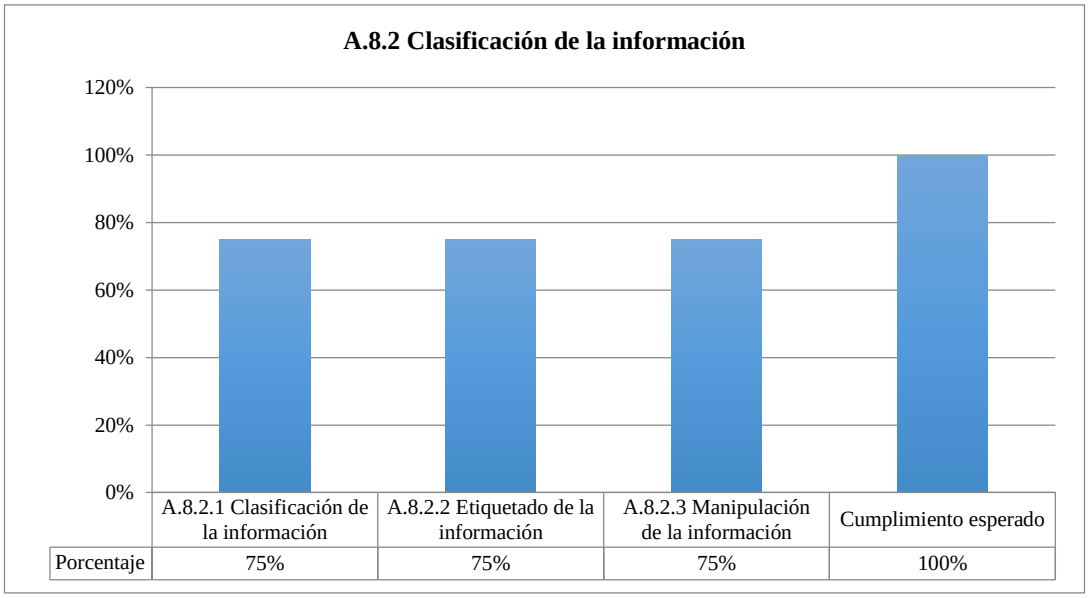


Fig. 25.- *Análisis porcentual - clasificación de la información*

Elaborado por: *Investigador*

A.9 Control de Acceso

A.9.1 Requisitos de negocio para el control de acceso

- ***A.9.1.1 Política de control de acceso***

AMBACAR carece de la documentación de políticas de control de acceso a la información, sin embargo, así se lleven a cabo los diferentes procesos para salvaguardar el acceso de información, únicamente se aplican ciertas normativas básicas, por lo tanto, no se garantiza un control total de acceso a la información.

- ***A.9.1.2 Acceso a las redes y a los servicios de red***

TECNOLOGÍA DE LA INFORMACIÓN - AMBACAR es el encargado de proporcionar las redes de acceso y servicios de la información conforme la autorización de acceso previa.

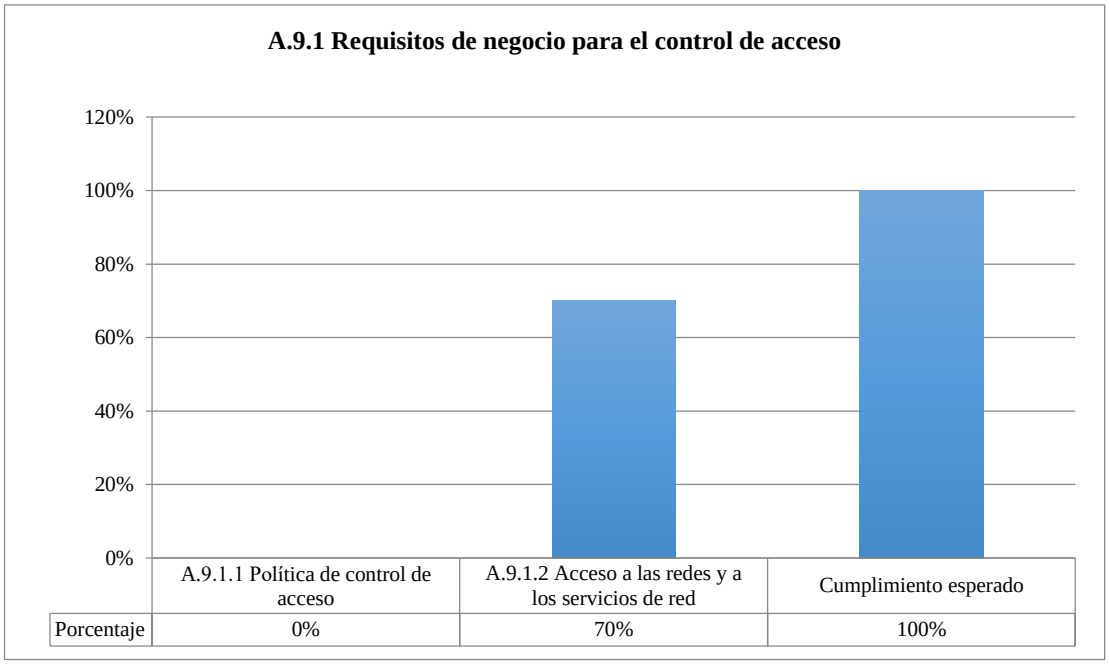


Fig. 26.- *Análisis porcentual - requisitos de negocio para el control de acceso*

Elaborado por: *Investigador*

A.9.2 Gestión *de* acceso de usuario

- ***A.9.2.1 Registro y baja de usuario***

TECNOLOGÍA DE LA INFORMACIÓN - AMBACAR es el encargado realizar los procesos de asignación de usuarios para el registro y retirada de los mismos, generando los permisos correspondientes de los derechos de acceso.

- ***A.9.2.2 Provisión de acceso de usuario***

TECNOLOGÍA DE LA INFORMACIÓN - AMBACAR es el encargado realizar los procesos de revocación de derechos de acceso a la información a todo tipo de usuarios, generando las prohibiciones pertinentes de acceso a todos los sistemas y servicios de la empresa.

- ***A.9.2.3 Gestión de privilegios de acceso***

TECNOLOGÍA DE LA INFORMACIÓN - AMBACAR es el encargado de realizar el control restringido, así como también la asignación y el uso de privilegios de acceso a la información.

- ***A.9.2.4 Gestión de la información secreta de autenticación de los usuarios***

AMBACAR no posee un proceso formal de autenticación de la información secreta. Por tanto, se debería implantar procesos de asignación de usuarios para el registro y

retirada de los mismos, generando los permisos correspondientes de los derechos de acceso.

A.9.2.5 Revisión de los derechos de acceso de usuario

TECNOLOGÍA DE LA INFORMACIÓN - AMBACAR es el encargado de revisar los derechos de acceso de los usuarios en períodos de seguimiento regulares, procurando precautelar la seguridad de acceso de los usuarios.

- ***A.9.2.6 Retirada o reasignación de los derechos de acceso***

TECNOLOGÍA DE LA INFORMACIÓN - AMBACAR es el encargado realizar los procesos de retiro o finalización de derechos de acceso a la información a los usuarios una vez terminado el empleo, contrato, acuerdo o cambio.

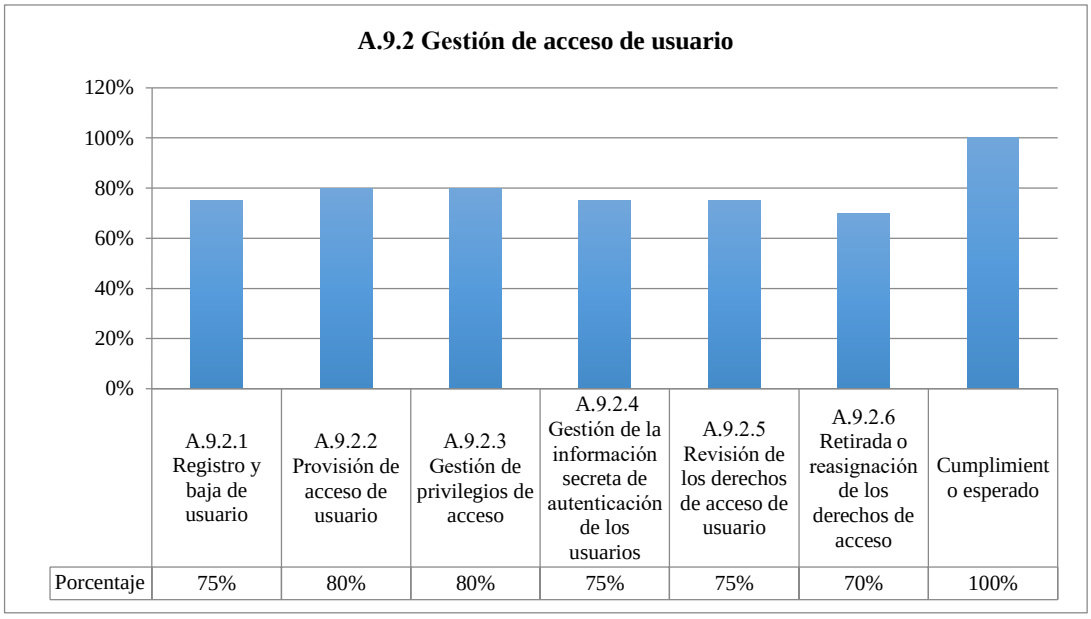


Fig. 27.- *Análisis porcentual - gestión de acceso de usuario*

Elaborado por: *Investigador*

A.9.3 Responsabilidades del usuario

- ***A.9.3.1 Uso de la información secreta de autenticación***

TECNOLOGÍA DE LA INFORMACIÓN - AMBACAR mantiene un proceso de control hacia el personal para seguir adecuadamente las prácticas de organización de información secreta, precautelando la autenticación de los usuarios.

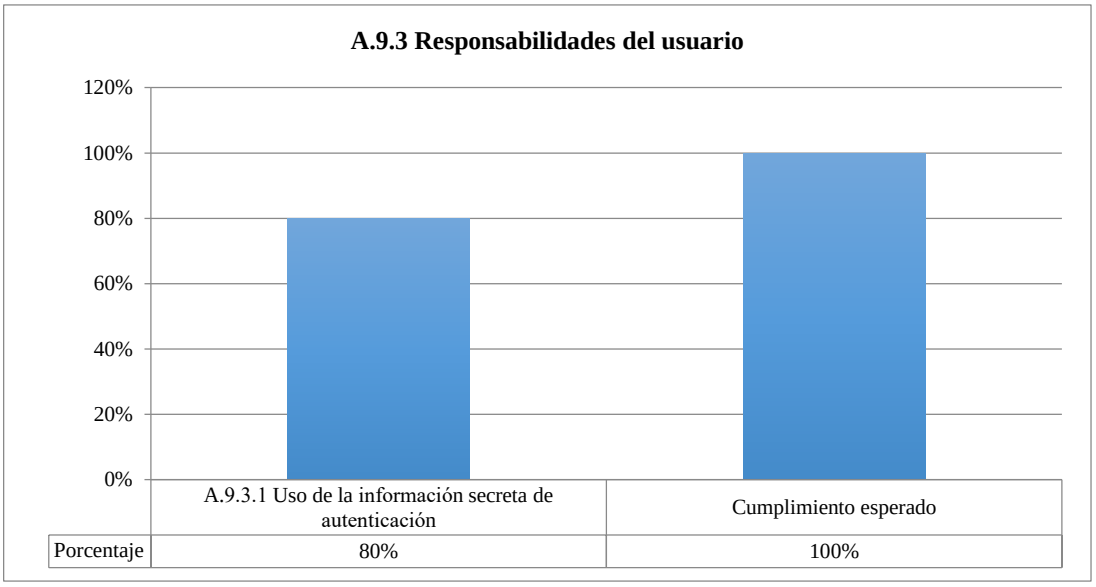


Fig. 28.- *Análisis porcentual - responsabilidades del usuario*

Elaborado por: *Investigador*

A.9.4 *Control* de acceso a sistemas y aplicaciones

- ***A.9.4.1 Restricción del acceso a la información***

AMBACAR carece de la documentación de políticas de restricción de acceso a la información, sin embargo, así se lleven a cabo los diferentes procesos para salvaguardar el acceso de información, únicamente se aplican ciertas normativas básicas, por lo tanto, no se garantiza un control total de acceso a la información.

- ***A.9.4.2 Procedimientos seguros de inicio de sesión***

AMBACAR carece de la documentación de procedimientos seguros de inicio de sesión a la información, sin embargo, así se lleven a cabo los diferentes procesos para salvaguardar el inicio de sesión de información, únicamente se aplican ciertas normativas básicas, por lo tanto, no se garantiza un control total de inicio de sesión seguro a la información.

- ***A.9.4.3 Sistema de gestión de contraseñas***

TECNOLOGÍA DE LA INFORMACIÓN - AMBACAR lleva a cabo los procesos de generación o cambios de contraseña de los usuarios, verificando que las mismas contengan un nivel de seguridad óptimo, evitando el ingreso inadecuando de usuarios no autorizados.

- ***A.9.4.4 Uso de utilidades con privilegios del sistema***

TECNOLOGÍA DE LA INFORMACIÓN - AMBACAR controla el proceso de acceso a la información a través de roles y usuarios, para tener el privilegio de acceso pertinente según su importancia en la empresa.

- ***A.9.4.5 Control de acceso al código fuente de los programas***

TECNOLOGÍA DE LA INFORMACIÓN - AMBACAR establece las restricciones de acceso a los códigos fuente de los programas, para manejo confiable de información de desarrollo de software, teniendo en cuenta que el código fuente del sistema principal es contratado a empresas terciarias.

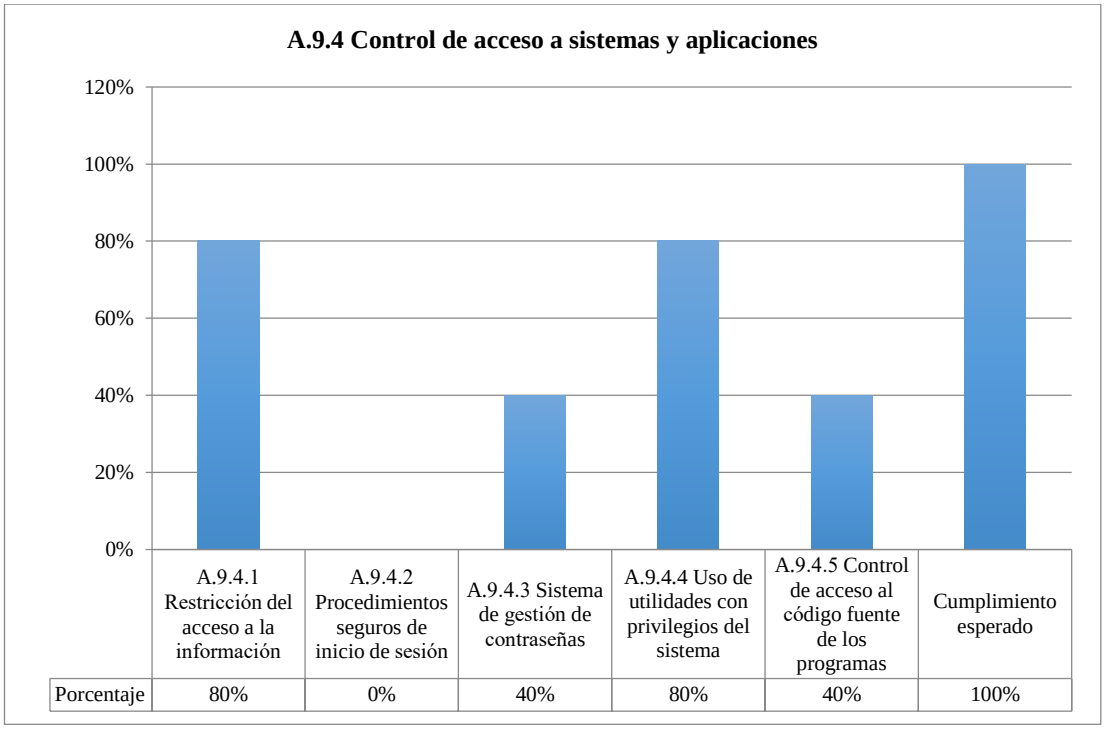


Fig. 29.- *Análisis porcentual - control de acceso a sistemas y aplicaciones*

Elaborado por: *Investigador*

A.11 Seguridad física y del entorno

A.11.1 Áreas seguras

- ***A.11.1.1 Perímetro de seguridad física***

  AMBACAR posee un área de seguridad compuesta por implementos de infraestructura básicos, por lo cual no asegura la protección completa de la información. Por tanto, se debería implementar un sistema de seguridad biométrico para precautelar el acceso a las áreas que contienen la información sensible de la empresa.

- ***A.11.1.2 Controles físicos de entrada***

AMBACAR posee controles físicos de entrada compuesta por implementos de infraestructura básicos, por lo cual no asegura la protección completa de la información. Por tanto, se debería implantar un diagrama de emplazamiento y protección de equipos en donde se detalle plenamente las ubicaciones de cada uno de los equipos y sus protecciones respectivas, para evitar riesgos y amenazas en sus empleados.

- ***A.11.1.3 Seguridad de oficinas, despachos y recursos***

AMBACAR posee la seguridad en un 80% en oficinas, despachos y recursos; sin embargo, no se mantiene este nivel de seguridad en los servidores debido a falta de un control de acceso ya sea biométrico, etc., donde se sustente la seguridad de la información.

- ***A.11.1.4 Protección contra las amenazas externas y ambientales***

AMBACAR, cuenta con protección para amenazas externas y ambientales, sin embargo, se debería instaurar estructuras sismo resistentes, así como también un sistema de monitoreo de seguridad con sensores para agilizar los procesos de evacuación o protección del personal y de la información.

- ***A.11.1.5 El trabajo en áreas seguras***

AMBACAR, cuenta con los procedimientos necesarios para trabajar en áreas seguras, precautelando la seguridad de los trabadores de la empresa

.

- **A.11.1.6 *Áreas* de carga y descarga**

AMBACAR, debería adecuar un espacio de carga y descarga adecuado a las necesidades de la empresa, en el cual se pueda desarrollar procesos seguros de almacenamiento de equipos de la empresa.

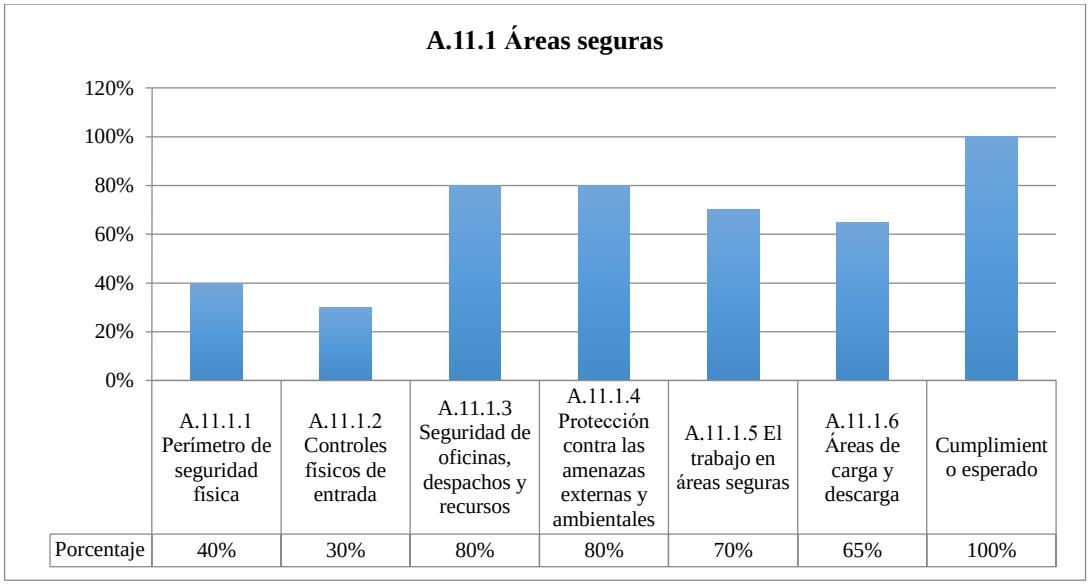


Fig. 30.- *Análisis porcentual - áreas seguras*

Elaborado por: *Investigador*

A.11.2 Seguridad de los equipos

- ***A.11.2.1 Emplazamiento y protección de equipos***

AMBACAR únicamente cuenta con un registro en donde se detallan los equipos con sus locaciones respectivas. El espacio no cuenta con la seguridad necesaria para el ingreso solo de personal autorizado.

- ***A.11.2.2 Instalaciones de suministro***

AMBACAR no posee protecciones adecuadas contra fallos de alimentación de energía eléctrica, debido a esto el generador no funciona a causa de la falta de mantenimiento.

Por otra parte, las herramientas de comunicación de la institución son: telefonía pagada con la empresa CNT quien además provee del servicio de internet de la misma manera se cuenta con Voz IP lo que permite la comunicación interna del personal.

- ***A.11.2.3 Seguridad del cableado***

AMBACAR cuenta con un cableado adecuado en cuanto a conexiones eléctricas y de telecomunicaciones, para proteger los servicios informáticos frente a interceptaciones, interferencias o daños.

La empresa utiliza cable UTP categoría 6 con conectores RJ45 para el cableado de datos, el cableado se preserva a través de las canaletas que son adecuadas correctamente dentro de AMBACAR para que no dificulten ni suspendan las actividades del personal.

- ***A.11.2.4 Mantenimiento de los equipos***

AMBACAR a través del departamento de tecnologías de la información realiza un proceso continuo de mantenimiento de activos para asegurar la disponibilidad e integridad de la información y activos de la empresa, generando así una confiabilidad del 85% de su mantenimiento general.

Los equipos que lleguen a mantenimiento y soporte técnico del Departamento del Tecnologías de la Información deberán ser revisados de manera meticulosa, primero se hace una limpieza general de los equipos, una vez realizada la limpieza del equipo se procede a revisar el software entre los cuales se examina: antivirus, licencias, actualizaciones de Windows Update y revisión general de las aplicaciones que se utilicen en AMBACAR.

- ***A.11.2.5 Retirada de materiales propiedad de la empresa***

TECNOLOGÍA DE LA INFORMACIÓN AMBACAR, realiza el proceso protocolario en el cual se establecen los requisitos y procedimientos necesarios para retirar información o software de las instalaciones de la empresa.

- ***A.11.2.6 Seguridad de los equipos fuera de las instalaciones***

AMBACAR cuenta con las metodologías y medidas de control para el uso adecuado de los equipos que son de uso externo a las instalaciones de la organización, precautelando la seguridad de sus empleados y de los activos utilizados en las diferentes áreas.

En caso de presentarse un incidente con el activo informático el responsable se verá en la obligación de comunicar inmediatamente a la gerencia para tomar las medidas correctivas.

- ***A.11.2.7 Reutilización o eliminación segura de equipos***

AMBACAR realiza todos los procesos de soporte de almacenamiento para información sensible de la empresa a través del departamento de contabilidad. De esta manera, se mantienen los procedimientos seguros de eliminación de información.

- ***A.11.2.8 Equipo de usuario desatendido***

AMBACAR tiene procesos ordenados para precautelar un mantenimiento eficiente de hardware y software de la empresa, por lo cual es casi imposible que un equipo esté desatendido; sin embargo, se debería llevar periódicamente un registro de atención de equipos para evitar futuras complicaciones.

- ***A.11.2.9 Política de puesto de trabajo despejado y pantalla limpia***

AMBACAR, no realiza un proceso exhaustivo de control de puesto de trabajo despejado y pantalla limpia. Por tanto, se debería proceder a implementar procesos de control más a menudo para evitar la acumulación de material inservible en el puesto de trabajo de los empleados, así como también, de la información digital en sus ordenadores.

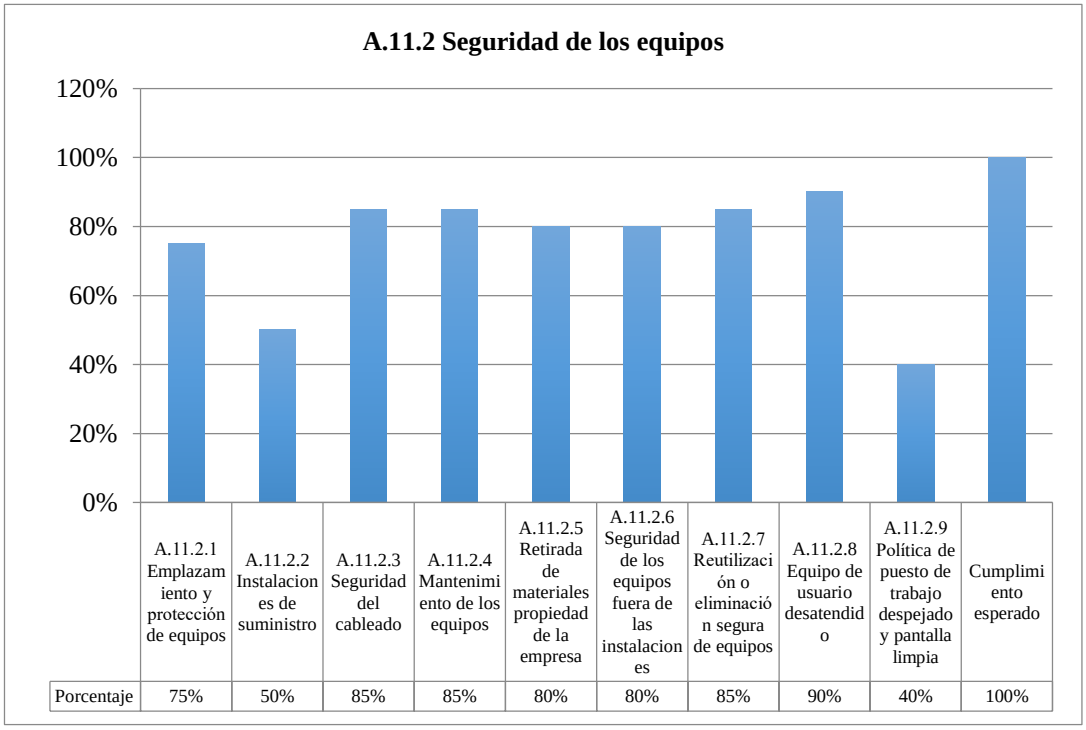


Fig. 31.- *Análisis porcentual - seguridad de los equipos*

Elaborado por: *Investigador*

A.12 Seguridad de las operaciones

A.12.2 Protección contra el software malicioso (malware)

- ***A.12.2.1 Controles contra el código malicioso***

TECNOLOGÍA DE LA INFORMACIÓN AMBACAR, asegura de manera eficaz el tratamiento de los recursos informáticos contra software malicioso en el sistema informativo de la empresa, implementando controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.

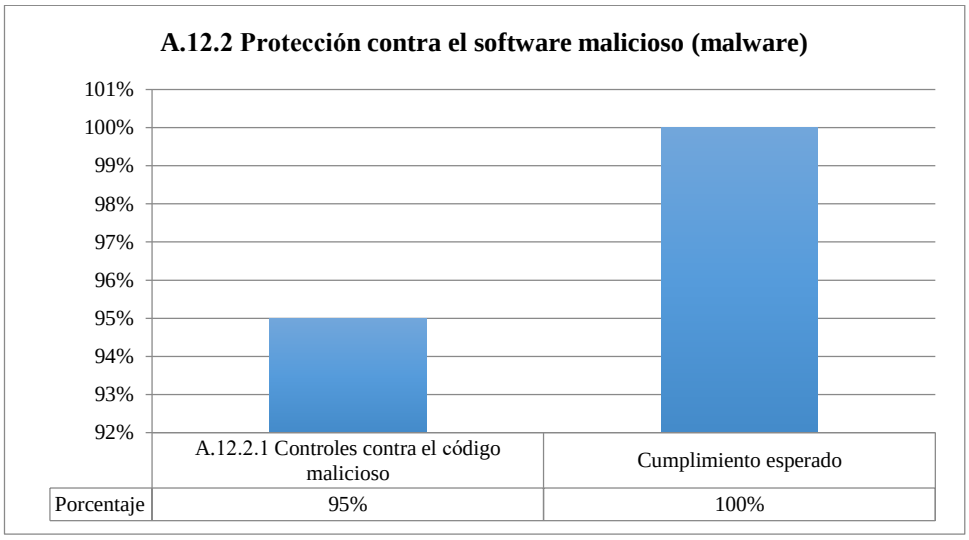


Fig. 32.- *Análisis porcentual - protección contra el software malicioso (malware)*

Elaborado por: *Investigador*

A.12.3 Copias de seguridad

- ***A.12.3.1 Copias de seguridad de la información***

TECNOLOGÍA DE LA INFORMACIÓN AMBACAR, realiza un proceso de archivo semanal con un backup propio, y de los demás archivos lo realiza en períodos definidos de tiempo.

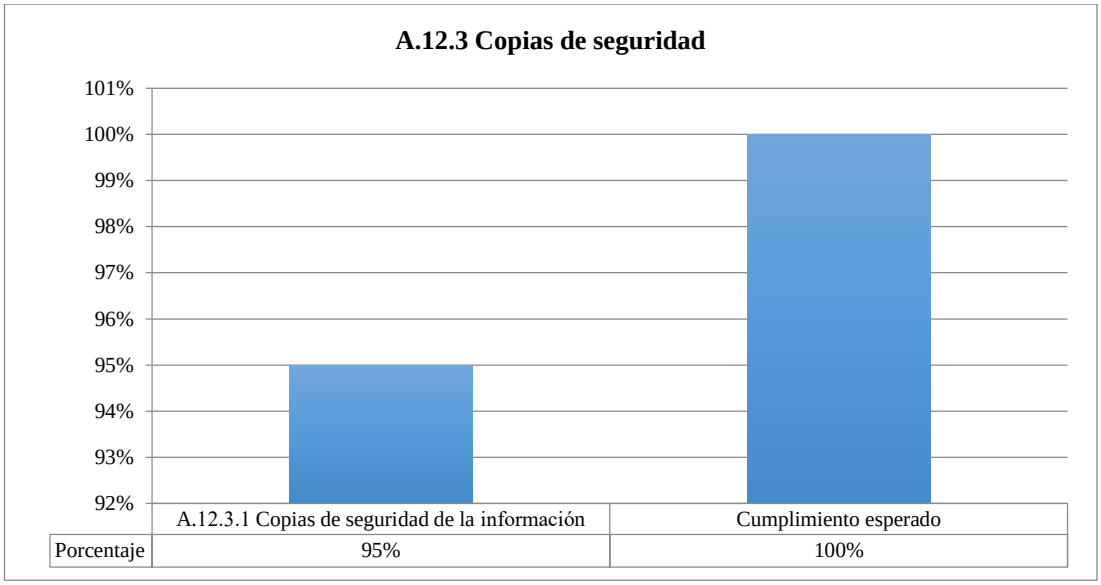


Fig. 33.- *Análisis porcentual - copias de seguridad*

Elaborado por: *Investigador*

A.12.6 Gestión de la vulnerabilidad técnica

- ***A.12.6.1 Gestión de las vulnerabilidades técnicas***

TECNOLOGÍA DE LA INFORMACIÓN AMBACAR, realiza la revisión de vulnerabilidad en un 60% debido a que es una empresa internacional, pero no existe un control periódico de tiempo para realizar estas vulnerabilidades. Por tanto, de debería procurar realizar un proceso de control de vulnerabilidad periódico para evaluar la exposición de la organización y adoptar las medidas adecuadas para afrontar el riesgo asociado.

- ***A.12.6.2 Restricción en la instalación de software***

TECNOLOGÍA DE LA INFORMACIÓN AMBACAR, no posee restricciones para instalaciones en las máquinas de los equipos. Por lo cual, se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.

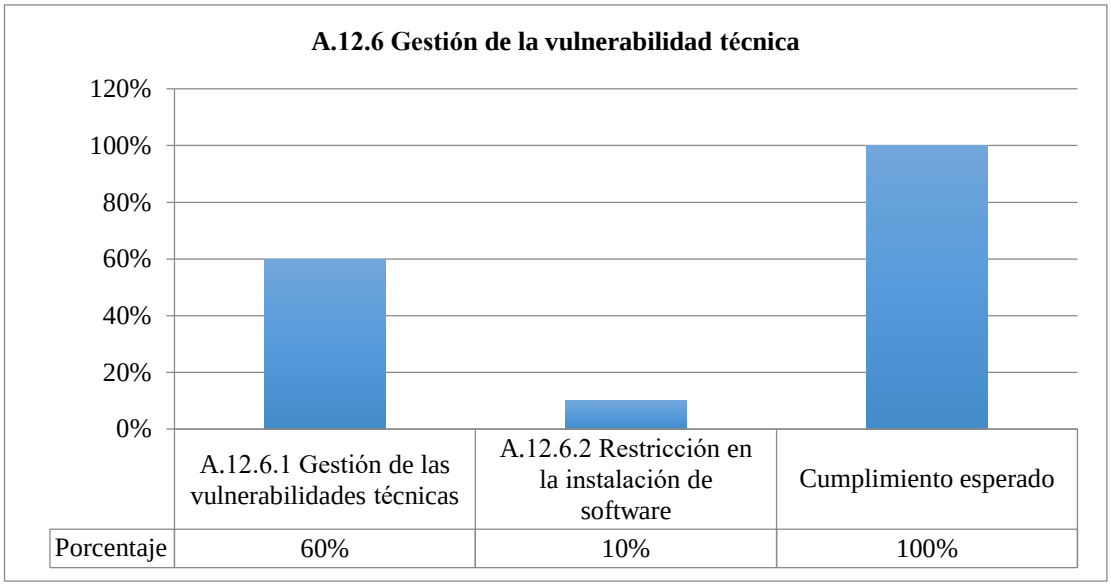


Fig. 34.- *Análisis porcentual - gestión de la vulnerabilidad técnica*

Elaborado por: *Investigador*

A.13 Seguridad de las comunicaciones

A.13.1 Gestión de la seguridad de las redes

- **A.13.1.1 Controles de red**

AMBACAR mediante el departamento de sistemas se encarga del control y gestión de sistemas y aplicaciones, sin embargo, la seguridad no cuenta con un control definido y seguridad de la información lo que conlleva a que puede sufrir robo de información, ataques a sus equipos, programas y sistemas.

- **A.13.1.2 Seguridad de los servicios de red**

AMBACAR al tener el departamento de sistemas en la matriz-Ambato se encarga de toda la administración de los servicios de red a las sucursales de todo el país, en este caso la persona encargada al tener sucursales en diferentes lados para enterarse o solucionar los problemas pertinentes debe esperar que la sucursal realice el llamado mediante vía telefónica y así poder solucionar le problema.

- ***A.13.1.3 Segregación en redes***

AMBACAR en cada sucursal qué posee se la trata como una red diferente, la seguridad se la realiza mediante roles y usuarios asignándole los privilegios pertinentes para proteger la información la cual es almacenada el cada servidor predestinado. Se debe

tener un manual o documento de asignación de roles, usuarios y privilegios asignados al personal de la empresa con el fin de prevención en caso de filtración o robo de información.

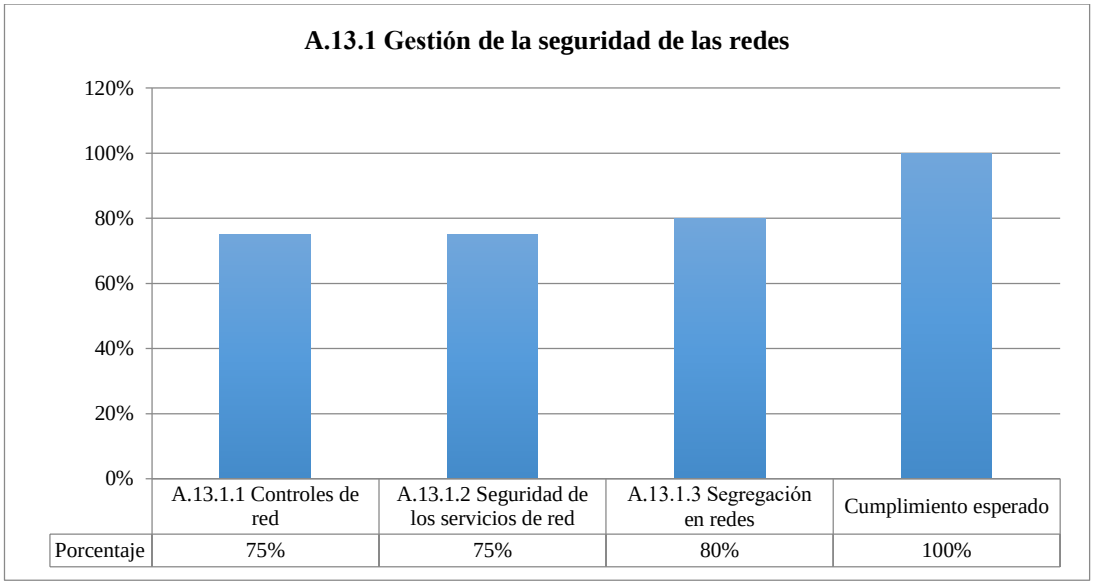


Fig. 35.- *Análisis porcentual - gestión de la seguridad de las redes*

Elaborado por: *Investigador*

A.13.2 Intercambio de información

- ***A.13.2.1 Políticas y procedimientos de intercambio de información***

AMBACAR carece de la documentación de políticas de intercambio de información, sin embargo, procedimientos a seguir en el caso de intercambio de información esencial de la empresa si posee y se rigen mediante dichos procedimientos. Se debe instaurar un manual de políticas de intercambio de información, mismo que deberá ser socializado con todo el personal de AMBACAR y documentado por el organismo de tecnologías de la información de la empresa.

- ***A.13.2.2 Acuerdos de intercambio de información***

AMBACAR si cuenta con acuerdos y procedimientos de intercambio de seguridad de información debido a que comparte información de repuestos con Automekano y Siauto, lo que se debe tener en cuenta es que tienen información compartida debido a las políticas de trabajo entre ellas y que los servidores son compartidos. Se debe tratar de manejar la información en los propios servidores de cada empresa para así disminuir el riesgo de robo de información.

- ***A.13.2.3 Mensajería electrónica***

AMBACAR cuenta con un servicio de protección alto en este sentido ya que trabaja mediante la G Suit de google la cual cuenta con un servicio de administración y un número ilimitado en el buzón de correo y da un espacio de almacenamiento de 20gb en sus servicios adicionales, pero se debe tener en cuenta que al ser un servicio basado completamente en web puede ser vulnerado o tener complicaciones de robo de información.

- ***A.13.2.4 Acuerdos de confidencialidad o no revelación***

AMBACAR no cuenta con un documento formal de acuerdos de confidencialidad o no revelación, pero si cuenta con pasos o procesos a seguir en el caso de revelación de información debido a que al trabajar con Automekano y Siauto necesitan información en el área de repuestos, etc.

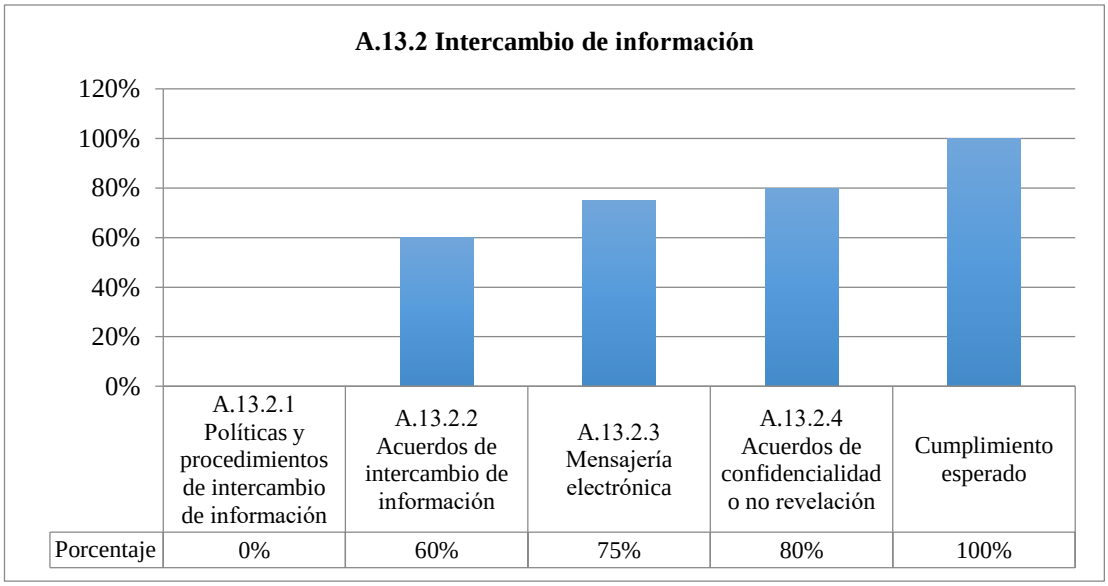


Fig. 36.- *Análisis porcentual - intercambio de información*

Elaborado por: *Investigador*

4.2.6. Políticas y controles establecidos para la seguridad de la información de AMBACAR

Una vez realizado el análisis de los controles aplicables con respecto a la norma IS0 27001, y tomando en cuenta cada uno de los escenarios presentes en AMBACAR para desarrollar sus actividades, se determinó que existen altos índices de probabilidad de que ocurran incidentes relacionados con la seguridad de la información de la empresa.

Por ende, es necesario establecer políticas de seguridad de la información, mismas que deberán ser elaboradas de manera coherente, concisas y dentro de los límites de cumplimiento empresarial, cuyo fin será proporcionar una guía que gestione adecuadamente la seguridad de la información.

A continuación, se definirán políticas que satisfagan las necesidades requeridas en las diferentes áreas de AMBACAR, como son la organizacional, física, lógica y legal en lo referente al manejo adecuado de la seguridad de la información.

Seguridad Organizacional

Se desarrollará un cuadro formal a través del cual se administrará la empresa incluyendo la gestión de activos, físicos, actividades complementarias, etc. Dicho documento estará enfocado a circunstancias que circunden la seguridad de la información.

Seguridad Lógica

Se establecerán normativas para la gestión de control de acceso por parte del personal de AMBACAR en el equipo informático, dichas normas evitarán alteraciones en la configuración de los mismos, de igual manera se establecerán normativas que permitan controlar vulnerabilidades a causa de software malicioso.

Seguridad Física

Se establecerán controles relacionados con el mantenimiento y soporte de equipos, además se precisarán limites en referencia a los perímetros de seguridad de AMBACAR.

Seguridad Legal

Se definirán políticas y normas de seguridad bajo el reglamento interno de AMBACAR, con el propósito de garantizar el cumplimiento de los mismos. Además, se puntualizarán las sanciones pertinentes al personal que no lleve un cumplimiento total de dichas normas y pongan en riesgo la seguridad de la información.

A.5 Políticas de seguridad de la información

A.5.1 Directrices de gestión de la seguridad de la información

Objetivo:

“Proporcionar orientación y apoyo a la gestión de la seguridad de la información de AMBACAR de acuerdo con los requisitos de la empresa, las leyes y normativa pertinentes”.

- Se instaurará un manual de políticas de seguridad, mismo que deberá ser socializado con todo el personal de AMBACAR.
- Se documentará el manual de políticas de seguridad de la información por el organismo de tecnologías de la información de la empresa.
- Se realizará el documento de políticas de seguridad de la información para luego ser revisado por el organismo pertinente
- Se requerirá que el documento tenga un régimen de revisión de un determinado período de tiempo.

A.8 Gestión de activos

A.8.2 Clasificación de la información

Objetivo:

“Asegurar que la información de AMBACAR reciba un nivel adecuado de protección de acuerdo con su importancia para la organización”.

- La información se clasificará en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas desde la gerencia de la empresa.
- Se adoptará un etiquetado pertinente acorde a los procedimientos y esquemas adoptados para la manipulación de la información dentro de AMBACAR.

A.9 Control de Acceso

A.9.1 Requisitos de negocio para el control de acceso

Objetivo:

"Limitar el acceso a los recursos de tratamiento de la información y a la información de AMBACAR".

- Se instaurará un manual de políticas de acceso a la información, mismo que deberá ser socializado con todo el personal de AMBACAR y documentado por el organismo de tecnologías de la información de la empresa.
- Se proporcionará a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados desde la gerencia de AMBACAR.

A.9.2 Gestión *de* acceso de usuario

Objetivo:

"Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios de AMBACAR".

- Se establecerá un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso, revocación de derechos de acceso y asignación de privilegios de acceso a la información de AMBACAR
- Se implantará procesos de asignación de usuarios para el registro y retirada de los mismos, generando los permisos correspondientes de los derechos de acceso de la empresa.
- Se asignará un control de derechos de acceso a los empleados y terceras partes que se inmiscuyan en AMBACAR, así como también a los recursos de tratamiento de la información en caso de cese de funciones, culminación de contratos o cambios realizados en la empresa.

A.9.3 Responsabilidades del usuario

Objetivo:

"Para que los usuarios se hagan responsables de salvaguardar la información de autenticación en AMBACAR".

- Se implantará control a los usuarios para el seguimiento ordenado de las prácticas de AMBACAR en el uso de la información secreta de autenticación.

A.9.4 *Control* de acceso a sistemas y aplicaciones

Objetivo:

"Prevenir el acceso no autorizado a los sistemas y aplicaciones de AMBACAR".

- Se instaurará un manual de inicio de sesión seguro a la información, mismo que deberá ser socializado con todo el personal de AMBACAR y documentado por el organismo de tecnologías de la información de la empresa.
- Se implementará un proceso seguro de utilización de contraseñas seguras y confiables, para salvaguardar la información, restringiendo el código fuente de los programas de la empresa.

A.11 Seguridad física y del entorno

A.11.1 Áreas seguras

Objetivo:

"Prevenir el acceso físico no autorizado, los daños e interferencias a la información de AMBACAR y a los recursos de tratamiento de la información".

- Se deberá implementar un sistema de seguridad biométrico para precautelar el control de acceso físico para el ingreso de personal autorizado a la información, protegiendo además las áreas que contengan información sensible y los recursos de tratamiento de la información.
- Se adecuará un sistema de control de ingreso a las oficias, despachos y recursos con un adecuado sistema de prevención de riesgos frente a desastres naturales o accidentes, inmiscuyendo las áreas de carga y descarga de recursos para salvaguardad la integridad física de los trabajadores de la empresa.

A.11.2 Seguridad de los equipos

Objetivo:

"Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de AMBACAR".

- Se implementará un proceso de mantenimiento periódico al generador de la empresa, para precautelar el uso y vida útil de los equipos que funciones con alimentación de energía eléctrica.
- Se realizará un proceso de mantenimiento de 6 veces anuales distribuidas en 6 bimestres, para precautelar el buen funcionamiento de activos e información y cubrir un mayor rango de confiabilidad porcentual de este control.
- La manipulación física y/o intervención a los activos informáticos estará a cargo del departamento de tecnologías de la información, queda prohibida la manipulación por parte de los usuarios sin previa autorización en caso de ser requerida la intervención de personas no pertenecientes al departamento de tecnologías de la información.
- El personal de infraestructura del departamento de tecnologías de la información será el encargado de velar por la seguridad de los equipos tecnológicos, de presentarse eventualidades imprevistas se realizar un documento en el cual se detallen todos los problemas con el fin de solucionarlo de la manera segura, pronta y eficaz.
- Se establecerá un plan de mejora continua en el manejo de información en pantalla limpia, con el objetivo de precautelar la información relevante de AMBACAR.

A.12 Seguridad de las operaciones

A.12.2 Protección contra el software malicioso (malware)

Objetivo:

"Asegurar que los recursos de tratamiento de información y la información de AMBACAR están protegidos contra malware".

- Se deberá mantener actualizado el antivirus tanto para servidores como para los equipos de cada usuario perteneciente a la empresa, mismo que deberá brindar protección en tiempo real y será actualizado constantemente.
- Se deberá aplicar normativas de restricción que denieguen el tráfico a través de la red y se habilitará el tráfico exclusivamente para los servicios se requieran.
- Se deberá realizar controles constantes ante eventualidades en la red, mismos que deberán tener respuestas rápidas permanentes y eficaces.
- Se deberá realizar los respaldos o backups necesarios en períodos de tiempo determinados con los componentes óptimos para almacenamiento de los respaldos de la información.

A.12.6 Gestión de la vulnerabilidad técnica

Objetivo:

"Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas de AMBACAR".

- Se desarrollará un procedimiento adecuado para establecer y aplicar reglas de instalación de software seguro por parte de los trabajadores de AMBACAR.

A.13 Seguridad de las comunicaciones

A.13.1 Gestión de la seguridad de las redes

Objetivo:

"Asegurar la protección de la información en las redes y los recursos de tratamiento de la información de AMBACAR".

- Se gestionará la información mediante controles periódicos los cuales deben ser definidos por el encargado pertinente a esta área, así también como brindar la comunicación pertinente a los empleados del departamento para mejor eficacia de los controles en caso de ser necesario.
- Se instaurará una subdivisión del departamento de sistemas en cada sucursal para que se pueda agilitar el tiempo de solución del problema.

A.13.2 Intercambio de información

Objetivo:

"Mantener la seguridad de la información que se transfiere dentro de AMBACAR con cualquier entidad externa".

- Se implementará el uso de Office 365 ya que contiene mejor soporte y disponibilidad de herramientas empresariales, aparte tiene su espacio de almacenamiento y soporte técnico de mejores condiciones que G Suit.
- Se creará un documento formal de confidencialidad con terceros y personal de la empresa para manejar la información de una manera adecuada y segura no solo para el bien de la empresa sino también para los interesados.

A.18 Cumplimiento

El departamento de sistemas de la empresa AMBACAR debe en primer lugar revisar los controles y las medidas de mejora mencionadas con anterioridad, así podrá por medio de un documento de políticas ya definidas por medio de los altos mandos de la empresa cumpla todos los reglamentos legales y regulatorios, donde este documento sea actualizado con regularidad para cada sistema de la información de la empresa.

El departamento de sistemas para garantizar la seguridad de la información deberá realizar monitorios en las áreas y controles de la empresa para así cumplir con las políticas y buenas prácticas de seguridad implementadas en AMBACAR.

La empresa tanto como el departamento de sistemas debe también hacer cumplir ya las políticas una vez creadas para poder tener un mejor control de la organización en el ámbito de seguridad de la información, en caso del incumplimiento de alguna de las partes se debe proceder a su respectiva sanción al infractor por medio del organismo encargado de la empresa.

4.4.Plan de seguridad

Para la implementación del plan de gestión de seguridad de la información se establecen los siguientes procedimientos a desarrollarse según el análisis de controles de la Norma ISO/IEC 27001, adjuntando acciones, recursos, resultados a obtenerse, el tiempo estimado en realizarse y la persona responsable de ejecutar dichas acciones.

El plan de seguridad se lo realizo conjuntamente con el ingeniero Byron Jiménez (Encargado del área de redes) especificando a los responsables a quienes se les asignará cada una de las tareas.

Los integrantes del departamento de sistemas son:

- Ing. Jorge Parra
- Ing. Byron Jiménez
- Ing. Jaime López
- Sr. Rafael Suin
- Sr. Oscar Muñoz
- Sr. Jhonatan Escobar

Tabla 42.- *Plan de Seguridad AMBACAR*

Elaborado por: *Investigador*

PLAN DE SEGURIDAD AMBACAR							
Plan	**Control**	**Objetivo**	**Acción**	**Recursos**	**Resultado**	**Tiempo Estimado**	**Responsable**
P001	Directrices de gestión de la seguridad de la información	"Proporcionar orientación y apoyo a la gestión de la seguridad de la información de AMBACAR de acuerdo con los requisitos de la empresa, las leyes y normativa pertinentes".	Instaurar y documentar el manual de políticas de seguridad, mismo que deberá ser socializado con todo el personal de AMBACAR.	Análisis previo de los controles de la norma ISO/IEC 27001. Análisis actual de la empresa.	Documentación de manual de políticas de seguridad de la información a ocuparse para la gestión optima de la información.	3 semanas	Jhonatan Escobar
P002	Clasificación de la información.	"Asegurar que la información de AMBACAR reciba un nivel adecuado de protección de acuerdo con su importancia para la organización".	Clasificar la información en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas desde la gerencia de la empresa, así como adoptar un etiquetado pertinente acorde a los procedimientos y esquemas adoptados para la manipulación de la	Activos informáticos actualizados de la empresa. Análisis de los activos de la empresa para su buen funcionamiento.	Etiquetado de información relevante para la empresa y clasificación de información para su mejor control y uso.	2 semanas	Rafael Suin

			información dentro de AMBACAR.				
P003	Requisitos de negocio para el control de acceso	"Limitar el acceso a los recursos de tratamiento de la información y a la información de AMBACAR".	Realizar manual de políticas de acceso a la información mencionada en el control P001, mismo que deberá ser socializado con todo el personal de la empresa con el objetivo de proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados desde el departamento de sistemas de AMBACAR.	Análisis previo de políticas de acceso de seguridad, manual de buen uso de los servicios de red existentes en la empresa.	Documentación de políticas de seguridad y manejo adecuado de los servicios de red existentes en AMBACAR	2 semanas	Ing. Byron Jiménez
P004	Gestión de acceso de usuario	"Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios de AMBACAR".	Procedimiento formal de derechos de acceso, revocación de derechos de acceso y asignación de privilegios de acceso a la información de AMBACAR, así como también a los recursos de tratamiento de la información en caso de cese de funciones, culminación de contratos o cambios realizados en la empresa.	Nómina de empleados existentes de la empresa, sus actividades asignadas y privilegios que poseen.	Control de manejo de información por parte de los empleados y destinación de las funciones que realizan en la empresa.	1 semana	Ing. Byron Jiménez
P005	Responsabilidades de usuario	"Para que los usuarios se hagan responsables de salvaguardar la información de	Implantar un control a los usuarios para el seguimiento ordenado de las prácticas de AMBACAR en el uso de la	Nómina de empleados de la empresa, nómina de empleados que manejen información crucial para la misma.	Control de la información de la empresa y control ante perdida o mal uso de la	1 semana	Ing. Jorge Parra

		autenticación en AMBACAR".	información secreta de autenticación.		información secreta o crucial de la misma.		
P006	Control de acceso a sistemas y aplicaciones	"Prevenir el acceso no autorizado a los sistemas y aplicaciones de AMBACAR".	Instaurar un manual de inicio de sesión seguro a la información, implementando un proceso seguro de utilización de contraseñas confiables, para salvaguardar la información, restringiendo el código fuente de los programas de la empresa.	Listado de programas usados en la empresa y quien son los responsables en cada área de ocuparlos.	Manejo y control seguro de contraseñas, código fuente e inicio de sesión en las máquinas de la empresa, asignación de estándar para la asignación de contraseñas seguras.	2 semanas	Rafael Suin
P007	Áreas Seguras	"Prevenir el acceso físico no autorizado, los daños e interferencias a la información de AMBACAR y a los recursos de tratamiento de la información".	Implementar un sistema de seguridad biométrico para precautelar el control de acceso físico para el ingreso de personal autorizado a la información, protegiendo además las áreas que contengan información sensible y los recursos de tratamiento de la información, así como también el ingreso a las oficinas y despachos.	Nómina de empleados que posean acceso a información relevante de la empresa, listado de recursos a implementarse para la seguridad (Sistemas biométrico, señaléticas, chapas de puertas seguras, etc.)	Seguridad de los activos físicos e informáticos de la empresa, también seguridad y control en áreas que contengan información sensible y los recursos de tratamiento de la información	4 semanas	Ing. Jaime López
P008	Seguridad de los equipos	"Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de AMBACAR".	Realizar un proceso de mantenimiento bimestral para precautelar el buen funcionamiento de activos e información y cubrir un mayor rango de confiabilidad porcentual de este control, incluyendo: generador,	Listado de activos tecnológicos de la empresa (laptops, computadores de escritorio, switch, routers, generadores de energía, etc) y de sus	Mantenimiento de los activos cada 3 meses (al final del mes) para evitar perdida, daño o robo de la información relevante de la empresa, así también para precautelar la eficacia y	4 mantenimientos en forma bianual.	Rafael Suin

			equipos tecnológicos, e infraestructura.	mantenimientos anteriores.	rapidez de procesos que se realizan.		
P009	Protección contra el software malicioso (malware)	"Asegurar que los recursos de tratamiento de información y la información de AMBACAR están protegidos contra malware".	Realizar los respaldos o backups necesarios en períodos de tiempo determinados con los componentes óptimos para almacenamiento de los respaldos de la información, protegiendo la información con un antivirus actualizado tanto para servidores como para los equipos de cada usuario perteneciente a la empresa, aplicando normativas de restricción que denieguen el tráfico a través de la red y se habilitará el tráfico exclusivamente para los servicios se requieran.	Listado de Antivirus y de la actualización de los mismo en las máquinas y servidores de la empresa, listado de normativas que se manejen para el tráfico de datos a través de la red.	Actualización de antivirus en la empresa, mitigación en la perdida de información o daño de la misma, control de transferencia de datos relevantes para la empresa, consumo de red de la misma y backups de la información actualizada de la empresa para evitar perdida de la información.	Backups y actualización de antivirus 2 veces al mes.	Ing. Byron Jiménez
P010	Gestión de la vulnerabilidad técnica.	"Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas de AMBACAR".	Desarrollar un procedimiento adecuado para establecer y aplicar reglas de instalación de software seguro por parte de los trabajadores de AMBACAR.	Listado de softwares manejados por la empresa, listado de software instalados en cada departamento.	Reducción de vulnerabilidades técnicas en la empresa.	2 semanas	Óscar Muñoz
P011	Gestión de la seguridad de las redes.	"Asegurar la protección de la información en las redes y los recursos de tratamiento de la	Asignar a un responsable pertinente del departamento de sistemas para el cumplimiento de las políticas de gestión y recurso de redes e	Nómina de empleados del departamento de sistemas, verificación de recurso económicos para el departamento	Eficacia y agilidad en tiempo de solución en caso de caída de la red de la empresa.	4 semanas	Ing. Jorge Parra

		información de AMBACAR".	instaurar una subdivisión del departamento de sistemas en cada sucursal para que se pueda agilitar el tiempo de solución de problemas que se den en este ámbito.	de sistemas en cada sucursal.			
P012	Intercambio de información.	"Mantener la seguridad de la información que se transfiere dentro de AMBACAR con cualquier entidad externa".	Documentación formal de confidencialidad con terceros y personal de la empresa para manejar la información de una manera adecuada y segura no solo para el bien de la empresa sino también para los interesados. Implementar el uso de Office 365 ya que contiene mejor soporte y disponibilidad de herramientas empresariales.	Office 365, G Suit, nómina de empleados que poseen información relevante de la empresa.	Confidencialidad de la información a terceros para evitar el mal uso o perdida de la información.	4 semanas	Ing. Byron Jiménez

4.5.Cronograma de actividades

Para la implementación del plan de gestión de seguridad de la información se establece el siguiente cronograma a desarrollarse:

Tabla 43.- *Cronograma de actividades a cumplirse*

Elaborado por: *Investigador*

CRONOGRAMA ACTIVIDADES A CUMPLIRSE																														
Plan	***Control***	***Objetivo***	***Semanas***																											
			1	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***	***11***	***12***	***13***	***14***	***15***	***16***	***17***	***18***	***19***	***20***	***21***	***22***	***23***	***24***	***25***	***26***	***27***	***28***	***29***
P001	Directrices de gestión de la seguridad de la información	"Proporcionar orientación y apoyo a la gestión de la seguridad de la información de AMBACAR de acuerdo con los requisitos de la empresa, las leyes y normativa pertinentes".																												
P002	Clasificación de la información.	"Asegurar que la información de AMBACAR reciba un nivel adecuado de protección de acuerdo con su importancia para la organización".																												

P003	Requisitos de negocio para el control de acceso	"Limitar el acceso a los recursos de tratamiento de la información y a la información de AMBACAR".																															
P004	Gestión de acceso de usuario	"Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios de AMBACAR".																															
P005	Responsabilidades de usuario	"Para que los usuarios se hagan responsables de salvaguardar la información de autenticación en AMBACAR".																															
P006	Control de acceso a sistemas y aplicaciones	"Prevenir el acceso no autorizado a los sistemas y aplicaciones de AMBACAR".																															

P007	Áreas Seguras	"Prevenir el acceso físico no autorizado, los daños e interferencias a la información de AMBACAR y a los recursos de tratamiento de la información".																															
P008	Seguridad de los equipos	"Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de AMBACAR".																															
P009	Protección contra el software malicioso (malware)	"Asegurar que los recursos de tratamiento de información y la información de AMBACAR están protegidos contra malware".																															
P010	Gestión de la vulnerabilidad técnica.	"Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas de AMBACAR".																															

P011	Gestión de la seguridad de las redes.	“Asegurar la protección de la información en las redes y los recursos de tratamiento de la información de AMBACAR”.																																	
P012	Intercambio de información.	“Mantener la seguridad de la información que se transfiere dentro de AMBACAR con cualquier entidad externa”.																																	

4.6.Interpretación de Resultados

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías [12].

Para Montaño en (2015), la información junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

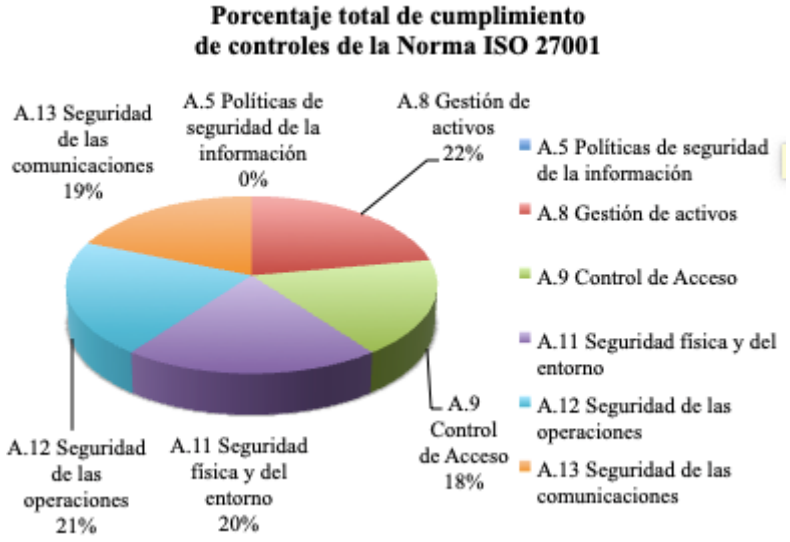
El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones [12].

Dentro de los resultados generales más importantes de la implementación de un sistema de gestión de la seguridad de la información están: el desconocimiento sobre aplicación de las normas de seguridad de la información y las limitaciones en la administración de seguridad informática y de la información que comprometen seriamente la imagen institucional.

Las posibles causas origen de los problemas están: mínima cultura en el tema de seguridad de información, la organización no formal del área informática, la no existencia de responsables de la seguridad, no existencia o falta de cumplimiento de políticas y procedimientos de seguridad dentro de la organización, falencias en el manejo de los inventarios de activos informáticos, en general la competencia limitada del personal para proteger los activos informáticos y de información frente a las amenazas y riesgos a que se ven enfrentadas [13].

El resultado muestra que es imperativo el apoyo y compromiso real de la gerencia o administración para el proceso de implementación de un SGSI de acuerdo al análisis realizado. Además, se debe formalizar los procesos y procedimientos que así lo requieran y documentarlos, ya que en la mayoría de casos se verificó la carencia de procesos de control, por lo cual se debe definir los procedimientos faltantes; también se debe implementar un sistema de control de seguridad informático estableciendo mecanismos que permitan el monitoreo permanente, orientando los protocolos hacia la mejora de la seguridad de la información.

Para Montaño (2015), ISO 27001 detalla en su Anexo C, punto por punto, la correspondencia entre esta norma y la ISO 9001 e ISO 14001. Ahí se observa la alta correlación existente y se puede intuir la posibilidad de integrar el sistema de gestión de seguridad de la información en los sistemas de gestión existentes ya en la organización. Algunos puntos que suponen una novedad en ISO 27001 frente a otros estándares son la evaluación de riesgos y el establecimiento de una declaración de aplicabilidad (SOA), aunque ya se plantea incorporar éstos al resto de normas en un futuro.



La figura muestra los resultados del análisis de brecha para los dominios en porcentaje (%) de cumplimiento. Los porcentajes en cada uno de los dominios son asociados a la escala de madurez e interpretados de acuerdo al porcentaje de cumplimiento de los mismos. Para los cálculos totales, se determinaron por el promedio de los valores para obtener el nivel de madurez en cada área y dominio de la norma ISO/IEC 27001.

La Gestión de la Seguridad de la Información debe pasar por varios niveles o escalones, cada uno con su coste asociado y contexto de aplicabilidad. Se comienza a perfilar una escala de progresión en lo que ahora conocemos como Sistemas de Gestión de Seguridad de la Información basados en la norma ISO 27001. Considerando los avances y las preocupaciones actuales, esta escala se compondría de los siguientes niveles:

- Nivel 0, el "sentido común".
- Nivel 1, el cumplimiento de la legislación obligatoria.
- Nivel 2, evaluación del proceso de Gestión de Seguridad.
- Nivel 3, analizar el riesgo y la gestión de su resolución.
- Nivel 4, adquisición de productos para integrarlos en los Sistemas de Gestión.
- Nivel 5, integración de los componentes certificados en sistemas compuestos y su certificación

Los niveles de madurez se pueden jerarquizar de la siguiente manera:

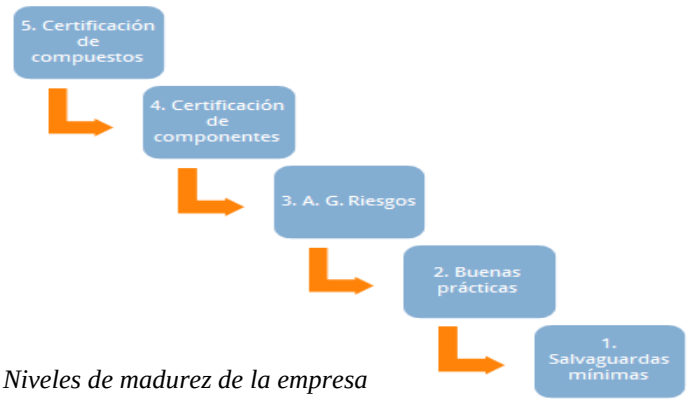


Fig. 37.- *Niveles de madurez de la empresa*

Tomado de: Montaño, V. (2015). Sistema de Gestión de la Seguridad de la Información

De esta manera, como resultado del análisis se encontró que frente a los requerimientos de la norma ISO/IEC 27001, la empresa analizada (AMBACAR) obtuvo una calificación promedio de 2, lo que se interpreta que se encuentra en un nivel de madurez Repetible, es decir, que se han adelantado actividades para la implementación de controles y buenas prácticas, que en su mayoría siguen un patrón regular, pero que no se han formalizado y por tanto sus procedimientos ejecutorios dependen de cada persona.

Es así que la empresa AMBACAR, al no disponer de un documento formal de políticas de seguridad de la información, no salvaguarda en su totalidad la información, exponiendo a factores de vulnerabilidad la misma.

CAPITULO 5

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- AMBACAR principalmente al no tener políticas de seguridad no posee una estructura sólida de protección de la información, es por esto que al manejar normas se cumple con el análisis y ocupación de la información requerido por la empresa pero sin cumplir la garantía de la integridad, disponibilidad y confidencialidad que deberían cumplir mediante la normativa ISO/EC 27001, así también, al mantener políticas de seguridad de la información los procesos serán realizados de mejor manera para cada uno de los controles analizados en el aparto de 4.2.5.
- Al analizar los servidores se evidencia que la seguridad de la información de la empresa no cuenta con un alto grado de salvaguarda donde se deberá tomar medidas correctivas contra amenazas y vulnerabilidades para el bien de la empresa.
- Al realizar el diseño de sistema de gestión de riesgos para la empresa AMBACAR de acuerdo a las necesidades de la empresa se concluyó que es posible mejorar la seguridad de la información así también como mejorar los controles de los activos informáticos los cuales son influyentes para que la información no sea sustraída, hackeada o vulnerada teniendo en cuenta las políticas que se deberán instaurar y donde deben ser revisadas periódicamente por el ente respectivo de la empresa.

5.2. Recomendaciones

- AMBACAR debe principalmente crear y analizar las políticas adecuadas mediante los controles estudiados en el apartado 4.2.5 y mediante el análisis de vulnerabilidades de los servidores con el fin de obtener la salvaguarda de la información de la empresa. Estas políticas deben ser revisadas con períodos pertinentes de tiempo con el fin de tener las políticas actualizadas.
- Las políticas deben ser socializadas a los empleados de la empresa con el fin de precautelar el manejo de manera eficiente la información.

- En cuestión de los servidores se deberá garantizar la integridad, disponibilidad y confidencialidad de la información contra posibles ataques o vulnerabilidades, esto se lo puede realizar mediante evaluaciones o ataques de prueba a los servidores en períodos paulatinos de tiempo establecidos y mediante controles periódicos de tiempo en cuestión de activos informáticos de la empresa.
- Se debe también asignar responsables para cada uno de los controles a realizarse con el fin de que el encargado pertinente lleve un control de cada uno de los aspectos que se evaluarán mediante las políticas instauradas por la empresa.

Bibliografía

[1] Guía Comercial de Quito, “Seguridad Informática.” 2015. [en línea]. Disponible en: www.guiaccq.com/product/index/403/.

[2] Ernst & Young, “Seguridad de la información en un mundo sin fronteras.” 2011. [en línea]. Disponible en: www.ey.com/Publication/vwluassets/Seguridad_de_la_informacion_en_un_m undo_sin_fronteras/$FILE/Seguridad_de_la_informacion_en_un_mundo_sin_fr onteras.pdf/.

[3] Terán Valenzuela, K. M. (2018). Guía para la implantación del SGSI con base en la NTE ISO/IEC 27000 para el servicio de agendamiento de citas del Contact Center del Ministerio de Salud Pública del Ecuador (Master's thesis, Universidad de las Fuerzas Armadas ESPE. Maestría en Gerencia de Sistemas.)

[4] Casadiegos santana, a. L., Quintero Jiménez, m. A. R. C. E. L. A., & toro rueda, m. I. L. E. I. D. Y. (2014). sistema de gestión de seguridad de la información (SGSI) para el área de contabilidad de la ese hospital local de rio de oro cesar (doctoral dissertation).

[5] Vallejo Cáceres, A. A. (2018). Propuesta de Sistema de Gestión de Seguridad de la Información para el centro de datos de la empresa Leterago del Ecuador SA (Bachelor's thesis, Quito).

[6] León León L. A. (2018) Planificación de un SGSI basado en la norma ISO 27001: 2013 en la empresa Mafelesa (Doctoral dissertation Universidad de Guayaquil, Facultad de Ingeniería Industrial, Carrera de Ingeniería en Teleinformática).

[7] Martelo, R. J., Madera, J. E., & Betín, A. D. (2015). Software para gestión documental, un componente modular del Sistema de Gestión de Seguridad de la Información (SGSI). Información tecnológica, 26(2), 129-134.

[8] Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. RISTI-Revista Ibérica de Sistemas e Tecnologías de Información, (22), 73-88.

[9] Iso27001, (2017). International Organization for Standardization. Recuperado de: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

[10] Delgado, M. F. (2017). Taller de Implementación de la norma ISO 27001. Recuperado de https://www.gobiernodigital.gob.pe/docs/ISO_27001_v011.pdf.

[11] Montaño, V. (2015). Sistema de Gestión de la Seguridad de la Información.

[12] Solarte, F., Enriquez, E., & Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001.

[13] Escuela Europea, 2019. Cómo evaluar las consecuencias y la probabilidad en el análisis de riesgos ISO 27001. Recuperado de: https://www.escuelaeuropeaexcelencia.com/2019/03/como-evaluar-las-consecuencias-y-la-probabilidad-en-el-analisis-de-riesgos-iso-27001/